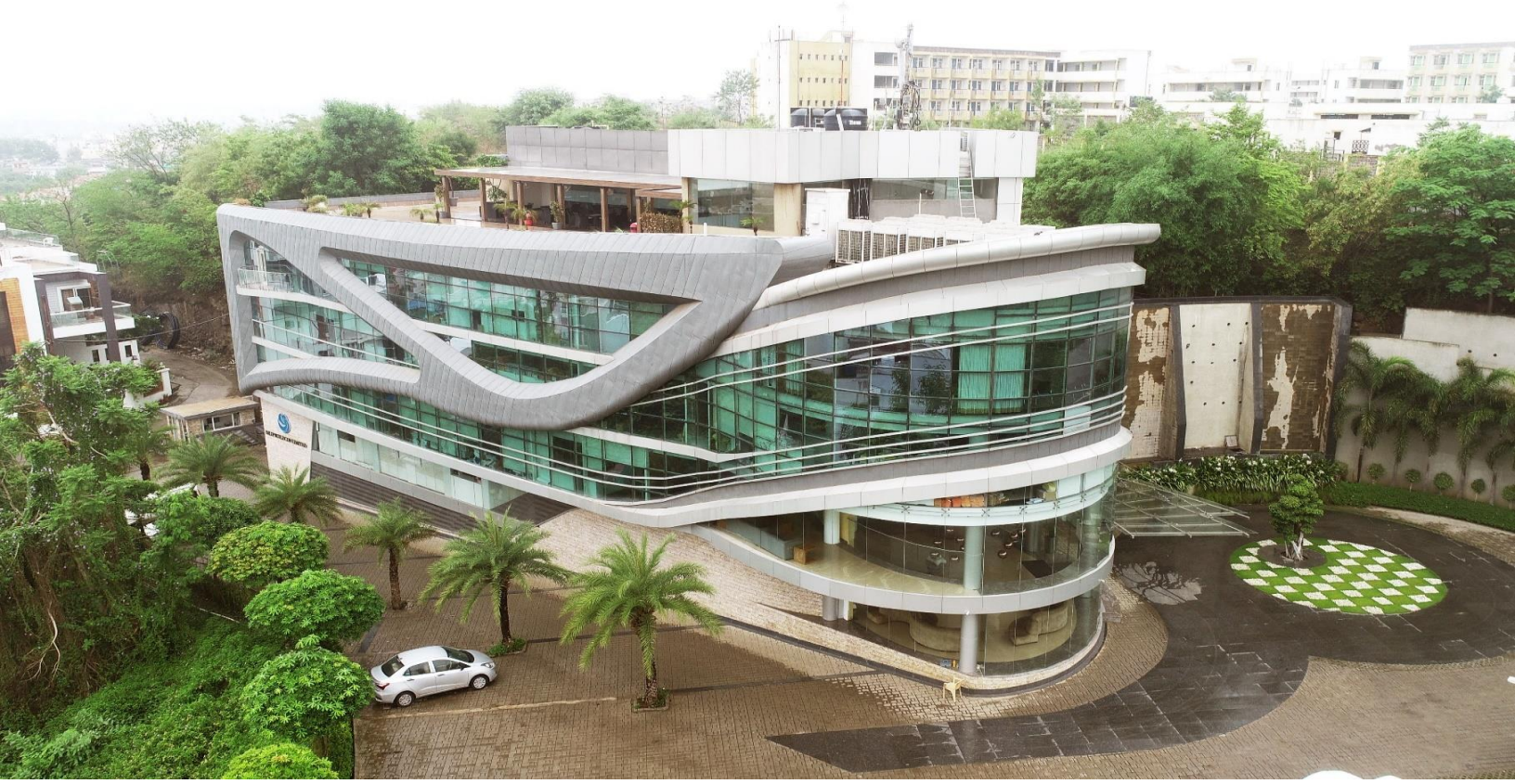
Dilip Buildcon Limited

IT Policy Manual

Issue No.1.0



	Prepared by	Reviewed by	Approved by
Name	Sachin Jaiswal	Satyanarayana Kasturi	Devendra Jain
Designation	AGM-IT	Chief Information Officer	MD & CEO
Signature			

DILIP BUILDCON LIMITED * BHOPAL *

S.No.	Section/ Policy No.	Details and reason for revision	Version No	Effective date
1	All	Initial Release	1.0	05-02-24
2	Access Control Policy	User Password Management	1.1	18-07-25
3	Access Control Policy	VPN Policy included	1.2	30-10-25

Dilip Buildcon Limited (DBL) has recognized the importance of Information Technology (IT) and IT infrastructure which is playing a major role in the company's growth. Having the high visibility and role of IT in the organization, strong IT policies and procedures have been implemented ensuring clear, transparent, and smooth business operations.

It is the policy of Dilip Buildcon Limited (DBL) that its information assets are appropriately protected against the consequences of breaches of confidentiality, failures of integrity and/ or interruptions to their availability. DBL IT Policy provides management direction and support for IT Management and security across DBL Project Offices.

The policies specified in this document are applicable to HO and all Project Offices where DBL's information assets are located and/or used. This policy is applicable to all associates and third party staff referred to as 'users' who are using information assets of DBL.

This manual is applicable to DBL as well as its subsidiaries i.e., Jalpa Devi Engineering Private Limited, Deevin Seismic Systems Private Limited, Aarneel Techno Craft Private Limited.

Acronym	Description
CAB	Change Advisory Board
DBL	Dilip Builldcon Limitied
DLP	Data Leakage Prevention
ERP	Enterprise Resource Planning
HOD	Head of Department
HR	Human Resources
MBSS	Minimum Baseline Security Standards
ISM	Information Security Manager
IT	Information Technology
ITCO	Information Technology Corporate
ITD	Information Technology Department
PAM	Privileged Access Management
PT	Penetration Testing
OS	Operating System
VA	Vulnerability Assessment

References

#	Description
1	ISO 27001: 2022

The Policy Manual of Dilip Buildcon Limited (here onwards referred as DBL) is issued under the authority of MD & CEO. All pages of IT Policy Manual include version number and effective date. The first issue will have Issue No.01 and all pages with version number 00. When any page of a particular section is revised, the version number of the particular section will be incremented. When the whole manual is revised or the more than twenty revisions are done or as decided by CIO, the issue number will be advanced with version number of all sections starting from 00

The changes will be identified in the amendment record sheet and approved by MD & CEO

Responsibility

It is the responsibility of CIO and all HODs to ensure that controls specified in the IT Policy Manual are implemented.

It is the responsibility of associates and third-party staff (those who are using DBL's information assets) to read, understand and adhere to the DBL IT Policy Manual

Exception Management

If, due to any constraint in the application or infrastructure environment or business mandate, it is not possible to implement any controls specified in the policy, an exception to override the IT policy shall be requested. The exception shall have a valid business justification, and be approved by the CIO.

These exceptions shall be valid only for the period substantiated by business function, or for a period of 60 days, whichever is less. Within this time period, an alternative solution shall be put in place to avoid overriding the IT Policy Manual. In a case where there is a need to renew the exception request, this shall be treated as a new exception.

Review and evaluation

The IT Policy Manual shall be reviewed at the time of any major change(s) in the IT environment or once every year, whichever is earlier.

Non-compliance

All associates and third-party staff using DBL's information assets shall comply with the DBL IT Policy Manual. Non-compliance with the IT Policy Manual is ground for disciplinary action(s), up to and including termination. If it is found that the action is inadvertent or accidental, first violation shall result in a warning. A relevant warning letter shall be placed in the involved individual's personal file. Subsequent violations could result in dismissal. All non-compliance must be dealt with disciplinary committee whose members should comprise minimum from IT and HR department and any other as per management discretion.

Schedule

This Policy Manual is reviewed once in a year for its continued suitability or earlier as deemed necessary due to required updates or changes

Enforcement

a) Violations of the provisions of this Policy are subject to DBL's **Disciplinary Process.** Disciplinary actions taken may be up to and include dismissal of the User or termination of contract and may extend to legal action.
b) Where allegations are made about violations of this Policy, the subject of such allegations and the events associated with them may subject to investigation by DBL or others acting on DBL's behalf.
c) Implementation of the policy will be verified during the internal audits and Management review meetings.

Confidentiality

This document contains restricted confidential information pertaining to DBL Employees and others must take steps to prevent intentional or accidental access outside the scope of access indicated.

Disclaimer

This document is confidential and is solely for the information of DBL and must not be used, circulated, quoted, or otherwise referred to for any other purpose, nor included or referred to in whole or in part in any document without DBL's prior written consent.

A. Objective

The objective of Access Control Policy is to establish the guidelines by which identity and access management for DBL's information and information systems (operating systems, applications, databases, network equipment and others information handling systems – collectively "**IT Systems**") is implemented.

B. Scope

This Policy applies to DBL's IT Systems and all DBL assets, including those in both electronic (e.g., information systems, applications, systems platforms, and computer operations) and physical (e.g., vendor contracts, loan documentation, client files, and personnel information) formats. This includes information assets processed, transmitted, or stored by third-party service providers.

C. Policy Statement

The access to DBL information and information systems (Operating Systems, Applications, Databases, network equipment and others) should be according to the principles of "least privilege" and only on a "need to know" basis. The procedures should be to protect the information in each application or system from unauthorized access, modification, use, disclosure, or destruction to ensure that information remains accurate, confidential, and is available when required.

The following shall be considered before granting access:

- eligibility criteria before granting access.
- the facilities, systems, and data to which access is required.
- the justification for granting various access based on business requirements.
- any special instructions from DBL before granting access.
- all contractual obligations regarding protection of (or access to) data and services.
- Access shall be provided on receipt of approved access control.

The implementation of this Policy and any accompanying procedures shall abide by applicable laws.
In case where customer needs to be provided access to DBL's IT Systems, the request should be directed to DBL's cyber security team and approved by the department head. All necessary security requirements should be identified and addressed before any access is provided.
Access controls must include an enforcement mechanism that operates at a minimum at three standard levels – facility, system, and data.

1. Access Management

1.1 User registration and de-registration

a) User access to DBL's IT Systems must be provided through formal user registration process that includes approval of access rights from HR-authorized personnel prior to access being granted.
b) Revocation of user access to DBL's IT Systems should follow a formal de-registration process, which includes provisions for automated or timely revocation of access rights by the business head and IT Team.
c) Unique User-IDs shall be assigned to all the users to ensure accountability of individual users for their activities.
d) Every New Joiner's Email id/General Departmental Email ID/Consultant Email
e) Users shall be responsible for all activities performed using their personal User-IDs. A User-ID shall not be used by anyone other than the individual to whom it has been assigned. Users shall not allow others to perform any activity using their User-ID.
f) Users shall use information processing equipment for authorized business purpose. Incidental personal use shall be allowed as long as it does not interfere with the business activity and productivity.
g) User-IDs shall be disabled/ locked if he/she does not logon to the system for more than thirty days. The User-ID shall be enabled/ unlocked only on written user request with the department head's approval.

h) Distinct User-IDs shall be assigned to temporary staff, contractors that can be easily identified and shall automatically expire after certain time interval.
i) It is recommended that User Registration and De-Registration should be done on online portal for records and easy tracking for compliance to ISO27001 Audits

2. Privilege Management

a. Privileges associated with each type of information system (such as network infrastructure, finance details, business applications, databases, and marketing) should be identified.
b. Privileges are allocated to individuals based on the requirements of their job function and role, on authorization from appropriate personnel. Additional privileges beyond what is identified as being required for the job function require written approval from appropriate personnel.
c. Administrative privileges shall not be given to users, unless it is a business requirement.
d. Any changes required in the privileges shall follow the Change Management Procedure

3. User Password Management

A. Users and authorized employees responsible for password administration must keep passwords confidential; passwords should not be shared, written, posted, or otherwise divulged in any manner. During the User creation process, an initial password will be securely provided to the User. The User must change this initial password immediately after the first login.
B. Every password must:
    - have at least 8 characters, 1 special character and 1 number.
    - have uppercase, lowercase, numeric, special characters.
    - changed regularly (admin passwords must be changed every 45 days; User account passwords must be changed every 90 days).
    - shall not be re-used.
C. The following password and account policy will be enforced for all users and administrative accounts on operating systems, applications, databases, and all other information protected by password controls:

Table 1 - User Password Management

	Operating System	Application	Database
Minimum password length	8 characters	8 characters	8 characters
Maximum password age	60 days	60 days	60 days
Password history	3	5	3

Inactivity timeout	20 minutes	20 minutes	-
Number of inactive attempts for account lockout	3 attempts	3 attempts	3 attempts

D. If it is reasonable to believe that a password has been disclosed or compromised, it must be promptly reset.
E. All Systems password strong policy should be implemented in Active Directory Group Policy so that user is enforced to keep strong passwords as recommended above
F. Intruder detection shall be implemented wherever possible.

4. Deactivation

Three consecutive invalid login attempts by Users will automatically lock or deactivate the User account. In case of logins of privileged accounts, exceptions to lockouts should be documented and approved by the IT department heads.

5. Reactivation

a) In case of a login account being de-activated, the administrator will only reactivate the same on receipt of a request from the User with approval of Department head.
b) During odd hours (late night hours / night shifts) the administrator will obtain approval from the team lead (who in turn will obtain consent from the Department head over phone. The admin also will respond to the User email request, stating details of telephonic approval and copying to the respective department head.
c) In case where telephonic approval could not be taken (due to the unavailability of the approving authority), the administrator will confirm the authenticity of the User email either by speaking to the User in person or calling user over the phone. After such confirmation, the administrator shall activate the User account and respond to the User mail request stating all details and copying the team lead/department head as applicable.

6. Review of user access rights

The respective department heads for all individual users or groups must review the access rights or privileges assigned to the corresponding SAP system once in a year and Active Directory system twice yearly.

7. User Responsibilities

Users shall be instructed that usernames and passwords must not be shared by Users.

8. Operating system access control

a. Minimum Baseline Security Standards ("**MBSS**") or hardening standards for all operating systems and critical applications should be developed and maintained. All installations of the operating systems and applications should be configured as per the MBSS.
b. Restrictions should be enforced at operating system level to ensure adherence to password requirements.
c. Wherever technically feasible operating systems, applications and databases should timeout and clear the screen automatically if the terminal is inactive for more than 5 minutes or as detailed in User Password Management (table 1, above).
d. All default administrator logins should be disabled. The domain administrator should be added to the administrator group for their day-to-day operations (e.g., desktop/laptop management).

9. Application and database

9.1 Application Access control

1. To safeguard applications, DBL will restrict business application system access information on a need-to-know basis.
2. User rights shall be based on a least-privileges basis, so that they are limited to only those functions which they are authorized (e.g., read, write, delete, and execute). User rights shall be reviewed regularly on a periodic basis to ensure that no user or group has excessive privileges.

9.2 Database access control

a. Database commands and utilities will be restricted to database administrators only.
b. The central database administrator will be responsible for maintaining a record of essential programs and utilities. Changes to these programs and utilities will be as set out in the Change Management Policy.
c. Access to information and application system functions by Users and support personnel will be restricted in accordance with this Access Control Policy and procedures.
d. Audits (with the scope defined and agreed to by the IT Committee) will be performed at least annually by the relevant IT department head to ensure application security is maintained. In case of third-party applications used by DBL, written assurance should be obtained from these vendors that their products satisfy DBL's application security requirements or otherwise meet or exceed recognized international security standards.
e. The use of utility programs that can override system and application controls must be restricted and tightly controlled.
f. Restrictions on connection times must be used, as applicable, to provide additional security for all high-risk applications.
g. No employee shall have direct access to the database of any application system.
h. Its recommended to employ a Database Access Monitoring (DAM) Tool for clear monitoring , restrict based access controls.

9.3 Network Access control

a) Once created, Users must change their password on the first logon. If passwords are required to be shared between multiple administrators, an entry must be made by the respective administrator in the register.
b) Occasionally, password and account policy parameters may not be able to be followed due to system limitations or business necessity. If this occurs, specific mechanisms should be put in place to obtain approvals and implement countermeasures to mitigate the risk of not following the password policy.
c) Where it is not possible to implement individual User-IDs and passwords within the application itself (due to design parameters), alternative solutions for restricting and auditing access privileges should be evaluated for feasibility and security and should be implemented, but only after approval is obtained from the IT Department.
d) Network access passwords:
e) shall not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.
f) shall not be stored at the System / Application level in clear text or in any easily reversible form.
g) In case of authentication through public networks use of strong encryption is to be encouraged. Passwords must not be transmitted over the network (internal or public) using clear text.
h) If it is reasonable to believe that a password has been disclosed or compromised, it must be promptly reset.

10. Sensitive system isolation

All sensitive systems should be identified. All sensitive systems should have a dedicated (isolated) computing environment.

11. IT Ticketing and Help Desk Management

S. No.	Activity Description	SLA (TAT) Business Hours			Remarks
		High	Medium	Low	
1	SAP access grant/revoke controls	4	8	16	Minimum one working day. If there is any deviation, user shall be notified through email.
2	Website Access/Removal	4	8	16	Minimum duration of 1-2 Hours. If there is any deviation, user shall be notified through email.
3	NAS Drive access grant/revoke	4	8	16	Minimum one working day.if there is any deviation, user shall be notified through email.
4	USB/Bluetooth Device access Grant/revoke	4	8	16	Minimum duration of 1 Hour. If there is any deviation, user shall be notified through email.
5	Email ID creation/modify/deletion	4	8	16	Minimum one working day. If there is any deviation, user shall be notified through alternate email.
6	ESS access grant/revoke	4	8	16	Minimum one working day. If there is any deviation, user shall be notified through email.
7	User network rights permissions grant/revoke	4	8	16	Minimum duration of 4-5 Hours. If there is any deviation, user shall be notified through email.

12. VPN Policy

An inhouse AD server is in place, whenever a user is in the local network then policy will apply on that user.
The tracking is enabled through AD. For the users who are outside the domain network and login through VPN. The controls are established through VPN passwords which will expire in 30 days.

1. Authentication:
   - VPN access will be granted only to authorized users with valid credentials. Passwords will expire every
   30 days and must meet complexity requirements.
2. Authorization:
   - Access will be granted based on least privilege principle.
   - User access will be reviewed regularly.
3. Monitoring and Logging:
   - VPN connections will be logged and monitored for security incidents.
   - Logs will be retained for a period of three months or as decided by CIO

4. Security Controls:
   - VPN connections will use encryption (e.g., SSL/TLS).
   - VPN clients will be configured to meet security standards.
5. User Responsibilities:
   - Users will maintain confidentiality of VPN credentials.
   - Users will report security incidents or suspicious activity.

Implementation and Maintenance:

1. VPN access will be provisioned and deprovisioned based on user status.
2. Regular security audits will be performed.
3. Users will be trained on VPN policy and security best practices.

A. Objective

The objective of this Anti-Malware Policy is to minimize the impact of any malicious code such as viruses, worms, script attacks, backdoors, active content, and Trojan horses (collectively, "**Malicious Code**" or "**Malware**") that can spread in the DBL Network.

B. Scope

This Policy is applicable to all computing resources of DBL including desktops, laptops, servers, software, application source code, and communication equipment (e.g., routers etc.).

C. Policy Statement

All IT infrastructure facilities shall be protected against attacks by Malicious Code using industry standard safeguards. Adequate resources shall be provided to prevent malware attacks and to contain the impact and damage in the event of a successful attack. Procedures shall be developed to ensure continuous compliance with the above requirements across all the IT infrastructure of DBL.

1. Salient features:

a) All of DBL's computing resources shall be adequately protected with anti-virus software and periodically scanned for virus existence by IT infrastructure team. If a computing resource is required to use antivirus software, that software must be configured to automatically install updates to both the antivirus software and the virus definitions.
b) Ensuring up-to-date virus signature files on desktops/laptops & servers shall rest with the IT infrastructure team.
c) The server operations team should ensure that antivirus software is installed on all servers with the latest virus signatures.
d) User responsibility shall include checking for the existence of up-to-date virus signature files on his/her desktop/laptop and reporting to the IT department in case of failure of automatic update/signature files.
e) Failure to use appropriately configured antivirus software may result in loss of access to the DBL network.
f) Unless absolutely required and otherwise approved, administrative rights will not be provided to Users in desktops and laptops. This will help:
g) prevent the installation of unauthorized / unlicensed / untested software; and
h) prevent Users from disabling antivirus software.
i) In the event a User believes that Malicious Code has infected their computing resource (e.g., desktop or laptop), he/she shall promptly ensure that their desktop network interface cable is disconnected from the network and report immediately to the IT infrastructure team.
j) Users shall install and use only licensed and approved software on DBL IT Systems (including desktops, laptops, and servers). Users shall not use or install unlicensed or unauthorized software on to DBL IT Systems or their computing resource. Users who do so will be held responsible for all damage or consequences that result.
k) Users shall refrain from sharing their folders. If required to do so, any shared folder must be protected with a password.
l) Responsibility for conducting periodic software audits on desktops/laptops or other computing resources shall rest with the infrastructure Head in coordination with the IT infrastructure team.
m) All incoming mails to the DBL domain should be scanned for malware at the gateway level. The same shall be done for the outgoing mail leaving the DBL domain.
n) Daily monitoring activity of security patch(s) update or any failure
with IT SLA(TAT) as below
High Priority: 4 Business Hours
Medium Priority: 8 Business Hours
Low Priority: 24 Business Hours

2. Controls Against Malware

To protect the integrity of software and information from damage by malicious software the following activities are carried out:

a) Antivirus within built firewall software is installed on all servers and Laptops to protect the systems from any threats arising out of virus attack. Antivirus is updated automatically as and when latest patches are released. (The options are invoked to check for automatic updates). IT Team subscribes to specialist groups to keep a track of the threats or virus attacks arising out of various sources; accordingly users are alerted of the potential damage and precautions are taken.
b) Virus scan software will be updating every laptop and server every day. This is an automated process.
c) When the laptop is in offline mode the Antivirus patches do not get updated, the moment laptop gets connected online, automatically, the patches get updated.
d) Firewall with subscriptions of Anti-Spam, Anti-Virus, Intrusion Detection and Prevention services, ensure protection for external virus attacks through internet tunnel.
e) DBL employees are not allowed to use any of the pirated software under any circumstances. To prevent such installations IT Team shall block the options to install the software at laptop level thru domain controllers for all the users.
f) Users are informed to bring to the notice of IT Team if they encounter with malicious software. Depending on the severity, actions are initiated by IT Team to prevent any damage to information processing systems.
g) Windows software updated service configured for servers and laptops for deployment of Patches, before deploying the patches to workstations and laptops they are tested in IT Team Laptops, once testing has done successfully then tested patches will be deployed to user laptops as per Schedule.
h) Users are trained in using the systems in efficient manner with clear note on do’s and don’ts. This policy requires that the individuals are aware of the way the systems and information processing facilities are used.

A. Objective

The objective of this Asset Management Policy is to provide a framework for structured and secure management of Information Assets of the DBL throughout their lifecycle and to manage and maintain software in compliance with license agreements to ensure delivery of value at optimal cost.

B. Scope

This Policy applies to DBL's IT Systems and all DBL Information Assets including those in both electronic (e.g., information systems, applications, systems platforms, and computer operations) and physical (e.g., vendor contracts, loan documentation, client files, and personnel information) formats. This includes Information Assets processed, transmitted, or stored by third-party service providers.

C. Policy

1. Asset management

This Policy is established to ensure that: all the Information Assets of DBL:

a. All Information assets are classified and managed based on their criticality to ensure (confidentiality, integrity, and availability)
b. All Information assets are appropriately protected.
c. Information handling or exchange of information is in accordance with the classification; and
d. To prevent unauthorized disclosure, modification, removal, or destruction of Information Assets, and/or interruption to business activities.
e. Information Asset management assists an organization to keep track of its information assets, software assets, physical assets, document assets, services assets, and people assets.

2. Responsibility of Assets

2.1 Inventory of Assets

a) Each business function shall be responsible for the identification of Information Assets and Information Systems used for processing and storing information; they shall maintain an inventory of such assets in concurrence with the IT Team of the local DBL entity.
b) IT Team of the local DBL entity shall be responsible for ensuring that the Information Asset Register is accurate, updated and maintained regularly.
c) The Information Asset Register shall contain the following necessary information as a minimum:
    - Type of Information Asset along with a brief description(Physical, Software, Service, People, Document etc,)
    - Information Asset owner/custodian
    - Information Asset location
    - Information Asset value for confidentiality, integrity, and availability
    - Classification of the Information Asset
    - Serial Number
    - Make Model and Warranty information

2.2 Ownership of Information Assets

a) All the information and Information Assets associated with information processing facilities shall be assigned ownership to an individual or department that has management responsibility for controlling the production, development, maintenance, use and security of an Information Asset.
b) Each Information Asset shall have an owner and nominated custodian who may be different from the asset owner.

c) The owner shall be responsible for:
   - Ensuring that information and Information Asset associated with information processing facilities are appropriately classified.
   - Defining and periodically reviewing access restrictions and classifications, considering applicable access control policies.

d) Information Asset owners or their delegates shall be responsible for the following activities:

   - Approve information-oriented access control privileges for specific job profiles.
   - Approve information-oriented access control requests that do not fall within the scope of existing job profiles.
   - Select special controls needed to protect the information, such as additional input validation checks or more frequent backup procedures.
   - Approve all new or substantially enhanced application systems that use their information before these systems are moved into production operational status.
   - Select a security classification category relevant to their information and periodically review this classification for possible downgrading or upgrading.

e) Asset owners shall not delegate ownership responsibilities to third-party organizations such as outsourcing organizations, or to any individual who is not a full-time employee of DBL.

f) Software asset management includes maintaining software license compliance, tracking the inventory and usage of software assets in a software inventory and maintaining control over the deployment and use of software assets.

g) Procurement details, such as the number of licenses granted, expiry date of licenses, etc., of software purchased shall be recorded by the IT team.

h) Data in the software inventory shall be synchronized with software purchase data e.g., date of purchase, expiry date of the license and number of licenses etc. Original physical or soft copy of the license received from the vendor, if any, on purchase shall be filed appropriately and stored securely.

i) Software usage and deployment shall be tracked and reconciled against purchase data on a periodic basis. Any discrepancies, if observed, shall be reported to the asset owner, and IT Team.

j) In the event a provision of a software license agreement is believed to have been contravened, the asset-owning team shall initiate immediate corrective actions.

k) Software purchases and related data shall be tracked and regularly monitored. The IT Team, along with the respective business owner of the applications, shall be responsible for conducting annual reviews on this data to determine, but not limited to, the following:

   - If more licenses are being used than purchased; and
   - If new software or a greater number of licenses need to be procured to meet future business requirements.

l) The IT team shall, at least once per year, conduct a review of servers, desktops & laptops to determine if any unauthorized and unlicensed software is installed.

2.3 Acceptable Use of Information Assets

- Acceptable use of Information Assets associated with information processing facilities shall be clearly defined.
- All Users who use or interface with Information Assets associated with information processing facilities shall acknowledge in writing their awareness of acceptable use of such assets.

2.4 Return of Assets

a. Upon termination of their employment or contract, DBL employees and contract partner shall return / hand-over, all DBL's Information Assets in their custody or under their control.
b. In case of any damage/deterioration/impairment to Information Assets which are assigned to employees, the penalty/repair amount is recoverable from employees as part of the termination/exit process; any exceptions to the process shall be approved by senior management.

2.5 Information Classification

2.5.1 Classification of information

a) To ensure that confidentiality, integrity, and availability of Information Assets is maintained, an information classification scheme shall be created and maintained by the level of security to be applied to the Information Assets of DBL will depend directly on the classification of the information.
b) Information Assets and information processing systems shall be classified based on their business value, legal requirements, sensitivity, and criticality to the organization.
c) Information Assets shall be classified under one of the following four categories based on the sensitivity and criticality of DBL

- **Highly Confidential:** Information, the unauthorized disclosure, alteration, misuse, or destruction of which would cause a significant level of damage to the business, stakeholders, business partners, employees, and/or customers. This information, if not adequately protected, may result in non-compliance with applicable laws. Access to this information requires approval from the owner of the information and shall be given on a need-to-know basis. Examples of highly confidential data include login passwords, keys, audit logs, personally identifiable information, bank account information, and credit card information.
- **Confidential:** This classification applies to the Information Assets containing the information of DBL, the disclosure unauthorized disclosure, alteration, misuse, or destruction of which would cause damage to the business, stakeholders, business partners, employees and/or customers. Access to this information requires approval from the owner of the information and shall be given on a need-to-know basis.
- **Internal:** This classification applies to the Information Assets containing the information internal to DBL. While its unauthorized disclosure is against DBL's Policy, such disclosure is not expected to impact the business seriously or adversely, stakeholders, business partners, employees, and customers; and
- **Public:** Data would be classified as public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the intended users. Examples of public data include whitepapers, User guides. While few or no controls are required to protect the confidentiality of public data, some level of control is required to prevent unauthorized modification or destruction of public data.

d) The Information classification process must be completed for existing data and must be undertaken for any new information whether it is in hard copy or soft copy.
e) Information stored in several media formats (either hard copy or electronic) shall have the same level of classification.

3. Labelling of Information

a. All Information Assets shall be labelled as per the Information Assets classification. The asset owners are required to ensure that their Information Assets are appropriately labelled (marked)

to provide adequate level of protection. This shall exclude Information Assets classified as 'Public'.

b. The Information Asset and information processing system handling and level of security provided shall be in accordance with the labelling of the Information Asset.
c. Information labelling procedures shall be developed and implemented. All Information Assets shall be labelled as per each asset's classification. Employees who may encounter 'highly confidential' and/or 'confidential' information are expected to familiarize themselves with the information classification scheme, and to consistently use it in their business activities.

d. Labels for sensitive information shall appear on the outside of external hard disks, magnetic tape reels, USBs, and other storage media. If a storage volume such as a hard disk contains information with multiple classifications, the most sensitive category shall appear on the outside label.

4. Handling of Information Assets

1. Information Asset handling procedures (including the secure processing, storage, transmission, and destruction) shall be followed for each classification level. Retention period for all records must comply with applicable legal requirements.
2. To protect information from unauthorized disclosure or misuse, handling and storage of Information Assets shall be in accordance with the established standard.

5. Media Handling

5.1 Management of Removable Media

1) DBL shall establish procedures for the management of removable media consistent with the information classification, and which shall stipulate the requirements for authorization, issue, operation, use, inspection, retirement, and disposal of media.
2) If removable media are used (e.g., tapes, removable HDD, CDs, DVDs, USB, SD cards) to store DBL information, adequate protection shall be used by the asset owner to protect content on the media against unauthorized access, misuse, and corruption.
3) Users shall be responsible for protection of removable media being used by them and shall ensure its storage under lock and key in their absence.
4) To mitigate the risk of media degrading while stored data are still needed, the data should be transferred to fresh media before becoming unreadable.
5) Where there is a need to use removable media the transfer of information to such media shall be monitored

5.2 Disposal of Media

a) Prior to disposing (which includes destruction, sale or disposal) of any storage media or computing devices containing storage media (including, but not limited to, desktops, laptops, PDAs, etc.) such media or device shall be inspected by competent personnel from the IT department, to ensure no DBL information continues to reside on the media/device in a form that may be used or rendered usable, who shall then formally sign off on same before releasing the device or media from secure custody.
b) Media shall be disposed of securely when no longer required, using documented procedures. The level of destruction or disposal of media will depend on the information or data stored in the media (if any) and the criticality of the information as per the information classification guideline.

S.No	**Request For**	**Requirement Type**	**Subject Type**	**Approval Required**	**Action Performed**	**Condition**	**Turn around Time for all IT related request**
1	Laptop	New requirement for an official	NA	**HR-Head/Management :** Mail for GM and above should come through HR-Head/Management. Approval is not required. **Rest of cases Management approval is a must.**	**First Step:-** Laptop handover from existing stock (either new or old) meeting the requirement.	The IT team will inform the store team to issue the system as per the user's request.	When store team hand-over the system to us, we will configure the system and issue it to the user **(Minimum duration of 4-5 Hours).** And if there is any deviation, we will inform the user via email.
					Second Step:- If above condition not met then - initiation to procure new laptop	The IT team will inform the purchasing team to purchase the system as per the user's request. Which **takes 10–15 days.**	
2	Laptop	Issue in existing laptop	Repair	NA	1) IT team would check and	If the laptop is not repairable at the office	**In the case of repair :** The vendor require

					repair the laptop.	premises, then send it to the vendor for repair.	s a minimum of 3-4 days. And if there is any deviation, we will inform the user through email.
					2) Standby laptop could be provided if available in stock.	In this case, issued a temporary laptop, to the user.	As soon as the store team hands over the system to us, we will configure the system and issue it to the user **(Minimum duration of 4-5 Hours)**. And if there is any deviation, we will inform the
					3) After vendor confirmation, the system is not repairable. 1) Issue a similar configuration system to the user after approval from the IT head.	After approval from the IT head, the IT team will give a request to the store team to issue the system.	

							user via email.
3	Laptop	Issue in existing laptop	Replacement	1) IT Head	1) If IT team found the laptop cannot be repaired then:	Replacement laptop would be provided (either new or old as per the stock and requirement)	As soon as the store team hands over the system to us, we will configure the system and issue it to the user **(Minimum duration of 4-5 Hours).** And if there is any deviation, we will inform the user via email.
				2) **Management Approval required** only for hi-end configuration	If user requests, please replace my existing laptop with a higher configuration laptop - initiation to procure new laptop post approval from Director Sir.	The IT team will inform the purchasing team to purchase the system as per the user's request. **Which takes 10–15 days.**	
4	Desktop	New requirem	NA	1) Dept. Head	1) Desktop handover from	After confirmaiom mail. The IT	As soon as the store team

		ent for an official			existing stock (either new or old) meeting the requirement.	team will inform the store team to issue the system as per the user's request.	hands over the system to us, we will configure the system and issue it to the user **(Minimum duration of 4-5 Hours).** And if there is any deviation, we will inform the user via email.
				2) HR	For new employee : Mail should come through HR department.		
				3) IT Head (only for new pruchase)	2) If above condition not met then - initiation to procure new desktop	The IT team will inform the purchasing team to purchase the system as per the user's request. Which takes 10–15 days.	
5	Desktop	Issue in existing desktop	Repair	NA	1) IT team would check and repair the desktop.	After confirmaiom mail. The IT team will inform the store team to issue the system as	As soon as the store team hands over the system to us, we will
					2) Standby desktop		

					could be provided if available in stock.	per the user's request.	configure the system and issue it to the user **(Minimum duration of 4-5 Hours).** And if there is any deviation, we will inform the user via email.
6	Desktop	Issue in existing desktop	Replacement	1) IT Head (only for new pruchase)	1) If IT team found the desktop cannot be repaired then: Replacement desktop would be provided (either new or old as per the stock and requirement)	After confirmaiom mail. The IT team will inform the store team to issue the system as per the user's request.	As soon as the store team hands over the system to us, we will configure the system and issue it to the user **(Minimum duration of 4-5 Hours).** And if
					2) It team would follow	The IT team will inform	

					the process to procure new desktop post approval from IT head	the purchasing team to purchase the system as per the user's request. **Which takes 10–15 days.**	there is any deviation, we will inform the user via email.
7	Rest of the IT Hardware Like: Plotter/Photocopier/Printer/Scanner	New requirement for an official	New requirement for an official	**Management Approval required**	After getting all the necessary approvals	The IT team will inform the purchasing team to purchase the system as per the user's request. **Which takes 20–30 days.**	As soon as the store team hands over the system to us, we will configure the system and issue it to the user **(Minimum duration of 5-7 Working days).** And if there is any deviation, we will inform the
		Issue in existing	Repair	**IT head/management approval is required** according to the cost.		Proceed to repairing	
		Issue in existing	Replacement			Proceed to replacement	

							user via email.

1. Laptop and Desktop will be provided to DBL Employees per the grades and designations for official usage.

2. The store department should publish available inventory every weekend to the IT Department.

3. The HR Department should provide new recruitment details on a monthly basis to the IT department.

4. Whenever a new employee Joins the organization 8 working Hours are required to allocate the System as per grade and designation.

5. Procurement of New Laptops and Desktops as per Store inventory replenishment with CIO & Procurement Head approval (Mont

6. Replacement of existing Laptop / Desktop users should send requests/recommendations to the CIO

7. Replacement Required New Laptop / Desktop HOD should send a request to the CIO with cost justification for New procurement.

8. Quarterly Rate Contracts will be signed by the CIO and Procurement Head in Advance for every quarter.

S.No.	Grade / Designation	Grade wise Eligibility for Laptop/Desktop	Application
1	PRESIDENT / VICE PRESIDENT / ASSOCIATE VICE PRESIDENT / CHIEF INFORMATION OFFICER / CHIEF FINANCIAL OFFICER.	**Laptop** - 12th+ Gen i7 (14" touchscreen display/16GB RAM/500 GB SSD)	Windows OS Additional M Presentation
2	SR.GM / DY.GM / GM / PLANT HEAD / HEAD / SR PM / DY.PM / PM / PROJECT HEAD / AGM.	**Laptop** - 12th+ Gen i5 (14"/16GB RAM/500 GB SSD) Windows 11+MS-Office	Windows OS
3	DY MANAGER / MANAGER / ASSISTANT MANAGER / SR CONSTRUCTION MANAGER / CONSTRUCTION MANAGER / ASST CONSTRUCTION MANAGER / ASST ENGINEER / ASST FUEL INCHARGE / ASST MATERIAL ENGINEER / ASST MATERIAL ENGINEER (PQC) / ASST QUANTITY SURVEYOR / ASST SURVEYOR / ASST SURVEYOR DRAUGHTSMAN (CAD) / SR GEOLOGIST / SR SURVEYOR / SR SYSTEM ENGINEER / SR SYSTEM EXECUTIVE / SR ACCOUNTANT.	**Laptop** - 12th Gen i3 (14-15"/16GB RAM/500 GB SSD) **For special cases** : like CAD, MINEX, high configuration software, high usage of financial calculations & reports, etc HOD to send justification for requirement to CIO for i5 Laptop or Higher Configuration.	Windows+G (For recruitn 1. Users Sho with HOD Ap Head.

4	SR EXECUTIVE / SR ENGINEER / SR ACCOUNTANT / SR DOCUMENTS CONTROLLER / SR DRAUGHTSMAN (CAD) / SR ELECTRICIAN / SR FOREMAN / SR LAB TECHNICIAN / SR QC ENGINEER / SR QUANTITY SURVEYOR / SR SUPERVISOR / SR SYSTEM ENGINEER / SR SYSTEM EXECUTIVE / MATERIAL ENGINEER / MANAGEMENT TRAINEE / LAB CHEMIST / JR GEOLOGIST / JR ENGINEER / GRADUATE ENGINEER TRAINEE (GET) / GEOLOGIST / ASSISTANT / EXECUTIVE / PURCHASE ASSISTANT / QC ENGINEER / SECTION INCHARGE / SECURITY INCHARGE / SHIFT INCHARGE / ESS COORDINATOR / DEO / FUEL INCHARGE / TRAINEE.	**Desktop** - 12th Gen i5 (16GB RAM/500 GB SSD)Windows+Google Sheets (8 GB Extra for Design tool users) **For special cases :** like CAD, MINEX, high configuration software, high usage of financial calculations & reports, etc HOD to send justification for requirement to CIO for Additional configuration in Desktop or Laptop.	Windows+G (For recruitn 1. Users Sho with HOD Ap Head.
5	Special Requirements Like Apple Mac Book / Microsoft Surface	For Special users / Special Clients	With all star

Note: Laptop / Desktop Minimum Life will be 3-5 Years , This will not be replaced with New one unless and until if there is any se Technical Issue in the system

>Asset allocation will be done as per the store stock availability FIFO Method

>HR Department will provide advance recruit plan to IT department - IT department should ensure sufficient inventory in Store as per the recruitment plan

> 5 Desktops , 5 Laptops of i5, 5 Laptops of i3, 2 i7 Laptops should be there in store stock for New Projects systems requirement wil case for every project

> USB access will not be provided to any User (Exception will be with MD sir for Limited time case to case MD sir

A. Objective

The objective of this Change Management Policy is to control the lifecycle of all changes in the DBL, enabling beneficial changes to be made with minimum disruption to IT services/process functions.

B. Scope

This Policy is applicable to all DBL computing resources such as applications, production servers, network infrastructure appliances, and communication equipment where DBL manages changes. Changes to both logical and physical assets shall be considered and documented.

C. Policy

Changes to Information Assets (including applications, servers, network devices, changes to application code and physical infrastructure) shall be performed in a controlled manner to ensure that the risks associated with such changes are managed to an acceptable level. Critical changes shall be tested in a non-production environment before deployment and ineffective changes shall be rolled back.

1. Baseline configuration management of systems

System administrators shall capture the system baseline configuration before the system is moved into production. The System baseline configuration document shall capture detailed information about the systems including:

1.1 Hardware Configuration of the systems
- CPU
- Memory
- Disk

1.2 Operating system and networking details
- OS Versions/Release updates
- Host Name

1.3 Operating System Accounts
- IP Address and related network parameters

1.4 Security hardening settings
- Patches
- Services
- Permissions
- Security Settings and Program libraries

1.5 List of Software applications installed and upgrade of Software Configuration Parameter of each of the applications.

1.6 Any changes in the baseline document shall be accompanied by change in the version of the document. All changes made to the system shall be traceable in the baseline document. All configuration files that contain parameters defined by the baseline configuration document shall be identified and a backup of these files shall be done before and after every change. In cases where the values are not defined in configuration files, scripts shall be used to capture these values so that the configuration parameters can be traced.

2. Change request and approval (Change Records)

All the details of the change, documenting the lifecycle of a single change, are documented in a record, which can be created by any individual who identifies a need for a change to the IT infrastructure/applications/network ("**Change Record**").

2.1 Timing

Lead Times:

A lead time is referred to the window between the Change Record initiated time and the proposed implementation time.

Emergency Change:
An emergency Change Record must be created in less than 24 hours of its implementation time.
Normal Change:
A normal Change Record must be created 3 days before its implementations.
Expedite Change:
An expedite Change Record must be created in less than 3 days of its implementation time.
Latent Change:
A latent Change Record must be created in less than 24 hours post the implementation of change.

Activity commence post Approvals

Backup and Restoration Policy:
- Backup performed daily & verification quarterly

Change Management Policy:
- New Business Process
- New Reports
- Change in the existing report
- Change in the existing review process
- Software Version Upgrade

Patch Management Policy:
- Implemented under AD/Other Automated Software Solution(s)
- SAP Patch Management (SUM) – Activity conducted on Quarterly basis.

with IT SLA(TAT) as below
High Priority: 4 Business Hours
Medium Priority: 8 Business Hours
Low Priority: 24 Business Hours

2. 2. Handling Changes

a. **Change record creation:**
A Change Record can be created by any individual who identifies a need for a change to the IT infrastructure/applications/network. The Change Record contains all the details of the change, documenting the lifecycle of a single change.
b. **Change Record Approval:**
Once the change record is created, it should be approved by Department head/Business Approver: An individual who validates the change before and after the change implementation from the technical standpoint.
c. **Change Advisory Board ("CAB"):**
A group of individuals who validate the change from all possible and potential impact to provide a sign off.
d. **Information Security/Change Record Manager**:
ISM will facilitate the CAB in managing the CR and will assign the change record to the implementer for execution.
e. **Change Record Implementation:**
Once the change is approved it is ready to be installed. Before the implementation, a detailed communication would be sent out to all the teams who are involved with the change or getting affected by it.
f. **Change Record Review:**
After the change gets implemented, it needs to be reviewed by the department head to check the success criteria. If the change is not successful, then it would be either backed out or fight forward and then it needs to be closed with proper comments.
g. **Change Record Closure:**
Once the change is successfully implemented, the implementer will attach the evidence of success of the change and close it.

3. Change Advisory Board

a) The CAB shall consist of IT committee leads.
b) CAB meeting will be held monthly, and as and when there is a need for change.
c) ISM will present the changes scheduled in the CAB meetings.
d) Any change request that is presented into the CAB should have Department head/business approval from the relevant person who will validate the change request post implementation.
e) The CAB has the authority to approve or reject any change based on risk and impact.
f) Once the CAB has approved the change request, ISM will assign the change request to the implementer.

4. Change Management Process:

4.1 Change Record Creation:

An implementer/ requester identifies the need for a change and create a change record.

4.2 Change Record Assignment Process:

The change record is assigned to the Department head/ business approval sign-off is gained. If the Department head/business approval identifies the change to be not fit for implementation, it is either rejected or cancelled.

a. If the Change Record is rejected, then it is assigned to the implementer for further modifications.
b. If the Change Record is cancelled, then the change request is closed.
c. If the Department Head provides a sign off, the change request is then assigned to ISM for further validation.
d. ISM team will analyse the change request with the information provided in its ex. Implementation steps roll back plan, lead time.

4.3 Change Record Categorization by ISM:

1) ISM will also identify if the CR is a Change, Emergency, Expedite or Latent type of change.
2) If it is a Standard Change, then ISM will approve the change directly and the change is implemented.
3) If it is any other type of Change, then it is subjected to an approval from CAB.
4) ISM also has the authority to reject/cancel the change depending upon the information provided in the Change record, lead time, implementation plan or the roll back plan.

4.4 Change Record Approval by CAB:

a) Once ISM identifies that the change is not a standard one, it is presented in the CAB.
b) CAB analyses the change for all perspective and approves/rejects the change.
c) If the change is rejected by CAB, it is assigned to implementer for necessary modifications.
d) Once CAB approves the change, ISM will provide a final sign off and assign the Change Record to the implementer for its execution.

4.5 Change Record Review:

Once the change is implemented, the Department Head validates the change for its success.

4.6 Closing a Change Record:

a) If the change is a success, then the Change Record is closed, attaching the evidence of the success of the change.
b) If the change is not a success, then the rollback/fight forward mechanism is used.
c) Any changes performed on production systems including servers, clients, network devices, applications and physical infrastructure shall go through change management reviews and approval.

d) Changes shall be reviewed and approved by the CAB before their implementation.
e) Any modification to the system other than regular administrative activities shall go through the change management process. These changes may include:

- Applications installation, modification, and upgrade
- Operating system installation and/or upgrade patch management
- Changes to parameters in configuration files of applications, systems, or other devices
- Hardware and/or firmware additions, deletions, reconfigurations, software changes by the vendor
- Changes to electrical installations, such as UPS, stabilizers, etc., that may impact data processing services.
- Changes to applications including new releases, bug fixes, parameter changes and maintenance activities.

f) All changes that have an impact on the functionality and security level of the application shall require approval from the CAB. Application owners should identify and document the changes that need to go through the change management process for their applications.

g) The system administrators/application owners shall raise a request for change. The request shall be validated by the Head of respective department before the change is forwarded to the CAB for approval. The change request shall contain the following details.

1. Change objective: There shall be a clear justification for change. This could include new business requirements, product feature enhancements changes or additions to infrastructure and problem rectification.
2. Background of change: The circumstances or context in which the change is initiated or was required to be initiated shall be captured. These could include previously occurred incidents, bug identified and reported by the users.
3. Description of the change: The details regarding the changes including configuration changes, installation of additional components and system restart requirements shall be documented.
4. Change Impact: The (possible) impact of the change on other systems shall be captured here including processes, application, servers, operating systems, database, and networking. For example, a new program that may influence performance of any other associated program or function such as End of the Day (EOD) reports generation.
5. Change Priority: The urgency and importance of the change shall be used to decide the change priority. Priority can be one of the following:
   - Normal: The request will be reviewed during scheduled CAB meetings.
   - High: CAB will review the change request on a priority basis.
   - Low: The request will be reviewed during scheduled CAB meetings. The changes with 'Low' will be reviewed but CAB may choose to hold the change so that multiple changes can be clubbed together.
6. Emergency: Such changes can be performed without going through the CAB review after obtaining approval from the Department Head. The documentation and post-implementation review and approval of the change should happen within one working day. Emergency changes are not encouraged and should be performed only when the application functionality or security is severely impeded and can lead to downtime or other issues.
7. Change Executed by: The personnel who is expected to perform the change (Change requester).
8. Roll Back /Fall Back Plan: The proposed method for reverting the change or taking a different option in case of a failure.
9. Approval from the Change Advisory Board and IT head is must before performing testing and change implementation.
10. List of documents attached: Additional supporting documents shall be attached where applicable. These may include the previous Request for Change applications/ approvals, Business Analysis Document, and other such documents.

11. Rollback strategy should be in place before changes are implemented. An audit log is maintained of all updates to operational program libraries.
12. CAB shall take a decision on proceeding with the change request based on the following.

    - Need for change: The objective of change shall be evaluated to see if it is in line with business requirements.
    - Impact of change: The impact of the change on the overall system and network shall be considered. For example, a change in the router access control list might impact another application. CAB shall ensure that all users and departments affected by the change are informed about the same.
    - Priority of change: The criticality of the change shall be evaluated. The priority will determine if the change needs to be done immediately or can be implemented later.
    - Security implication: CAB shall consider the security implication of the change. If the change affects the existing security level, necessary steps shall be taken to ensure that all risks associated with the change are mitigated. Security related inputs will be provided by the Information Security Team. The team responsible for implementing the change shall develop a detailed implementation plan that includes the following details.
    - Time and resource requirements: The time and resource (in terms of people or additional software/hardware) requirements for implementing the change shall be documented.
    - Pre-requisites: If there are pre-requisites including taking a full backup that need to be met before the change can be done, these shall be documented.
    - Downtime requirements: If the change involves system downtime, then it shall be scheduled during non-business hours. Arrangements shall be made for availability of system personnel and specific users needed to implement and verify the change.
    - Implementation steps: The steps that need to be executed to implement the change and the personnel responsible for executing the steps shall be documented in detail.
    - Test plan: The procedure for testing the change shall be documented. The team responsible for implementing the change needs to consult with end-users while creating the test plan.
    - Roll back plan: There shall be a documented roll back plan for restoring the system to original state. The time and resources required to implement the roll back plan also shall be documented.
    - Fallback procedures should define and implemented, including procedures and responsibilities for aborting, and recovering from unsuccessful changes and unforeseen events.
    - Application owner shall evaluate the implementation plan for completeness and operational feasibility before approval. The application owner shall inform the requestor and the implementation team about the decision.

4.7 Testing of the implementation plan

- The changes shall be initially tested on a non-production system as per the implementation plan. Testing shall be done to verify the changes.
- The rollback plan also shall be tested on the test system.
- Changes shall be made to the implementation plan (if required), based on the results of the testing.
- The team responsible for implementation shall update the application owner on test results.
- If the change does not meet the desired objective, application owner shall not proceed with the change.

4.8 Implementation of Change

a) The team responsible for implementing the change shall follow the plan approved by the application owner.
b) The implementation team shall submit a post implementation report to the application owner. It shall include the following details.
    - Time and resources utilized.

- Implementation steps involved.
- Test results
- Justifications for deviation (if any) from plan
- Confirmation from the application owner that only the changes approved by the CAB have been implemented.

4.8.1 Review of Change

A. On completion of implementation, the effectiveness of change (including minor/emergency changes) shall be evaluated by the CAB. The following areas shall be considered:
B. Changes achieving the desired objective: CAB shall evaluate if the objectives defined in the original change request have been met. This can be done by taking feedback from system administrators and users.
C. Adherence to implementation plan: CAB shall evaluate if all the steps that were proposed in the implementation plan have been followed and if the time and effort estimates were appropriate.
D. If the changes do not meet the desired objective, CAB shall inform the implementation team to roll back the change.
E. Application owner is responsible for maintaining all documents related to change management for future reference and audit purposes.

4.9 Emergency Change

Emergency Change Advisory Board Meeting will take place to take decision and perform the change.

- Ensure emergency changes are processed by the appropriate personnel to enable the change to be dealt with in the timescales required.
- Ensure relevant parties are available to review emergency changes within the timescales.
- Provide a technical and business assessment, independent of the change initiator/assignee of emergency changes.
- Secure the approval of an emergency change.
- Ensure emergency changes are scheduled effectively and that change assignees are notified that they can commence work.
- Build the emergency change for implementation to production.
- Test that the emergency change is fit for purpose.
- Confirm that the emergency change meets all requirements prior to implementation in the production environment.
- Implement the emergency change within the production environment.
- Ensure that unsuccessful emergency changes are backed out and all affected components returned to the status that existed prior to the change.
- Ensure that a Change Record exists on the toolset for emergency changes.
- Review the success of the emergency change in resolving the Incident/Problem and to learn from any issues arising for future changes.

5.0 Change Communication and Notification

a. All changes that may affect system security and availability are communicated by the IT Team to DBL Management.
b. Any changes that may affect user entities' system security and availability should be informed through email.

1. Objective

The objective of this Communication and Operation Policy is threefold:

a) to ensure the correct and secure operation of information processing facilities of the DBL.
b) to implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements; and
c) to minimize the risk of DBL's IT System failing.
d) The objective of this policy is to ensure secure access and usage of DBL e-mail services by its users. Users have the responsibility to use this resource in an efficient, effective, lawful, and ethical manner. Use of the DBL e-mail service amounts to the user's employment agreement to be governed by this policy.

2. Scope

This document is applicable to all processes and operations in DBL within the scope of the ISMS.

This Policy is applicable to all the employees, representatives and suppliers of our organization including our Subcontractors and Affiliates

3. Policy

3.1 Operating Procedures

Operating procedures for all processes of DBL shall be developed, maintained, and published to enable the authorized Users, and network and system administrators to perform their daily operations.
Where applicable, the Policy and Procedures shall include and abide by applicable laws.

3.2 Operational Change Management

a. Changes to IT assets (including applications, servers, systems software, security architecture, and network devices) shall be performed in a controlled manner to ensure that the risks associated with such changes are managed to an acceptable level. This involves obtaining prior approval, performing impact analysis, testing, and maintaining up-to-date documentation for the entire process.
b. Changes shall be tested in a non-production environment before deployment and ineffective changes shall be rolled-back.
c. Appropriate procedures shall be put in place for all changes requiring emergency actions and response process, which bypass the Policies and Procedures outlined.

3.3 Segregation of Duties in Operational Procedures

a) All processes shall adopt the principle of segregation of duties to the maximum extent possible. The initiation of an event shall be separated from its authorization.
b) Where segregation of duties is not possible or practical, the process shall include compensating controls – such as monitoring of activities, maintenance and review of audit trails and management supervision.

3.4 Information Back-up (Ref: Backup Management Procedure)

a) As applicable, all application and operating systems software, hardware configuration information, software, and log files (logs from various systems that need to be backed up) essential to the continued operations of DBL shall be identified, documented, and periodically backed up.
b) Where applicable, the policy and Procedures shall include and abide by the applicable laws.
c) Frequency of backup, medium of backup and storage of the backup shall be identified and documented.
d) The security controls over the backup of information and media shall be commensurate with the classification of the information backed up, contractual obligations and other applicable guidelines.

Backup shall be retained in accordance with the requirements set out in the contractual obligations. Backup register shall be maintained by personnel who takes backup and shall be updated regularly.

e) In addition to the scheduled backups, backups shall be taken in case any of the events occur during the configuration changes.

3.5 Recovery Policy

- Backed up data shall be provided for restoration purposes after appropriate approval and authorization.
- A log of all restoration requests shall be maintained.

3.6 Restoration testing Policy

- To verify the readability of backup media, periodic mock restoration tests shall be carried out on the test systems.
- The entire restoration testing process shall be documented detailing the test plan, the activities carried out and the test results.
- Exceptions identified during the testing process shall be documented and reported.

3.7 Network security management (Ref: Network Security Procedure)

a) DBL's network shall be used for valid business purposes only. The protection of information contained on the DBL network is therefore the responsibility of the management and the activity and content of User information on the DBL network is within the scope of review by management. Where applicable, the Policy and Procedures shall include and abide by the applicable laws.

b) DBL shall develop and implement network security systems and procedures, and provide network security resources (Firewall, IDS, etc.) to protect all business data, related application systems and operating systems software from unauthorized or illegal access at a level that is appropriate for the information or computing resources.

3.8 Network access

a. All network and network services in DBL shall be identified and documented.

b. Access to the DBL network and network resources shall be on need-to-know basis and authorizations shall be obtained from appropriate authorities before providing access. All such Access shall comply with DBL's Access Control Policy. Network and network services required for every job function and role shall be identified and documented.

c. Connection capability of Users shall be restricted through access-control lists in firewalls and switches. Additional services more than what is required for the job function shall be allowed only after getting approval from appropriate personnel.

d. Administrators shall ensure that the host operating system is configured to validate each User prior to allowing network access.

e. Remote access shall be controlled and allowed only after approval by authorized personnel.

f. Physical and logical access to diagnostic and configuration ports shall be controlled. Network and network services access shall be periodically reviewed to ensure that unauthorized network services are not used, or authorized network services are not accessed by unauthorized personnel.

g. Networks shall be logically or physically divided based on the criticality of the information stored in the network. If the network is logically separated, appropriate perimeter security devices shall be put in place. If the network is physically separated, controls shall be in place to protect physical access to the network at all endpoints.

h. All network equipment's default passwords (e.g., routers) shall be changed by administrators during installation.

i. To maintain the privacy of the DBL information, DBL networks shall not be used for personal and/or private information unrelated to business activities. The DBL computers and resources shall be used for valid business purposes only.

j. The use of personal communications equipment (modems, ISDN cards, etc.) attached directly to personal computers with remote control software shall be prohibited.

k. Access to third parties shall be given after carefully analyzing needs and after assessing risks involved in providing such access.
l. Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control requirements of the business applications.

3.9 Internet Service Management

a) Access to the Internet shall be provided only to those employees who have a legitimate business need for such access.
b) There should be no internet access to systems present in the Network operation center.

3.10 Network security Management

a. All network equipment's communication lines shall be identified, documented, and updated regularly.
b. Network diagrams at all levels (WAN and LAN segments) shall be maintained and updated regularly.
c. Minimum Baseline Security Standards ("MBSS") shall be developed and maintained, and all network equipment's shall be configured as per MBSS.
d. All connection between DBL's network and any third-party network shall be established only after appropriate authorization from Information Security Coordinators.
e. Before establishing connection with any third-party network, a network security check of third-party network shall be performed. The security check shall include vulnerability assessment and penetration testing of the third-party networks. Past vulnerability assessment and penetration testing reports can be used as a reference while providing access. Further, any third-party network shall abide by DBL's Information Security Policies and Procedures to establish connection with DBL network.
f. No third-party user shall be allowed to connect to their home network via the DBL network. If such connection is deemed necessary case deemed necessary, explicit permission shall be obtained from the ISC.
g. Vulnerability Assessment – Performed annually Twice.
with IT SLA(TAT) as below
High Priority: 4 Business Hours
Medium Priority: 8 Business Hours
Low Priority: 24 Business Hours

3.11 Data Transmission

a) Any information from DBL's environment travelling over third-party networks or public networks shall be encrypted, wherever feasible. Appropriate encryption algorithms shall be used to maintain the integrity and confidentiality of the data.
b) Appropriate technology shall be used for encryption.
c) Confidential or restricted information transmitted over any communication network shall be sent in an encrypted form.
d) Software that performs unattended file transfer to or from other systems shall authenticate the username-password unless the information being transferred is classified as Public.

3.12 Network assessment

a. Network vulnerability assessments shall be performed on an ongoing basis by competent personnel. The risks identified shall be documented in the assessment report.
b. Assessment report shall be submitted to the Information Security Coordinators regularly.
c. Third-party independent network assessment shall be performed annually to provide assurance to the management, customers, and stakeholders.

3.13 Media Handling

3.13.1 Management of Removable Media

a) Removable media shall be blocked on all endpoint devices. Endpoint access to removable media will only be enabled only if there is a business reason for doing so and appropriate approvals are obtained. All such removable media shall be managed in accordance with DBL's Asset Management Policy.
b) All media shall be stored in a safe, secure environment according to the manufacturer's specifications.
c) If no longer required, the contents of any removable media shall be made unrecoverable before disposal, in accordance with DBL's Asset Management Policy.

3.14 Disposal of Media

a. Media shall be disposed securely and safely when no longer required, in accordance with DBL's Asset Management Policy.
b. Items that require secure disposal shall be identified.
c. Disposal of sensitive items shall be logged to maintain an audit trail.

3.15 Information handling procedures

a) Handling and labelling of media shall be according to its classification level.
b) Access restrictions shall be deployed to prevent access from unauthorized personnel.
c) The distribution lists and list of authorized personnel shall be periodically reviewed and updated.

3.16 Security of system documentation

- System documentation shall be stored securely and shall be protected from unauthorized access.
- The system or application owner shall authorize or approve distribution lists for system documentation. This list shall be restricted to a minimum number of parties.

3.17 Exchange of Information

a. To prevent loss, modification, destruction, or misuse of information, DBL shall protect and control exchange of critical business information assets and software with third parties and outside organization.
b. Where applicable and legally acceptable, electronic signatures can be used. The use of electronic signatures shall be governed by the applicable laws where the transaction is being conducted. Further, controls shall be deployed to protect the electronic signature from unauthorized use.

3.18 Information and Software Exchange Agreements

a) Formal agreements shall be established for the exchange of critical business information assets or software with outside organizations. The department requiring this exchange shall be responsible for the formal agreements.
b) These agreements shall include both physical and electronic exchanges.
c) These agreements shall reflect the sensitivity of the critical business information assets being exchanged and shall describe any protection requirements.
d) These agreements shall specify management responsibilities, notification requirements, packaging and transmission standards, courier identification, responsibilities and liabilities, data and software ownership, protection responsibilities and measures, and all encryption requirements.

3.19 Physical Media in Transit

Media containing information shall be protected against unauthorized access, misuse, or corruption during transportation beyond an organization's physical boundaries.

3.20 Internet usage code of conduct

a. Each User will be responsible for the activities carried out through his / her allotted machine.
b. Ability to connect to a specific web site does not in itself imply that users of DBL Internet facility are permitted to visit that site. Users using DBL internet facility will immediately disconnect on discovering that they are connected to a potentially offensive site.
c. Uploading and downloading files for private personal use is not permitted. When downloading and uploading authorized commercial software for business requirements, copyright regulations shall be strictly adhered to. By downloading files, viruses can infiltrate the local system. Installing downloaded software (browser-related add-ons or operating system-related functions) may create system instability that results in unnecessary repair and helpdesk costs. Software installing may be embedded in the download procedure.
d. For all Internet activities, where an employee expresses himself publicly, the e-mail policy for message submission applies
e. All Users will be adequately made aware about DBL policy on the Internet usage.

3.21 Business Information systems

Measures shall be taken to protect information associated with the interconnection of business information systems.

3.22 Publicly available information

a) Any information stored or generated in DBL that is to be made publicly available for public consumption shall be identified, verified, and approved by appropriate authorities before making it public.
b) Adequate controls shall be put in place to ensure that integrity of such information is protected.

3.23 Monitoring, Auditing and Logging

a. User activities, exceptions, and security events shall be logged and monitored in accordance with DBL's Logging and Monitoring Procedure. Logs shall include the following:
b. System starting and finishing times.
c. System errors or faults and corrective action taken.
d. Confirmation of the correct handling of data files and computer output
e. The name of the person making the log entry
f. The activities of Users with high levels of access (privileged Users such as system administrators and system operators) shall be logged and independently reviewed on a regular basis.
g. All access to critical applications and DBL network shall be monitored for suspicious activities or security breaches. Adequate response mechanisms shall be in place for containing security breaches.
h. The audit logs shall be retained based on the record retention requirements.
i. Logging facilities and log information shall be protected against tampering and unauthorized access.
j. The clocks of all relevant information processing systems within DBL or security domain shall be synchronized with an agreed accurate time source
.

3.24 Security of system documentation

a) System documentation shall be protected from unauthorized access. The teams shall have their individual access-controlled folders in the common work area.
b) The system or application owner shall authorize or approve distribution lists for system documentation. This list shall be restricted to a minimum number of parties.

3.25 Protection against malicious and mobile code (Ref: Anti-Malware policy)

a) All servers, desktops, workstations, hand-held devices, gateways, and any other access points to DBL network shall be protected against malicious code, in accordance with DBL's Anti-Malware Procedure. The most current available version of the anti-virus software package will be taken as the default standard. Automatic update features will be installed on all newly installed systems.
b) All computers attached to the DBL network shall have authorized standard, supported anti-virus software installed if on Windows platform. This software shall be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.
c) Anti-virus application and processes shall ensure early detection, efficient containment, and eradication of malicious code.
d) Adequate User awareness measures shall be implemented for the same.
e) Controls shall be considered to prevent unauthorized mobile code execution.

3.26 System planning and acceptance

a. **Capacity monitoring and planning (Ref: Capacity Management Procedure)**
b. DBL shall continuously monitor the utilization and make projections for future requirements of information processing resources and plan accordingly to ensure that adequate information processing resources are available to meet the business requirements of DBL. Where applicable, the policy and Procedures shall include and abide by the applicable laws.

3.27 System acceptance

Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system shall be carried out prior to acceptance. All requirements and criteria for acceptance of new systems shall be clearly identified, agreed, documented, and tested.

3.30 Email

Email is to be used for the company's business purpose only
E-mail is provided as a professional resource to assist users in fulfilling their official duties.
The company's confidential information must not be shared outside of the company, without authorization, at any time
Employees should not conduct personal business using the company computer or email
Sensitive content like source code, customer contacts, project documents, organizational strategy information and any other information of the company must not be sent to employee's personal email addresses
Personal email must not be used as contact address for official purposes
Official email must not be used for publishing, distributing or disseminating any inappropriate, profane, defamatory, infringing, obscene, indecent or unlawful material
Official email must not be used for surveys, contests, chain emails, junk e-mail, spamming, unsolicited messages or messages that have racial or sexual slur, political or religious solicitations
Official email must not be auto forwarded to any personal email or public email domains

3.31 Spam Filtering

Employees must not open emails from dubious sources
Employees must not reply to spam or click on links, including 'unsubscribe' facilities, in spam
Employees must not accept spam-advertised offers
Employees must block incoming mail from known spammers
Employees must not post official email addresses on publicly available sites or directories. If one must do so, look for options, such as tick boxes, that allow one to opt out of receiving further offers or information

Employees must not disclose personal information to any online organization unless they agree (in their terms and conditions or privacy policy) not to pass information on to other parties

3.32 Social Networking Sites

Employees shall not:

Store, send or distribute confidential information, copyright material or other content which is subject to third party intellectual property rights, unless you have a lawful right to do so.

Do anything, including store, send or distribute material which defames, harasses, threatens, abuses, menaces, offends, violates the privacy of or incites violence or hatred against any person or class of persons or which could give rise to civil or criminal proceedings.

3.33 Privacy

Users should ensure that e-mails are kept confidential. Users must ensure that information regarding their password or any other personal information is not shared with anyone.

3.34 Non-compliance and Consequence

Non-compliance of this policy, like misuse of office equipment for personal work or negligent damage or attending to personal work during office hours without the explicit permission of Manager or HR and any such acts that construe to be a violation of this policy, will be viewed seriously by HR and appropriate action will be initiated, including termination of employment contract.

A. Objective

The objective of this Compliance Policy is to manage compliance risk and oversee the implementation of appropriate controls and processes to ensure compliance issues are resolved effectively and expeditiously with the assistance of compliance staff.

B. Scope

This document is applicable to all processes and operations in DBL

C. Policy

1. Identification of applicable legislation

a. All relevant statutory, regulatory, and contractual requirements, pertaining to the operations, shall be defined explicitly, and documented for each of DBL information systems. Where applicable, the policy and procedures shall include and abide by the applicable laws.
b. This shall include, but not be limited to the IT Act 2000 (Information Technology Act 2000), Companies Act, Labor Act any other laws, or acts applicable to the organization.

2. Intellectual Property Rights

The terms and conditions and license requirements of the copyrighted software or any other proprietary information used within DBL shall be complied with.

3. Protection of Organizational Records

DBL's important records relating to information security shall be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

4. Data protection and privacy of personal information

Data protection and privacy shall be ensured as required by relevant applicable legislation, regulations, and, if applicable, contractual clauses for each business.

5. Prevention of misuse of information processing facilities

Information processing facilities shall be used as per policies detailed in this document and related DBL policy documents. Disciplinary action shall be taken for any violation of the policies.

6. Regulation of Cryptographic Controls

- Various countries have implemented agreements, laws, regulations or other instruments to control the access to or use of cryptography. The import/export of computer hardware and software for performing cryptographic functions, or which is designed to have cryptographic functions added to it, may be regulated. Some governments impose mandatory or discretionary methods of access to encrypted information (backdoors or key escrow).
- Advice from Legal Department must be sought to ensure compliance with applicable national laws, especially if encrypted information or cryptographic systems are moved between countries.

6. Compliance with security policies, standards, and technical compliance

Heads of Departments and Cyber security team shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

7. Independent technical compliance review and reporting

a) Information processing resources and associated documentation shall be reviewed immediately after installation of such resource and thereafter on an annual basis to verify that they are compliant with the security policies and standards. Findings and recommendations in the report shall be communicated to the concerned department personnel for implementation.
b) DBL's information processing resources shall be reviewed for compliance with DBL policies and applicable laws by an independent third-party at least on an annual basis. The findings shall be reported to senior management.

8. Information Systems Audit Considerations

a. DBL shall retain a competent independent party to conduct periodic audits of DBL's by to ensure compliance with the information security policies, procedures, standards, and guidelines. Formal written procedures shall be developed for planning and reporting audits and audit findings and ensuring the implementation of a prompt and accurate remedial action.
b. Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.
c. Access to IT Systems audit tools shall be protected to prevent any misuse or compromise.

1. Objective

The objective of this Configuration Management Policy is to ensure that Information Technology (IT) resources are inventoried and configured in compliance with DBL's IT security policies, standards, and procedures.

2. Scope

This Policy is applicable to all departments and users of IT resources and assets, and to applies to DBL' Information Assets and all DBL electronic information.

3. Policy

1. Baseline Configuration

The IT Department shall:

a. Develop, document, and maintain under configuration control, a current baseline configuration of Information Assets.
b. Review and update the baseline configuration of the Information Assets periodically.
c. Securely retain one previous version of baseline configurations of Information Assets to support rollback.

2. Configuration Change Control

The IT Department shall:

a) Determine the types of changes to the IT System that are configuration controlled.
b) Review proposed configuration-controlled changes to the IT System and approve or disapprove such changes with explicit consideration for security impact analyses.
c) Document configuration change decisions associated with the IT System.
d) Implement approved configuration-controlled changes to the IT System.
e) Retain records of configuration-controlled changes to the IT System for at least six months.
f) Audit and review activities associated with configuration-controlled changes to the IT System.
g) Test, validate, and document changes to the information system before implementing the changes on the operational system.
h) It is recommended Change Control for any device/application configuration is done in Sandbox environment and tested to ensure no impact and then rolled to production.

3. Security Impact Analysis

The IT Department shall analyse changes to the information system to determine potential security impacts prior to change implementation and create an Impact Analysis Document

4. Access Restrictions for Change

The IT Department shall define, document, approve, and enforce physical and logical access restrictions associated with changes to the IT System.

5. Configuration Settings

The IT Department shall:

a) Establish and document configuration settings for information technology products employed within the IT System using DBL- defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements.
b) Implement the configuration settings.
c) Identify, document, and approve any deviations from established configuration settings for DBL-defined IT System components based on DBL-defines operational requirements.

d) Monitor and control changes to the configuration settings in accordance with policies and procedures.

6. Least Functionality

The IT Department shall:

a. Configure the IT System to provide only essential capabilities.
b. Review the IT System quarterly to identify unnecessary and/or non-secure functions, ports, protocols, and services and disable them promptly if they are found to be unnecessary and/or non-secure.
c. Prevent program execution in accordance with policies regarding software program usage and restrictions and rules authorizing the terms and conditions of software program usage.
d. Identify software programs not authorized to execute on Information Assets and remove and/or disable as appropriate.

e. Employ a whitelisting methodology (permit-by-exception does not allow any software to run except if on an authorized software list) to prohibit the execution of unauthorized software programs on the IT system.
f. Review and update the authorized software list annually.
g. It is recommended to setup centralized Log analyzer integrated with network firewall and servers like SolarWinds/FMC for easy extraction of the logs.

7. Information System Component Inventory

The IT Department shall:

a) Develop and document an inventory of IT System components that:
   - Reflects the current IT System accurately.
   - Includes all components within the authorization boundary of the IT System.
   - Is at the level of granularity deemed necessary for tracking and reporting.
   - Includes information deemed necessary to achieve effective IT System component accountability.

b) Review and update the IT System component inventory every six months.
c) Update the inventory of IT System components as an integral part of component installations, removals, and IT System updates.
d) Employ automated mechanisms quarterly to detect the presence of unauthorized hardware, software, and firmware components within the IT System.
e) Take the following actions when unauthorized components are detected:
   - Disable network access by such components, or
   - Isolate the components and notifies the Chief Information Officer and system owner.
f) Verify that all components within the authorization boundary of the IT System are not duplicated in other IT System component inventories.

8. Configuration Management Plan

IT shall develop, document, and implement a configuration management plan for the IT System that:

a) Addresses roles, responsibilities, and configuration management processes and procedures.
b) Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items.
c) Defines the configuration items for the IT System and places the configuration items under configuration management.
d) Protects the configuration management plan from unauthorized disclosure and modification.

9. Software Usage Restrictions

The IT Department shall:

a. Use software and associated documentation in accordance with contract agreements and copyright laws.

b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution.
c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

10. User-Installed Software

The IT Department shall:

a) Establish policies governing the installation of software by users.
b) Enforce software installation policies through controlling privileged access and blocking the execution of files using a policy applied by directory service and/or application whitelisting.
c) Monitor policy compliance periodically.

11. Configuration Management Hardware and Software Changes

Capturing Hardware and Software Changes: To evidence configuration management within in IT ecosystem, a comprehensive approach is followed to capture hardware and software changes:

- Baseline Establishment: A stable baseline of configurations is created and maintained for all hardware and software components. This initial snapshot serves as a reference point for detecting any unauthorized changes.
- Change Identification: Changes are systematically identified through regular audits, automated monitoring tools, and real-time alert systems. Deviations from the established baseline are promptly flagged.
- Change Documentation: All changes, whether they involve hardware modifications or software updates or location changes, are meticulously documented. This includes details such as the nature of the change, the rationale behind it, the personnel responsible, and the timeline. Details w.r.t software or hardware changes are captured in the asset register providing details such as previous version number, new version number, date of change, remarks providing reason of change.
- Version Control: For software changes, version control systems are utilized. This ensures that changes are traceable and reversible if required.
- Process for Integrating Change Management with Configuration Management: While change management traditionally focuses on controlling the process of change implementation, it can be seamlessly integrated into the configuration management framework:
- Change Request Documentation: Change requests are generated through an established process. These requests are then logged and linked to the configuration management system. This integration ensures that all changes are systematically tracked, evaluated, and documented.
- Change Approval: Before any change is implemented, it goes through the requisite approval processes. These approvals are logged and linked to the associated configuration items.
- Change Implementation: Upon approval, changes are implemented in alignment with the established configuration management practices. All changes are verified against the baseline and documented for future reference.

1. Objective

The objective of this Continuity Management Policy is to form a continuity management framework and to be used as a source of reference by DBL to continue critical functions and maintain availability of vital information and Information Assets in an event of a significant disruption.

2. Scope

This includes information assets processed, transmitted, or stored by third-party service providers.
The Continuity Management Policy will address following aspects of information technology service continuity management ("ITSCM"):

- Conducting business impact analysis and risk analysis exercises.
- Establishing recovery requirements.
- Developing IT service continuity strategies and plans.
- Testing developed IT service continuity plans and implemented mechanisms.
- Conducting regular reviews on the IT service continuity plan / BCP

3. Policy

DBL shall adhere to the policies, processes, and procedures defined in the DBL's IT Governance Framework for ensuring ITSCM activities are planned, managed, and aligned with the organization's goals and objectives, as per the compliance and waiver criteria defined in the policy which shall enable DBL to achieve the continuity of Critical Processes and maintain availability of information at a level acceptable to the enterprise in the event of a significant disruption.

1. Define the Service Continuity Objectives and Scope

a) The IT Leadership Committee shall define service continuity objectives and scope.
b) IT service continuity shall be managed through a process. The Business Continuity Manager shall define the process which covers at a minimum the following:
    - Impact analysis.
    - Risk analysis.
    - Formulation and documentation of a business continuity strategy consistent with DBL's business objectives and priorities.
    - Documentation and implementation of testing times BCP.
    - Update the BCP to reflect changes in operational environment.

2. Develop and Maintain a Continuity Response

a. The Business Continuity Manager shall perform a Business Impact Assessment ("BIA") exercise annually to ensure that any changes in the DBL's operations are considered and adequately addressed in the BCP.
b. The BIA shall identify, quantify, and prioritize risks against criteria and objectives relevant to the organization, including critical resources, impacts of disruptions, allowable outage times, and recovery priorities.
c. The BCP shall be developed and implemented to maintain the continuity and recovery of the DBL's critical business operations at the required level and within the required time scales.
d. The BCP shall, at a minimum, address the following topics:
    - The conditions and criteria for plan activation.
    - Emergency and fallback procedures.
    - The role and responsibilities of designated individuals.
    - The critical assets and resources needed to be able to perform the emergency, fallback, and resumption procedures.
    - Conditions and criteria for Plan de-activation, and a return to normal operations.
    - Post-incident debriefs, and review of BCP response and lessons learned.
e. BCP's corrective measures shall be implemented.

3. Test, Review and Maintain the Service Continuity Arrangement

a) ITSMC Plan shall be tested and updated annually to ensure that they are up-to-date and effective.
b) The ITSMC Manager shall establish suitable mechanisms to monitor, measure, and maintain the effectiveness of the BCP and processes.
c) The ITSMC Manager shall ensure that the shortcomings of the BCP identified in testing and actual incidents are identified and post-incident meetings discussing opportunities for improvement are conducted. The ITSMC Manager shall make recommendations for improvement.

4. Conduct Continuity Plan Training

Business Continuity Manager shall ensure that relevant staff shall receive regular training arranged and planned regarding the procedures to be followed in the event of a disaster.

5. Manage Backup Arrangements

a) Create Backup Policy based on Business Criticality
b) Create backup SLAs (Full / Daily incremental / retention etc.)
c) Its recommended to setup Automated Backup Solution with encryption and compression so that Data backup is success complete and restoration of backup as per defined SLAs
d) The Business Continuity Manager shall ensure the off-site storage of critical backup media, documentation, and other IT resources necessary for the BCP and Business Continuity Plan.
e) The Business Continuity Manager shall identify the data to be backed up through discussion with business process owners and determine the frequency of such backups.
f) Mock restoration tests shall be carried out annually to verify the readability of backup media. The entire process shall be documented detailing the test plan, the activities carried out, and the test results.

1. Objective

The Objective of this Data Privacy Policy defines requirements to help ensure compliance with laws and regulations applicable to DBL collection, storage, use, transmission, disclosure to third parties and retention of Personal and sensitive personal data.

2. Scope

This Policy applies to all processing of personal data either in electronic form or where it is held in manual files that are structured in a way that allows ready access to information about individuals. Wherever the context requires in this Policy, personal data shall be interpreted to also include sensitive personal data. This policy has been designed to establish a worldwide baseline standard for the processing and protection of personal data by all DBL entities.

3. Policy

1. Management

a) A Data Privacy Policy shall be developed and maintained to document the privacy principles and practices followed by DBL. Data Privacy Document should cover complete Data Life Cycle Stages for each business Application (Data collection, process / store etc., archived, deleted etc.)
b) A privacy organization shall be defined for governance of data privacy initiatives.
c) A Data Protection officer shall be appointed to process complaints and requests for information related to DBL privacy practices.
d) Establish procedures for the identification and classification of personal information.
e) The Privacy Policy statement shall be made available on the internal portal.
f) The Data Privacy Policy shall be communicated to the internal personnel.
g) Procedures shall be established for disciplinary and remedial action for violations of the Data Privacy Policy.
h) Changes or updates to the Data Privacy Policy shall be communicated to all internal personnel when the changes become effective.
i) Establish procedures for performing mandatory registration with regulatory bodies.
j) Risk Assessment is to be carried out on a periodic basis to ensure risks to personal information are identified and mitigated.
k) The potential impact on data privacy is assessed when new processes involving personal information are implemented, or when significant changes are made to such processes.
l) Its recommended to follow best practices of Data Privacy and PII regulations and identify the relevant controls applicable to DBL and implement them

2. Notice

a. Appropriate notice shall be provided to data subjects at the time personal information is collected.
b. The privacy notice or policies and other statements to which they are linked shall provide as full information as is reasonable in the circumstances to inform an individual how their personal information will be used so that the use is fair and lawful. The following information should be considered for inclusion in a notice:
c. Purposes for which personal information is collected, used, and disclosed.
d. Choices available to the individual regarding collection, use and disclosure of personal information, wherever applicable.
e. Period for which personal information shall be retained as per identified business purpose or as mandated by regulations, whichever is later.
f. That personal information shall only be collected for the identified purposes.
g. Methods employed for collection of personal information, including ‘cookies and other tracking techniques, and third-party agencies.

h. That an individual's personal information shall be disclosed to Third Parties only for identified lawful business purposes and with the consent of the individual, wherever possible.
i. That an individual's personal information may be transferred within the entities, globally as per requirement, for business purposes with adequate security measures required by law or as per guidance of provided by industry leading practices.
j. Consequences of withholding or withdrawing consent to the collection, use and disclosure of personal information for identified purposes.
k. Data subjects are responsible for providing DBL with accurate and complete personal information, and for contacting the entity if correction of such information is required.
l. Process for an individual to view and update their personal information records.
m. Process for an individual to register a complaint or grievance regarding privacy practices.
n. Contact information of person in charge of privacy practices and responsible for privacy concerns with address at DBL.
o. Process for an individual to withdraw consent for the collection, use and disclosure of their personal information for identified purposes; and
p. That implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires or allows otherwise.
q. Data subjects shall be provided a Privacy Notice in case any new purpose is identified for using or disclosing personal information before such information is used for purposes not previously identified.

3. Choice and Consent

a) Implicit or explicit consent shall be obtained from data subjects at the time of collection of personal information or as soon as practical thereafter.
b) Explicit consent shall be obtained from data subjects for the collection, use and disclosure of sensitive personal information, unless a law or regulation specifically requires or allows otherwise. A record is maintained of explicit consent obtained from data subjects.
c) Implicit consent shall be considered adequate for the collection, use and disclosure of personal information which does not qualify as sensitive personal information.
d) Consent shall be obtained from data subjects before their personal information is used for purposes not previously identified.
e) Appropriate consent shall be obtained from data subjects before their personal information is transferred to or from their information processing systems.

4. Collection of Personal Information

a. The collection of personal information shall be limited to the minimum requirement for lawful business purposes.
b. Methods of collecting personal information shall be reviewed by management to ensure that personal information is obtained:
c. Fairly, without intimidation or deception, and
d. Lawfully, adhering to laws and regulations relating to the collection of personal information.
e. Management shall confirm that Third Parties from whom personal information is collected:
f. Use fair and lawful information collection methods, and
g. Comply with the Data Privacy Policy and their contractual obligations with respect to the collection, use and transfer of personal information.
h. Data subjects shall be notified if additional information is developed or acquired about them.

5. Limiting Use, Disclosure and Retention

a) Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.
b) Personal information retention shall be only for the duration necessary to fulfil the identified lawful business purposes or as prescribed by law.

c) Guidelines and procedures shall be developed for the retention and disposal of personal information. These shall address minimum and maximum retention periods, and modes of storage.
d) Upon the expiration of identified lawful business purposes or withdrawal of consent, DBL shall either securely erase or anonymize the data subjects' personal information. Data is anonymized to prevent unique identification of an individual.

6. Access for Review and Update

a. Processes shall be established for data subjects to:
b. Request access to their personal data or information as prescribed by law.
c. Correct or update their personal data or information; and
d. Withdraw consent for the collection, use and disclosure of their personal information.
e. The identity of data subjects requesting access their personal information, or the identity of the data subjects authorized by the data subject to access the data subject's information, shall be verified before providing access to such information.
f. A response shall be given to data subjects requesting access to their personal information in an accessible form, within a defined period from receipt of complaint/ request as prescribed by law.
g. Data subjects shall be notified, in writing, of the reason for any denial of requests for access to personal information to the extent required by applicable law.

7. Disclosure to Third Parties and Outward Transfers

a) Personal information shall be disclosed to third parties only for identified lawful business purposes and after obtaining appropriate consent from the data subjects unless a law or regulation allows or requires otherwise.
b) Where possible, management shall ensure that third parties collecting, storing, or processing personal information have:
c) Signed agreements to protect personal information consistent with the Data Privacy Policy and information security practices or implemented measures as prescribed by law.
d) Signed non-disclosure agreements or confidentiality agreements which includes privacy clauses in the contract; and
e) Established procedures to meet the terms of their agreement with DBL to protect personal information.
f) Personal information may be transferred across geographies from where DBL operates for storage or processing where any of the following apply:
g) The individual has given consent to the transfer of information.
h) The transfer is necessary for the performance of a contract between the individual and DBL, or the implementation of pre-contractual measures taken in response to the individual's request.
i) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between DBL and a third party.
j) The transfer is necessary or legally required on important public interest grounds or for the establishment, exercise, or defence of legal claims.
k) The transfer is required by law.
l) The transfer is necessary to protect the vital interests of the individual.
m) The transfer is made under a data transfer agreement.
n) The transfer is otherwise legitimised by applicable law.
o) Remedial action shall be taken in response to misuse or unauthorized disclosure of personal information by a third party collecting, storing, or processing personal information on behalf of DBL.

8. Security Practices for Privacy

a. The information security policy and procedures shall be documented and implemented to ensure reasonable security for personal information collected, stored, used, transferred, and disposed by DBL.
b. Information asset labelling and handling guidelines shall include controls specific to the storage, retention, and transfer of personal information.

c. Management shall establish procedures that maintain the logical and physical security of personal information.
d. Management shall establish procedures that ensure protection of personal information against accidental disclosure due to natural disasters and environmental hazards.
e. Incident response protocols are established and maintained to deal with incidents concerning personal data or privacy practices.

9. Quality of Personal Information

- DBL may perform additional validation procedures to ensure that personal information collected is accurate and complete for the business purposes for which it is to be used.
- DBL shall ensure that personal information collected is relevant to the business purposes for which it is to be used.

10. Privacy Monitoring and Enforcement

a) Procedures shall be established for recording and responding to complaints/ grievances registered by data subjects.
b) Each complaint regarding privacy practices registered by data subjects shall be validated, responses documented and communicated to the individual.
c) Annual privacy compliance review shall be performed for identified business processes and their supporting applications.
d) A record shall be maintained of non-compliances identified in the annual privacy reviews. Corrective and disciplinary measures shall be initiated and tracked to closure, guided by DBL management.
e) Procedures shall be established to monitor the effectiveness of controls for personal information and for ensuring corrective actions, as required.
f) Any conflicts or disagreements relating to the requirements under this policy or associated privacy practices shall be referred to the Data Privacy Officer for resolution.

11. Retention of records

DBL has a statutory duty to keep certain records for a minimum period. In other cases, DBL shall not keep personal information for longer than is necessary or as may be required by applicable law.

12. Monitoring

a) Monitoring of the systems
b) DBL's IT and communications systems are intended to promote effective communication and working practices within our organisation.
c) Monitoring is only carried out if and to the extent permitted or as required by law and as necessary and justifiable for business purposes. The resulting log files may be used so that instances of attempted misuse and other security events can be detected, and that information is available to support any subsequent investigation. To the extent permitted by law and, where breaches of this and other policies or applicable law are found, action may be taken under the disciplinary procedure.
d) The employees are informed that the telephone system used by the Company allows identification of all dialled numbers and received calls.
e) DBL reserves the right to retrieve the contents of messages, check searches which have been made on the internet, require the immediate return of devices supplied by DBL and access data stored on such devices for the following purposes (this list is not exhaustive):
f) to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy (and employees acknowledge that the Company can use software to monitor the identity of senders and receivers of emails).
g) to find lost messages or to retrieve messages lost due to computer failure.
h) to assist in the investigation of wrongful acts; or
i) to comply with any legal obligation.
j) If evidence of misuse of DBL's IT systems is found, DBL may undertake a more detailed investigation in accordance with the disciplinary procedures, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any

witnesses or managers involved in the disciplinary procedure. If necessary, such information may be handed to the police in connection with a criminal investigation. Investigations and disclosure of information to the relevant authorities shall be carried out only to the extent permitted by law.

Appendix A: Privacy Principles

The Data Privacy Policy aligns with Generally Accepted Privacy Principles. In view of the changing legislative and technological environment for data privacy, the Data Privacy Policy will undergo revisions. The guiding privacy principles articulated in this policy document are as follows:

a. Management: Define, document, communicate, and assign accountability for Data Privacy policy and procedures
b. Notice: Provide notice about Data Privacy policy and procedures and identify the purposes for which personal information is collected, used, retained, and disclosed
c. Choice and Consent: Describe the choices available to the individual and obtain implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
d. Collection of personal information: Collect personal information only for the purposes identified in the notice.
e. Limiting Use, Disclosure and Retention: Limit the use, storage and retention of personal information is limited to the purposes identified in the data privacy notice and for which the individual has provided implicit or explicit consent. Retain personal information for only if necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately dispose of such information.
f. Access for review and update: Provide data subjects with access to their personal information for review and update.
g. Disclosure to third parties: Disclose personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
h. Security practices for privacy: Protect personal information against unauthorized access (both physical and logical)
i. Quality of personal information: Maintain accurate, complete, and relevant personal information for the purposes identified in the notice.
j. Monitoring and enforcement: Monitor compliance with Data Privacy policy and procedures and have procedures to address privacy related complaints and disputes.

1. Objective

The objective of this Human Resources Security Policy is to establish the processes by which DBL protects the Organization's sensitive human resources information from unauthorized access, loss, or inaccuracy. The Human Resources Security Policy specifies the information security requirements that need to be integrated into the Human Resources ("**HR**") processes.

2. Scope

This policy applies to all employees, external consultants, contractors, and third-party users (including housekeeping staff and security personnel) having access to DBL Information Assets and Assets that are hosted/located in DBL Centers.

3. Policy

1. Prior To Employment

1.1 Screening:

All prospective employees of DBL shall be subjected to pre-employment screening after prior notification or consent obtained from the prospective employee, as per the applicable laws and regulations. The screening process shall include the following background verification depending on the country of employment: address confirmation, previous employment validation, educational background checks, criminal check, Aadhar (or other applicable government identification) check, right to work verification, global database check and credit check.

1.2 Terms and conditions of employment:

The contractual agreements with employees shall clearly state:

- both their and the organization's responsibilities for information security.
- the requirement for the employee to sign a confidentiality agreement which will hold the employee liable for any unauthorized disclosure, theft, modification and/ or destruction of DBL's information.
- the employee's responsibility for maintaining the confidentiality and integrity of DBL's information and the actions that shall be taken against the employee if they disregard the requirements of the information security policy of DBL.

2. During Employment

2.1 Management Responsibilities:

Management shall ensure that importance of information security is communicated to all employees via training both at time of onboarding and annually thereafter. The cybersecurity team shall be responsible for the implementation of and compliance with information security controls by all employees. Management, along with the cybersecurity and Department Heads shall:

- ensure that the importance of information security and adherence to industry standard information security practices are communicated to all third parties having access to DBL's Information Assets and Assets associated with information processing facilities; and
- ensure that these third parties are obligated to communicate to their employees having access to DBL's Information Assets and Assets associated with information processing facilities the importance of information security and adherence to industry standard information security practices.

2.2 Information security awareness, education, and training:

Formal information security training shall be delivered to the employees at the time of their onboarding and on an annual basis thereafter. All employees shall receive appropriate training on organizational Policies and procedures, including security requirements, legal responsibilities, and other business controls as well as training in the acceptable use of information processing facilities e.g., login procedure, software privileges and likewise. Periodic assessments of the information security awareness shall be conducted, and training modules shall be updated on an annual basis and based on the feedback and recommendations received.

3.Disciplinary Process:

A formal disciplinary process shall be established for all employees who violate the information security policy and procedures. The disciplinary process shall provide the guidelines for actions to be taken in case of breach of the Information Security Policy and procedures or in case any employee is found to have committed any misconduct. All employees shall be made aware (via training / awareness sessions) of the disciplinary process should they violate the information security policy or commit / participate in any kind of security breach.

4. Termination and Change of Employment

4.1 Termination or change of employment responsibilities:

The HR function shall formalize and document a termination process including the return of all issued assets such as equipment, access cards and / or any other asset that is the property of DBL. The HR function shall also ensure that termination /change of employment responsibilities of the employees is clearly defined, assigned, and communicated to them. The Department Head of the departing employee shall ensure that, in case of any change in the responsibilities of the user, the access rights are promptly after termination or separation revoked or modified as required. If the account is required to remain active for any business reason, the Department Head of the departing employee shall obtain appropriate approvals from the CIO and ensure that passwords and other access credentials for such active accounts of a User are changed immediately on the departure of the User and ensure that the access rights of the User to information assets are revoked within twenty-four hours of separation of their employment, contract, or agreement.

1. Objective

The objective of this Information Classification Policy is to ensure the appropriate handling of all formats of information by establishing a DBL system of categorizing information in relation to its sensitivity and confidentiality, and to define rules for the handling of each category of information, to ensure the appropriate level of security of that information.

2. Scope

This policy covers all information held by and on behalf of DBL, whether digital or paper. The handling rules will apply to employees of the DBL including contractors, consultants and to third parties processing or handling DBL information where the organization holds information on behalf of clients with its own information classification, agreement will be reached as to which set of handling rules will apply.

3. Policy

Information should be protected throughout its lifecycle of generation, usage, access, modification, transmission, storage, and destruction. The degree of protection should be commensurate with the sensitivity, confidentiality, criticality, and regulatory needs of the formation. Information should be distributed in on a need-to-know and need-to-do basis. Information should be classified and labelled in a standardized manner across DBL.

1. Applicability

a) Information in all forms is covered by the requirements of the policy.
b) Information should be protected during the entire lifecycle from generation to disposal.
c) Information should be classified to indicate the need, priorities, and degree of protection and to
d) communicate the need for special handling measures to users.
e) An information owner is defined as the creator or caretaker of the information asset. The systems
f) owner will automatically have ownership for information stored in systems such as those in database.

2. Information classification framework

a) Information classification framework will define how information should be managed and protected.
b) according to its sensitivity and confidentiality requirements.
c) Information will be classified under one of the following categories:
d) Its recommended to classify digital content with a tool like Titus Data classification for automated data classification based on the content keywords etc. and monitor the data classification and its flow of information
    - Internal use
    - Public use
    - Confidential use
    - Highly Confidential

2.1 Public Information

a. The information that has been released by DBL for the public outside of DBL falls under this classification level.
b. Public Information has value, and its integrity needs to be maintained.
c. Disclosure of public information would not be a breach of confidentiality and it can be routinely made available to interested members of the public.
d. Public information should be protected from unauthorized modification.

2.2 Internal Information

a) Internal information is sensitive to external exposure. Any unauthorized disclosure to parties outside DBL would cause loss to DBL, embarrassment, difficulty, or legal issues. Internal information can be freely shared with all employees of DBL.
b) Internal information consists of information that should be public knowledge within DBL including email address books of employees, internal memos, and staff disciplinary matters.
c) Any information, which is not explicitly classified, should be treated as Internal and should be treated as such.
d) Internal information should be protected from unauthorized exposure to external parties. Specific authorization for Internal information is not required for DBL employees. Who may have access to the system or email? For example, internal memos should not be sent to "All" users of the email system by specially created groups for all employees.

2.3 Confidential Information

a. Information about the internal affairs of DBL, which are not required by all employees on the principle of 'need-to-know, need-to-do' basis, should be treated as confidential.
b. Information needed for the purpose of routine operations or conducting business by designated.
c. personnel fall under this category. For example, Customer information should be restricted to the appropriate personnel in the respective departments. Confidential information includes, but is not limited to, operational data, staff disciplinary matters, staff appraisal data, confidential reports of analysts and senior executives.
d. The authorized end users of the confidential type of information should be identified explicitly when such information is circulated within DBL. The end users can also be identified in terms of DBL-specified designations such as the Finance Officer, Information Security Forum, or other such groups' internal to DBL.
e. Recipients of confidential information should ensure that the information is made available to authorized personnel only. Recipients of this class of information should take measures to protect the information from accidental or malicious unauthorized access.
f. Information of this classification level and its holders should be protected and should be kept under lock and key and when contained in physical format. Information in soft format should be accessible only with logical access authorizations.

2.4 **Highly Confidential:**

a) Information would be classified as highly confidential, when the unauthorized disclosure, alteration, misuse, or destruction of that information would cause a significant level of damage to the business, stakeholder, business partners, employees, and customers.
b) This information, if not adequately protected, may result in non-compliance with applicable laws.
c) Access to this information requires approval from the owner of the information and shall be given on a need-to-know basis.
d) Examples of highly confidential data include login passwords, keys, Audit logs, PII, Bank account information, and Credit card info.

2.5 Classification of information

a. Information owner should classify their data based on the requirements defined in the previous sections. The Information Owner can only downgrade the classification level to a lower category.
b. The Information Owners will be responsible for periodically reviewing information classification to determine if current classification levels are valid. When the existing classification of information is modified, the data owner should:
    - Notify known recipient of data and/or information.

- Notify the next higher authority as deemed appropriate. Guidance on classification of information can be obtained from the Quality Assurance Department.

2.6 Labelling of Information with classification

a) Information and/or its holders where applicable should be labelled with the requisite classification level. The labelling should be performed in a manner that it is communicated and understandable to the recipients of the information.
b) Assets (Desktops and Laptops) should be classified and labelled as Internal and (Servers, Network devices) should be classified and labelled as restricted.
c) Documentation assets should be classified as Public, Internal and Confidential.

2.7 Authorized disclosure of classified information to external parties

Classified information should be disclosed to required external parties after proper authorization and only after the external party or the external party's organization has signed the Non-Disclosure Agreement in DBL approved format.

2.8 Determining Classification:

The goal of information security, as stated in the DBL Information Security Plan, is to protect the confidentiality, integrity and availability of information assets and systems. Data classification reflects the level of impact to DBL confidentiality, integrity, or availability of the data is compromised.

	Potential Impact		
Security objective	**Low**	**Medium**	**High**
Confidentiality- Preserving authorized restrictions on information access and disclosure, including means. For protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, Organizational assets, or individuals.
Integrity- Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity	The unauthorized modification or destruction of information could be expected to have a limited. adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, Organizational assets, or individuals.

	Potential Impact		
Security objective	**Low**	**Medium**	**High**
Availability- Ensuring timely And reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

2.9 Data Handling Requirements

For each classification, several data handling requirements are defined to appropriately safeguard the information. It is important to understand that overall sensitivity of institutional data encompasses not only its confidentiality but also the need for integrity and availability. The following table defines required safeguards for protecting data and data collections based on their classification. In addition to the following data security standards, any data covered by federal or state laws or regulations or contractual agreements must meet the security requirements defined by those laws, regulations, or contracts.

Security category control	**Data classification**		
Access controls	Tier 3-Public	Tier 2 -Internal	Tier1- Confidential/Restricted/ PII
	No restriction for viewing	Viewing and modification restricted to authorized. Individuals as needed for business-related roles	Viewing and modification are restricted to authorized. Individuals as needed for business-related roles
	Authorization by Data Owner or designee is required for modification; supervisor approval is also required if not a self-service function	Data Owner or designee grants permission for access, plus approval from a supervisor	Data Owner or designee grants permission for access, plus approval from supervisor
		Authentication and authorization required for access.	Data should only be printed when there is a legitimate need
	No restrictions	Data should only be printed when there is a legitimate need	Data should only be printed when there is a legitimate need
		Copies must be limited to individuals with a need to know.	Copies must be limited to individuals authorized to access the data and have signed a confidentiality agreement.

Copying/Printing (Applies to both paper and electronic forms)		Data should not be left unattended on a printer/fax	Data should not be left unattended on a printer/fax
		May be sent via Mail	Copies must be labeled “Confidential.”
			Must be sent via Confidential envelope; data must be marked “Confidential.”
	May reside on a public network	Protection with a network firewall required	Protection with a network firewall using "default deny" rule set required
	Protection with a firewall recommended	IDS/IPS protection required	IDS/IPS protection required
	IDS/IPS protection recommended	Protection with router ACLs optional	Protection with router ACLs optional
	Protection only with router ACLs acceptable	Servers hosting the data should not be visible to entire Internet	Servers hosting the data cannot be visible to the entire Internet, nor to unprotected subnets within LAN and guest wireless networks
Network security		Maybe in a shared network server subnet with a common firewall rule set for the set of servers	Must have a firewall rule set dedicated to the system
			The firewall rule set should be reviewed periodically.

System security	Must follow general best practices for system management and security	Must follow OS-specific best practices for system management and security	Must follow OS- specific best practices for system management and security
	Host-based software firewall recommends.	Host-based software firewall required	Host-based software firewall required
		Host-based software IDS/IPS recommended	Host-based software IDS/IPS recommended
	May be hosted in a virtual server environment	May be hosted in a virtual server environment	May be hosted in a virtual server environment
	All other security controls apply to both the host and guest	All other security controls apply to both the host and guest	All other security controls apply to both the host and the guest
Virtual Environments	The guest virtual machines	The guest virtual machines Should not share the same virtual host environment with guest virtual servers of other security classifications	virtual machines Cannot share the same virtual host environment with guest virtual servers of other security classifications

Physical Security	System must be locked or logged out when unattended	System must be locked or logged out when unattended	System must be locked or logged out when unattended
	Host-based software firewall recommended	Hosted in a secure location required; a Secure Data Centre is recommended	Hosted in a Secure Data Centre required
			Physical access must be monitored, logged, and limited to authorized individuals 24x7
The data		temporary access via secure protocols Over the Internet	
Data Storage	Storage on a secure server recommended	Storage on a secure server recommended	Storage on a secure server required

	Storage in a secure Data Centre recommended	Storage in a secure Data Centre recommended	Storage in Secure Data Centre required
		Should not store on an individual's workstation or a mobile device	Should not store on an individual workstation or mobile device (e.g., a laptop computer); if stored on a workstation or mobile device, must use whole-disk encryption
			Encryption on backup media Paper/hardcopy: do not leave unattended where others may see it; store in a secure location
Transmission	No restrictions	No requirements	Encryption required (for example, via SSL (Secure Sockets Link) or secure file transfer protocols)
Backup/Disaster Recovery	Backups required; daily backups recommended	Daily backups required Off- site storage recommended	Daily backups required Off-site storage in a secure location required
Media Sanitization and Disposal (hard drives, tapes, paper, etc.)	No restrictions	Recycle Reports. Wipe/erase media	Shred reports Destruction of electronic media

Training	General security awareness training recommended	General security awareness training required Data security training required	General security awareness training required Data security training required Applicable policy and regulation training required
Auditing	Not needed	Logins	Logins, access, and changes
Mobile Devices	Password protection recommended. locked when not in use	Password protected, locked when not in use	Password protected, locked when not in use, Encryption used

Un-classified Information:

Data that is generally available without specific asset owner approval, public data example policy document, Intranet Website / SharePoint site content. The following general guidance is followed with respect to classification:

- All customer data is classified as Company confidential.
- All data must be labelled to reflect their criticality (including their confidentiality, integrity, and availability)
- Data that has not yet been classified must be treated as confidential (e.g. newly created documents should be stored on secure network drives instead of on unsecured user laptops).
- All data must be classified within three (3) months of creation. Data owners or their documented delegates should set data classification levels.
- Following initial classification, data must remain classified at the initial level or reclassified as required by data owner (or his/her documented delegate) until destroyed as per policy.
- Classifications assigned to data must be reviewed at least once every three (3) years and reclassified based on changing usage, sensitivities, regulations, or legislations. (E.g. data currently classified as restricted may be elevated to confidential with the passing of new state or federal laws).
- Data must be protected in accordance with the security controls specified for the classification level that it is assigned.
- The classification level and associated protection of replicated data must remain consistent with the original data [e.g. (i) confidential HR data maintained in Azure Cloud, SharePoint, One Drive, retains its confidential classification; (ii) printed copies of confidential data is also confidential].
- Data, electronic or printed, must be protected according to policies, regulations, standards, and procedures.
- All confidential data, electronic or printed, and data containers (e.g. filing cabinets, servers, and magnetic or optical storage media) must be clearly labelled.
- Before systems or media are reused, they should be erased according to standard to ensure no residual data remains on the systems.

1. Objective

The objective of this Information Security Incident Management Policy is to provide a framework within which information security events and weaknesses associated with DBL information systems are communicated in a timely manner and necessary corrective actions are taken.

2. Scope

This Policy applies to all Users, and anyone else having access to DBL's premises, assets and information assets including corporate data, as well as the application and systems software.

3. Policy

DBL shall establish methods for handling and managing Incidents. DBL shall put in place Security Incident Response Team ("**SIRT**") comprising members from IT and Administration departments who shall manage problems and support requirements of Users, support users in case of Incidents and manage them without disruption to DBL's business.

1.Management of Information Security Incidents and Improvements

1.1Responsibilities and Procedures

a) This Information Security Incident Management Procedure for DBL defines procedures and responsibilities to ensure quick, effective, consistent, and orderly response to Information Security Incidents. A procedure for reporting major intrusions, attacks and frauds shall be defined.
b) The Information Security Manager shall be appointed for:
c) Investigation/co-ordination of reported Information Security Incidents and Security weaknesses.
d) Tracking closure of identified corrective and preventive actions; and
e) Interfacing with the DBL SIRT and provide /receive necessary feeds to and from SIRT as and when required.

1.2 Reporting Information Security Events

a. Information Security events shall be reported through appropriate management channels as quickly as possible.
b. Different channels as email, phone line, and intranet shall be implemented to facilitate reporting of an Information Security event. All Information Security events shall be recorded in an Information Security incident database.
c. The details of the steps to be followed for reporting an incident shall be communicated to all employees and third-party contractors of the Company. (**Refer**: Information Security Incident Management Procedure)
d. Incident reporting and management procedure shall be made available for easy access and reference for the purpose of reporting of security incidents and weaknesses by the users; and
e. Facility for monitoring (like Security Operations Centre) shall be set up for proactive monitoring of intrusions, attacks, and frauds.

1.3 Reporting information security weakness

a) Users of DBL information processing facilities and services are required to note and report any suspected information security weakness.
b) Users shall be made aware of their responsibilities in the event of a suspected security weakness such as users shall not attempt to prove (or test) a security weakness identified. Such action on part of Users will be interpreted as a potential misuse of information systems and users found doing so may be liable to disciplinary action.
c) Information security weaknesses, both actual and suspected, shall be reported through different channels like email, phone line, and intranet.
d) Incident reporting and management procedure shall be made available for easy access and reference for the purpose of reporting security incidents and weaknesses by the users; and

e) Centralized database shall be maintained of all reported Information Security weaknesses.

1.4 Assessment of and decision on information security events

a. Information security events shall be assessed, and it shall be decided if they are to be classified as information security Incidents.
b. If required, the DBL Information Security Team ("**IST**") shall have the necessary rights to determine the classification or re-assess the event and access the systems and applications for forensic purposes.
c. Assessment and decision results shall be recorded for future reference and to avoid false positives; and all such incidents shall be classified as per the classification criteria mentioned in the Incident Management Procedure

1.5 Response to information security Incidents

a) Response plan and strategy for appropriate handling of security incident shall be formulated which covers incident cycle from identification to root cause analysis to resolution.
b) The overall response to reported incidents shall include identification of corrective actions.
c) Where a follow-up action against a person or organization after an Information Security Incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdictions.

1.6 Learning from information security Incidents

a. Analysis shall be conducted for the Information Security Incidents and shared with the appropriate authorities on a periodic basis.
b. Knowledge gained from resolution of security events shall be used to reduce likelihood of similar incidents in the future and help with limiting the impact of the Incident.
c. The analysis shall consider the following factors:
    - Type of Information Security Incident
    - Volume of Security Incidents; and
    - Wherever possible, costs incurred due to Information Security Incidents.
d. The output of the analysis shall be used to improve the security posture and to identify recurrence or impact tolerance.

1.7 Collection of Evidence

a) Procedures for identification, collection, acquisition, and preservation of information which can serve as evidence shall be defined and documented.
b) Where a follow-up action against a person or organization after an Information Security Incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).
c) Before the seriousness/criticality of the incident is realized, due care shall be taken to ensure that necessary evidence/information is not destroyed intentionally or accidentally.

1. Objective

The objective of this Information Security Policy is to ensure that “Due Care” is exercised in protecting information assets of DBL and “Due Care” is defined as the cost-effective protection of information at a level appropriate to its business value. The value of the information assets can be quantified as the risk to DBL and if the confidentiality and/or integrity and/or availability are compromised.
The objective of the policy is to :

- Demonstrate organization’s commitment to establish information Security by establishing comprehensive management process throughout the organization.
- Convey management’s mission and vision for incorporating Information Security in the Organization’s culture
- identify groups/teams and individuals responsible for implementation, maintenance, compliance, and improvement of Information Security
- establish requirements for DBL employees to understand and adhere to Information Security Policies and Procedures.

2. Scope

The information security policy applies to all DBL employees & employees of enabling functions including Network and Data Centre Operations, Application development and testing, Human Resource, IT department, Facility team and Internal Audit at DBL regardless of position.

The policy shall also be applicable to all external/ third party personnel (i.e. vendors, third party resources, consultants, interns, contractors employed with DBL and clients/ customers visiting DBL offices who engage in work and have access to DBL information or information processing facilities).
ISMS applies to all assets (i.e. physical assets, paper assets, people assets, information assets, site as an asset, software assets and services as an asset) at DBL.

The ISMS applies to all IT technologies and services (i.e storage, backup, server hosting services, application services etc) that are delivered as an enabler to support DBL delivery. Technology will also act as an enabler in implementing the information security controls across the organization. To support technology,
As a part of the ISMS the following departments are covered, supported externally by HR, Physical Security, Facilities, IT, Internal Audit:

- Data Centre Operations
- Network Operations
- Application Development and Testing

The Organizations ISMS shall be maintained as per the Statement of Applicability highlighting all the controls that are implemented and justifying the controls that are not implemented.

3. Policy

Information is an asset which, like other important business assets, has a value to the organization and consequently needs to be protected. Therefore, DBL recognizes its information assets as a significant and valuable resource. The DBL information security policy provides management direction and support to ensure protection of DBL information assets, and to allow access, use and disclosure of such information in accordance with appropriate standards and laws. The specific information security objectives for DBL and its enabling functions are:

a) To develop and maintain an effective ISMS consisting of an information security policy, supporting procedures and a risk assessment framework.
b) To identify all assets that directly or indirectly impact the client operations and understand their vulnerabilities and the threats through appropriate risk assessment.

c) To comply with applicable laws and contractual obligations pertaining to information security and data privacy, for its client data and internal data; and
d) To raise awareness of information security risks within DBL and create & maintain a security-conscious culture ensuring that all breaches of information security and suspected weakness are reported, investigated and adequate actions are taken.

1. Policy Framework

DBL Information Security Policy is supported by detailed information security policies and procedures, implementation guidelines and templates. The information security procedures are derived from the policy statements and provide the details of necessary actions to achieve the objectives of the policy statement. The templates are derived from the detailed procedures and aim at facilitating the implementation of the Information Security Management System.

2. Policy Owner

a. The ownership and responsibility for the maintenance of this information security policy lies with the CIO.
b. User must be contacted in the event of any questions on the contents of this policy, suggestions for improvements, specific security recommendations and any other areas relating to the security of systems, data, or information of DBL and all the enabling functions.

3. Policy Review and Approval

a) This policy document shall be reviewed at least annually by the Leadership and Cybersecurity team or in events of any significant changes (i.e., change in operations, change in technology, regulatory changes, major security incidents) in the existing information security environment affecting policies and procedures. The policy owner will be responsible to make the changes to the policy document. The ITC will be responsible to approve the changes to the policy.
b) All changes to the policy shall be communicated by the cybersecurity team to all employees and third-party personnel through appropriate forums and channels.

4. Compliance

a. All employees, stakeholders and third-party vendors, contractors and consultants having access to DBL information and all the supporting processes of information processing facilities shall comply with the information security policy. All violation or any attempted violation of the information security policies shall result in disciplinary action to be taken by the ITC in consultation with human resources. Disciplinary action shall be consistent with the severity of the incident, as determined by an investigation department (in accordance with DBL Code of Conduct); and
b. All violations of the information security policy must be reported to the respective Location/ Department Head (for all the supporting processes) and the cybersecurity team.

5. Exceptions

a) Approval for exceptions or deviations from the policies, wherever warranted, will be provided only after an appropriate assessment of the risks arising out of providing the exception. This assessment will be conducted by the cybersecurity team. Exceptions will not be universal but will be agreed on a case-by-case basis, upon official request made by the asset owner. These may arise, for example, because of local circumstances, conditions or legal reason existing at any point of time. Exceptions to the Information Security Policy may have to be allowed at the time of implementation of these policies and guidelines or at the time of making any updates to this document or after implementation (ad-hoc).

b) All exceptions during implementation must be submitted by IT department to the ITC; and
c) For any ad-hoc exception required by a User, a request for exception must be submitted by the user through formal channels to the ITC. This request must be approved by the User Department Head / asset owner.

6. Inquiries

Any inquiries relating to policy, or the application of this policy shall be referred to the ITC.

7. Management direction for information security

The management, consisting of the ITC, shall be accountable for enforcing the implementation of DBL information security policy. The location/ department heads along with the ITC shall be responsible for managing the overall information security for DBL. All employees shall read, understand, and adhere to DBL Information security policy. The information security policy for DBL shall be reviewed at least once in a year and at a time of any major change(s) in the existing environment affecting the policies and procedures The review shall be conducted for assessing the following:

- Impact on the risk profile due to, but not limited to, the changes in information assets, deployed technology/ architecture and/ or legal requirements, emerging threat landscape; and
- Effectiveness in policies.

1. Objective

The objective of this Logging and Monitoring Policy is to ensure that DBL can detect unauthorized access to its Information Assets and provide the necessary and timely input to mitigate the associated risks.

2. Scope

This Policy applies to all computing and network resources that are used for information processing of DBL Logging activities of physical security control activities like electronic entry access control and CCTV activities shall be addressed as environment controls. All Users shall be subject to this Policy and as a result, should have no expectation of privacy in their use of DBL's Information Assets, in accordance with applicable law.

3. Policy

DBL shall develop a methodology to record and monitor User activities to ensure that errors, exceptions, privileged & unauthorized access with respect to the computing and network resources are recorded and monitored with time synchronization.

These logging and monitoring activities shall ensure:

a) Audit logs recording exceptions are produced for critical systems and kept for an agreed period to assist in future investigations and access control monitoring.
b) Procedures for monitoring the usage of information processing facilities are established and the results of the monitoring activities are reviewed periodically.
c) Controls are implemented to protect logging facilities and log information against tampering and unauthorized access.
d) Administrator and system operator activities (such as the time at which the event occurred, the information of the event or failure, which account and which administrator or operator was involved, etc.) are to be logged.
e) Suitable actions shall be initiated based on the system and security logs to protect all information systems and network infrastructure from external and internal attacks.
f) Event Logging: Servers, routers, firewall and critical application related logs are captured and stored for assessment. The event logs should be monitored by administrator and address any issues needing attention from time to time. The log is stored for one month before deleting from the storage.

1. Objective

The purpose of this Physical and Environmental Security Policy is to prevent unauthorized physical access, damage, and interference to premises of DBL and to ensure sensitive information and critical information technology are placed in secure areas.

2. Scope

This document is applicable to all the locations of the DBL

3. Policy

1. Physical security perimeter

a) Physical protection can be achieved by creating several physical barriers around the building premises and information processing facilities.
b) Each barrier establishes a security perimeter increasing the total physical protection provided. A security perimeter can be a wall, a card-controlled entry gate or a staffed reception desk.
c) The DBL offices shall be logically divided into different zones. Each zone shall have the appropriate level of access restrictions and access authorization requirements. areas containing critical IT equipment (such as the Network room and the data centers) shall be designated as high-security zones. Where applicable, the policies and procedures shall include and abide by the applicable laws.

2. Physical entry controls

a. Only those employees, whose job description demands access to DBL systems, shall be allowed to enter the premises. Visitors' entry into the premises shall be restricted by appropriate security validations like checking the identity of the visitor, random frisking, checking their belongings and bags, etc.
b. A designated security agency shall have 24×7 guarding of premises.
c. The credentials of the security personnel posted at such premises shall be verified with the agency to mitigate risks of theft or vandalism. The contact information of the security agency shall be maintained by the DBL Administration department for easy identification in the eventuality of a mishap. The information of the security personnel shall be verified with the security agency whenever required by DBL.

3. Securing offices, rooms, and facilities

Depending on the sensitivity of information managed within, the physical security for offices, rooms and facilities shall be designed and applied. Access to Network room shall be restricted. Only the IT team personnel and those authorized shall be allowed to access the Network room.

4. Protecting against external and environmental hazards

a) DBL offices shall be fitted with appropriate firefighting devices at critical locations to arrest the fire and to avoid damage to the various resources of DBL. Safety measures like fire and earthquake evacuation drills shall be practiced regularly.
b) Appropriate safety measure shall be taken to avoid loss and damage due to water flooding or inappropriate drainage system within the premises of DBL.
c) Physical protection against damage from natural or man-made disaster shall be designed and applied.

5. Working in secure areas

Physical protection and guidelines for working in secure areas shall be defined and applied. Third party support service personnel shall be granted restricted access to secure areas. The access shall be authorized and monitored.

6. Public access, delivery, and loading areas.

Access points such as delivery areas and other points where unauthorized personnel may enter the premises shall be controlled and isolated from information processing facilities.

7. Equipment sitting and protection.

All electronic office equipment including faxes, printers, photocopiers etc, shall be physically secured.

8. Security of Desktops and Networks

a) Desktops shall be adequately protected from fire, water and pollution damage and power supply fluctuations.
b) Networks shall be secured from fire, heat, dust, and water.
c) Interception or damage to Network cables shall be controlled.

9. Media Handling and Security

a. Media shall be protected from physical damages like fire, moisture, and magnetic interference.
b. A stock or inventory of all the media shall be maintained.
c. Media shall be disposed of securely and safely when no longer required. Formal procedures for the secure disposal of media shall be established to minimize the risk of sensitive and confidential information being disclosed to unauthorized persons.

10. Supporting utilities

a) Equipment shall be protected from power failures and other electrical anomalies. A suitable electrical supply shall be provided that conforms to the equipment manufacturer's specifications.
b) Options to achieve continuity of power supplies include:
   - Multiple feeds to avoid a single point of failure in the power supply.
   - Uninterruptible power supply (UPS)
   - Back-up generator
c) A UPS to support orderly close or continuous running shall be implemented for equipment supporting critical business operations. Contingency plans shall cover the action to be taken on failure of the UPS. UPS equipment shall be regularly checked to ensure it has adequate capacity and tested in accordance with the manufacturer's recommendations.
d) A back-up generator shall be considered if processing is to continue in case of a prolonged power failure. If installed, generators shall be regularly tested in accordance with the manufacturer's instructions. An adequate supply of fuel shall be available to ensure that the generator can perform for a prolonged period.
e) In addition, emergency power switches shall be located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. Emergency lighting shall be provided in case of main power failure. Lightning protection shall be applied to all buildings managed by DBL, and lightning protection filters shall be fitted to all external communications lines.
f) UPS Preventive Maintenance performed by service provider annually
with IT SLA(TAT) as below
High Priority: 4 Business Hours
Medium Priority: 8 Business Hours
Low Priority: 16 Business Hours

11. **Cabling security**

Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

12. Equipment maintenance

Equipment shall be maintained to ensure its availability and integrity.

13. Security of equipment off premises

Security shall be applied to off-site equipment (e.g., Laptops, Servers etc) considering the different risks of working outside the organization's premises.

14. Secure disposal or reuse of equipment

IT hardware and equipment shall be disposed of only after approval. Further, appropriate data and media destruction shall be performed prior to disposal. Disposal of retired hardware and media shall comply with prevalent environmental regulations.

15. Removal of property

a. Equipment, information, or software shall not be taken off-site without prior authorization.
b. The following controls shall be applied:
    - Employees, third-party and contractors who have the authority to take the equipment off-site shall be clearly identified.
    - Time limits for equipment removal shall be set and returns checked for compliance.
    - Equipment shall be recorded as being removed off-site and recorded when returned.

16. Environment controls

To address the threats posed by environmental hazards to the information systems assets, appropriate controls will be implemented to detect, correct, and prevent identified environment threats like Shock, Fires, Water Leakages, Power Fluctuations, Pests, Vandalism, and Robbery etc.

17. Cleanliness

Network room will be kept dust free and protected from any kind of spillage of water or other liquids. To ensure dust free environment, room will be cleaned by the House Keeping under the supervision of IT infrastructure team on a regular basis. The systems and peripherals will be cleaned by DBL 's housekeeping on daily basis. Smoking, spitting, eating, and drinking is prohibited in the Network room. To enable Temperature and Humidity

a) Temperature of the Network room will be checked every 30 mins as per the recommendation received from the infrastructure head.
b) The admin team will keep a record of DC temperature and humidity.
c) The air conditioners will be maintained by the admin department.

18. Fire Detection and Prevention

a. Cabling will be sheathed in fire-resistant conduits.
b. Smoke or Fire detectors will be installed to forewarn against fire.
c. The Fire detectors will be under the supervision and maintained by the Safety, Health, and Environmental team.
d. Appropriate portable gas-based fire extinguishers will be installed at easily accessible locations. These will be suitably serviced and tested at vendor-defined intervals. Adequate training will be imparted to appropriate personnel on the use of the equipment.

19. Water Leakage Prevention

a. Information assets will be housed in a dry environment with appropriate measures in place to prevent water leakage.
b. Waterproofing and tarring will be done prior to the monsoon.

20. Power Supply

a) Centralized Uninterrupted Power Supplies (CUPS) and power-conditioning equipment will be used and maintained. Critical electronic equipment will not be connected to raw power supply.
b) The admin department of DBL will maintain CUPS and Power Conditioning Equipment as per the admin department existing practices at applicable locations.

21. Cabling

a. The power and data cabling will be separated so that they are easily identifiable.
b. The cabling will be structured to remove clutters.

22. Pests and Insects

a) Pest and insect control mechanisms will be implemented to prevent damage to the information systems assets..IT infrastructure of DBL will periodically spray repellents in the rooms containing information system assets at sites wherever applicable.

1. Objective

The objective of this Problem Management Policy is to create a problem management framework to be used as a reference by DBL to increase availability of DBL's IT System, improve service levels, reduce costs, and improve customer convenience and satisfaction by reducing the number of IT Service Incidents for which a permanent resolution is required ("**Problem**"). The cause is not usually known at the time a problem record is created.

This Policy is based on leading practices and will assist DBL in:

- Identifying and classifying problems and their root causes and providing timely resolution to prevent recurring incidents.
- Providing recommendations for improvements.

2. Scope

This policy applies to all Users of DBL's Assets, and any other individuals using the IT resources of DBL. This includes contractors, consultants, third party associates and any temporary employees.

3. Policy

DBL shall adhere to the policies, processes, and procedures defined in the DBL's IT governance framework for ensuring Problem Management activities are planned, managed, and aligned with the organization's goals and objectives, as per the compliance and waiver criteria defined in the policy. This shall enable DBL to increase availability, improve service levels, reduce costs, and improve customer convenience and satisfaction by reducing the number of operational Problems.

1. Identify, classify, and diagnose problems.

a) The Problem Manager shall manage Problems through a defined Problem Management process. This process shall include identifying the root cause of any identified or potential Problem, introducing a resolution for the Problem, and implementing measures to prevent the Problem's recurrence.
b) Details of all performed activities at all stages of the Problem Management process shall be documented and included as part of the Problem record.
c) All Problems shall be registered and recorded in a unified and consistent manner by the service desk.
d) All Problems shall be categorized, classified, and prioritized for effective analysis and reporting.
e) The categorization of the Problem shall follow the categorization in its related incident/event record unless a correction is needed.
f) The prioritization of the Problem shall be decided based on an impact and urgency analysis.
g) The Problem Support Team shall investigate a problem's root cause and identify its resolution internally prior to any escalation (third party/vendor).

2. Resolve and close problems.

a. The Problem Manager shall allocate suitable resources to resolve the Problem based on an effort estimation exercise to ensure the timely resolution of a Problem. The allocated resources shall form the Problem Support team and shall comprise with the required expertise and skills from IT and / or from suitable vendors, if required.
b. All efforts shall be made to resolve the Problems within the defined resolution period. The Problem Manager and affected users shall be informed about any anticipated or unanticipated delays.
c. All Users shall be periodically updated on the status of their Problem record and on change of the record status.
d. The Problem Manager shall regularly review the status of unclosed Problem records, investigate delays, and address any identified delays with corrective actions.
e. For major Problems, the Problem Manager shall conduct post–resolution review sessions on lessons learned and identify opportunities for improvements.

f. The Problem Manager shall review problem records related to their divisions to identify trends on a periodic basis and ensure that their divisions implement suitable corrective actions to avoid any Problem recurrence.
g. The Problem records shall not be closed without:
   - Obtaining the user acceptance on the resolution, or
   - Notifying the user of the resolution and providing him with sufficient time to respond back.

3. Proactive problem management

a) The Problem Manager shall ensure that the Configuration Management, Incident Management and Problem Management processes and procedures are adequately integrated, to ensure effective management of Problems and enable improvements.
b) The Problem Assurance Team shall collect and analyze information from the various sources and identify emerging patterns that indicate a potential problem.
c) The Problem Manager shall conduct periodic reviews of the Problem Management to assess its effectiveness and efficiency; suitable recommendations shall be made for possible improvements.

4. Critical success factors

Critical Success Factors for the Knowledge Management process is given below:

a. Identification, classification, categorization, and prioritization of reported Problems.
b. Diagnosis of the Problem and analysis of the root cause.
c. Creation of known-error records, appropriate workaround, and identification of potential solutions.
d. Resolution and closure of Problems.
e. Collection and analysis of data to analyse emerging trends that indicate Problems.

1. Objective

The objective of this Service Request and Incident Management Policy (along with the accompanying procedures) is to form a Service Request and Incident management framework to be used as a source of reference by DBL employees to ensure that all Service Requests and Incidents related to the IT services are managed timely and efficiently.

This Policy is based on leading practices, and it:

- Establishes a Service Request and Incident management process within DBL's IT department to resolve of all types of Incidents and restore normal service, record, and fulfil User requests, and record, investigate, diagnose, escalate, and resolve Incidents.
- Ensures that Service Requests and Incidents related to DBL's Information Assets are reported, tracked, investigated, and resolved in an effective and efficient manner.

2. Scope

This Policy applies to all the Users of DBL's Information Assets. This includes contractors, consultants, third party associates and employees.

3. Policy

DBL shall adhere to the Policies and Procedures defined in the DBL's IT governance framework for ensuring Incident management and Service Request management activities are planned, managed, and aligned with the organization's goals and objectives, as per the compliance and waiver criteria defined in the Policy. This shall enable DBL to achieve increased productivity and minimise disruptions through quick resolution of user queries and incidents.

The Manage Service Requests and Incidents Policy will address the following:

- Recording the Service Requests.
- Fulfilling and updating Service Requests.
- Incident reporting and identification.
- Incident recording.
- Incident classification and prioritization.
- Incident management and resolution.
- Closing the Service Requests and Incidents.

3.1 Define Incident and Service Request classification schemes.

a) All reported Service Requests and Incidents shall be identified, recorded, and categorized based on a categorization scheme.
b) The Incident Manager shall define a workflow for handling and escalation of queries/Incidents.
c) All Service Requests and Incidents shall be reported to the Service Desk in a structured manner, fully logged with details of the Service Request or Incident, so that a historical record is maintained.
d) The Incident Manager shall prioritize all logged Incidents based on SLA service definition of business impact and urgency.

3.2 Verify, approve, and fulfill service requests.

a. The IT Service Request Manager shall fulfill the Service Requests by using, where possible, self-help automated menus and predefined request models for frequently requested items.
b. All service requests shall be recorded in a unified and consistent manner. For this purpose, a Service request record would be used.
c. The IT Service Request Manager shall conduct periodic reviews of the Service Request management process to assess its effectiveness and efficiency, and to make suitable recommendations for possible improvements.

3.3 Investigate, diagnose, and resolve Incidents.

- The Incident Analyst shall escalate un-resolved Incidents for further investigation and diagnosis and user shall be updated accordingly.
- The Incident Analyst shall document, apply, and test the identified solutions or workarounds and perform recovery actions to restore the IT-related service.
- The Incident Analyst shall perform sufficient testing to ensure that recovery action is complete and that the service has been fully restored.

3.4 Close and track Service Requests and Incidents

- The Incident Analyst shall check whether the Incident has been fully resolved and that the users are satisfied and willing to close the Incident.
- All the associated incident records shall be updated prior to the closure of the incident.

3.5 Critical Success Factors

Critical Success Factors for the Manage Service Requests and Incidents process are given below:

- Service Desk acts as a single point of contact for all Incidents reporting and recording.
- Clearly defined targets in agreed SLAs.
- Customer-oriented and technically strong training support staff with the correct skill levels, at all stages of the process.
- Integrated support tools to drive and control the process.

1. Objective

The objective of this Supplier Relationship Policy is to establish two-way, mutually beneficial relationships between DBL and its suppliers, and is intended to improve quality, cost, delivery, and innovation. This Policy sets out the details of how DBL will deal with and manage third parties who supply DBL with goods, materials, and services.

2. Scope

This Supplier Relationship Policy is applicable to all third-party providers of Information Technology-related goods, materials, and services to DBL ("**Suppliers**").

3. Policy

1. Service Delivery

a) DBL shall ensure that all services to be provided by Suppliers are clearly identified and the relationship with the Supplier is managed through clearly identified points of contact at both DBL and the Supplier.
b) A formal written contract shall be entered into between DBL and all Suppliers to DBL as well as with any Supplier having access to or using DBL IT Systems. Any services to be provided by the Supplier shall be covered by a strong Service Level Agreement ("**SLA**") that takes into consideration expected levels of service, security, monitoring, contingency, and other stipulations as appropriate.
c) Security controls and service levels specified in the SLA shall be implemented, operated, and maintained by the Supplier and regularly reviewed by DBL.
d) Contracts/Agreements shall include information security requirements to ensure Supplier compliance with DBL security policies and procedures.
e) All Suppliers shall be required to provide information to DBL about related sub-contractors and obtain DBL's permission for the subcontracting, prior to initiation of work by the sub-contractor.
f) Non-Disclosure/ Confidentiality agreements to protect DBL information assets shall be signed by vendors, third parties, contractors and by sub-contractors of the vendors.
g) Where applicable, the Policy and Procedures should include and abide by the applicable laws.

2. Information security policy for supplier relationships

a) At DBL Information security requirements for mitigating the risks associated with supplier's access to the organization's assets are agreed with the supplier and documented.
b) At DBL, controls should be addressed to secure the processes and procedures to ensure appropriate controls that may be implemented either within the organization or by the supplier. Access control, especially for sensitive information must be accurately defined, managed and monitored. Awareness training for both the organization's staff and supplier staff that handle or interact with data must be addressed. Finally, service transitions should be documented and include procedures for secure data transfers and availability as the relationship changes during the life-cycle.

3. Addressing Security within Supplier Agreements

a. All relevant information security requirements are established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

b. Supplier agreements should be established and documented to ensure there is no misunderstanding regarding both parties' obligations to fulfill relevant security requirements. Supplier agreements should include clear and concise information regarding:

- The types of data being accessed and methods of access.
- DBL data classification requirements as it apply to the supplier.
- Definition of acceptable uses for the data handled by the supplier.
- Processes and procedures for monitoring compliance with the contract requirements.
- A "right to audit" the supplier or regular access to external assessments
- Conflict and defect resolution.
- Required screening, training or other obligations of the supplier's staff.
- The use of sub-contractors to provide services and the extension of security requirements to them.
- It is important to address the risk early in the procurement phase of the relationships with external parties so that roles, and responsibilities and expectations can be clearly defined in agreements or contracts.

3. Monitoring and reviewing third party services.

Security controls and service levels, associated reports and records of Suppliers shall be independently assessed, reviewed, and monitored. Supplier audits shall be performed annually to review the services provided to DBL by the Supplier.

4. Managing changes in third party services

Changes to the provision of services, including maintaining and improving existing information security policies, procedures, and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

1. Objective

The objective of this System Acquisition, Development & Maintenance Policy is to protect DBL sensitive information from unauthorized access, loss, or inaccuracy.

DBL's IT Systems include products developed in-house and the development process followed at DBL. This System Acquisition, Development and Maintenance Policy sets out the approach to be taken for secure development activities within DBL.

2. Scope

This Policy applies to all DBL employees, sub-contractors and external consultants focuses on the development process for the DBL IT products.

3. Policy

1. Security requirements of information systems

a) Security requirements in an information system shall be identified and documented during the requirements gathering and analysis phase of acquisition, development or change of information systems. They shall be justified and agreed with business process owners.
b) Systems security requirements shall reflect the business value of the information assets involved (**Ref:** Asset Management Policy and Procedures) and the potential damage that may be caused due to the absence of sufficient security. Where applicable, the Policy and Procedures shall include and abide by the applicable laws.

2. Cryptographic control and key management policy

a) Risk assessment shall be conducted to identify the needs, methodology, business areas and usage of encryption or cryptography.
b) Cryptographic controls shall be used for securing information that is confidential and restricted. They shall be used (a) if the information cannot be protected by any other means and (b) wherever applicable and feasible.
c) When confidential information that is not actively being used is stored or transported in computer-readable storage media (such as servers, magnetic tapes, floppy disks, or CDs), it shall be in encrypted form wherever feasible and applicable.
d) Information used to verify the identification of remote terminals shall be appropriately protected. Static or reusable authentication information shall be encrypted during storage and while passing through the network using encryption software or hardware.
e) All cryptographic keys should be protected against modification, loss, and destruction. In addition, secret and private keys need protection against unauthorized disclosure. Equipment used to generate, store and archive keys should be physically protected.

3. Security of system files

a. Detailed procedures shall be developed to control the installation of software on operational systems.
b. Test data shall be selected carefully, protected, and controlled by the third party.
c. Program source code available to DBL shall be stored under restriction and only authorized personnel shall have access to the same.

4. Security in development and support processes

a) Formal procedures shall be developed for change management. All proposed system changes shall be authorized and reviewed to verify that they do not compromise the security of either the system or the operating environment.

b) Business critical applications shall be reviewed and assessed prior to installation of operating system patches or updates in a test environment to ensure that there is no adverse impact on security due to the changes in the operating system.
c) If the software is developed by a third- party the following shall be done:

- DBL shall ensure that software development processes comply with DBL's Information Systems Acquisition, Development and Maintenance Procedure.
- DBL shall have appropriate licensing agreements and contractual requirements for quality and accuracy of code.
- DBL shall get assurance from the third-party for quality and accuracy of the work conducted.
- DBL shall get the ownership of the source code. If this is not feasible, the code shall be kept under an escrow arrangement.
- DBL shall get the rights of access for audit of the quality and accuracy of the work.
- DBL shall outsource testing processes and approve the process.
- DBL shall ensure scanning of outbound media and periodic monitoring of systems activities are conducted to ensure no information leakage occurs.

5. Technical vulnerability management

Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

1. Objective

The objective of this Building Security Policy is to protect DBL information assets as per Information security Policy

2. Scope

This Policy applies to DBL Head Office premises

3.Policy

Normal / medium level physical security applies to offices and other locations which house information, information systems or IT equipment and where no sensitive or highly confidential information is stored (in an unencrypted form). It also applies to data and voice network infrastructure housed outside secure computer rooms. In general, there should at least be one substantial physical security measure in place at all times to protect unattended information assets. Staff must keep the doors and windows of unattended offices locked. Outside normal building opening hours building entrances, office doors and windows must be kept locked when unattended. Data and voice network infrastructure housed outside secure computer rooms must be physically secured, e.g. in locked security cabinets. Arrangements must be periodically reassessed in terms of performance and ongoing suitability.

High level physical security This applies typically to computer server rooms housing important information systems or communications systems equipment. However, it may also apply to other situations where high value or highly sensitive information in an unencrypted form is being held or handled. Physical security to an appropriate higher standard is required. Special requirements to achieve this may involve use of:

- Intruder detection (burglar alarms)
- Environmental monitoring and alerting systems
- Strong rooms
- Door and window locks
- Systems to control and log access to sensitive areas
- Out-of-hours security support
- Specialized fire extinguishing systems (which may be automatic)

Arrangements must be periodically reassessed in terms of performance and ongoing suitability.

Departmental managers are responsible for defining to Infra Admins their building security requirements and Infra Admins is responsible for determining the specifics of how to implement those requirements.

Company Staff are obliged to implement or comply with building security arrangements affecting the areas they work in or visit.

A proper system to manage building access controls must be in place to cover all Company buildings. This system is ultimately the responsibility of Infra Admins.

Where Infra Admins directly manages access controls it must hold accurate data about who is in possession of keys, access cards and access codes.

Where responsibility for managing access controls is delegated to departments, then Infra Admins must maintain accurate data about what access controls are delegated and to whom.

Where responsibility for managing physical access controls, such as door keys or access cards, is devolved to departments then it is the responsibility of the Head of Department to ensure that a proper system to manage them is in place.

1. Objective

The objective of Cryptographic Control and Encryption Policy is to ensure the confidentiality, authenticity / integrity, and availability of the information by applying appropriate levels of cryptographic controls. The encryption technique is applied to ensure the security for critical removable media, laptop hard-drives, portable devices, mobiles, and remote access should be allowed to the terminal services, and Wi-Fi protected encryption is mandatory for all the wireless networks.

2. Scope

The scope of this policy is establishing keying techniques which are applicable to protect physical and data access at DBL premises and the information assets. If any unauthorized access or breach of the information security management system, it should be reported to ITCO Team and the respective incidents will be recorded and reported.

3. Policy

1. As part of DBL IT Policy Manual, system is established to ensure that employees, contractors, and third-party users understand the how to use the cryptography controls in the organization in effective manner and implementation of required keying management techniques such as symmetric, key encryption and public / private key encryption.

2. At DBL, a policy on the use of cryptographic controls is developed and implemented to protect the information pertaining to DBL and to ensure the confidentiality, authenticity/integrity, and availability of the information by applying appropriate levels of cryptographic controls.

3. Cryptographic control applies to the information that is stored in the electronic devices. The information stored in DBL includes several electronic devices such as laptops, servers, LAN servers, mobile devices, etc.

4. Information security is achieved by applying cryptographic techniques such as encryption and decryption.

5. At, encryption technique is applied to ensure the security for critical removable media, laptop hard-drives, portable devices, mobiles, and remote access should be allowed to the terminal services, and Wi-Fi protected encryption is mandatory for all the wireless networks.

6. And all the E-mail attachments consisting of sensitive and critical information such as several documents (PDF's, Word Docs, Excel sheets) should be encrypted to safeguard the information and to survive from several threats.

7. The policy requirements on the use of cryptographic controls include such as

    - Encryption according to classification of data.
    - Encryption of data in transit.
    - Key management.
    - Avoiding adverse impacts in encryption technique.
    - Reporting security incidents in data management.
    - Roles and responsibilities
    - User awareness.

8. Encryption according to classification of data: The data should be encrypted depending on the severity of the information that the document contains. The encryption techniques are applied depending on whether the data is critical or sensitive.

9. Encryption of data in transit: Encryption of data in the transit includes the data which is already there in the public domain may be secured and unaccepted. This data may include sensitive or critical data.

10. Avoiding adverse impacts in encryption technique: At DBL, the whole data pertaining to DBL that is encrypted and stored in one central location should be secured and easily managed and if any threats are there the data should easily be decrypted from that central location, and all the adverse impacts of encryption techniques should be avoided.

11. Reporting Security incidents in data management: At DBL, all actual and potential data should be authorized and secured. If any unauthorized access or breach of the information security management system by the employees, it should be reported to ITCO Team and the respective incidents will be recorded and reported.

12. Roles and Responsibilities: At DBL, to ensure the information security the roles and responsibilities have been defined by providing the authentication. The roles and responsibilities should be defined to implement the encryption techniques to safeguard the information from the threats.

13. User Awareness: At DBL, the users should be aware of encryption and decryption techniques to protect the data from the threats and to safeguard the information.

14. This document sets out principles and expectations about when and how encryption of DBL.
This document includes statements on:

- Cryptography and India law
- Data encryption for secure network transit
- Required use of encryption
- Management of encryption keys
- Required use of digital signatures
- Unsupported use of encryption
- Cryptography implementation

15.Cryptography and India law

Export regulations relating to cryptography technologies are complex. (Any member of the Company becoming involved in export of cryptography is advised to seek specialist advice. Information Assurance Services can assist by coordinating access to such advice.)

The Regulation of Information Technology Act came into force in 2000. It includes a provision for public authorities to demand, where it is judged there are reasonable grounds, decryption keys or decryption of information stored on computer systems in the India. Anyone who could be assumed to have encrypted and stored data is very strongly advised to ensure that they retain the means to decrypt it.

16. Data encryption for secure network transit

Provided no other restrictions apply, it is permitted for all Company staff and staffs to use computer systems which would normally and by default use encryption, in order to secure data in transit on a communications network.

Whenever possible and appropriate, encryption shall be used to support security of remote access connections to the Company's network and computing resources.

17. Required use of encryption

A. Loss, theft, or unauthorized disclosure of certain information could be detrimental to the Company, its staff or staffs. Such information includes that defined as personal data by the IT Act 2008 amendments. Where the Company is handling digital personal data that cannot be sufficiently secured by physical controls, the data must be encrypted.

B. Data which must be handled securely, using encryption where pertinent, includes:
   - Any personal data classed as “sensitive” by the Data Protection Section of IT Act.
   - Any data, that is not in the public domain, about a significant number of identifiable individuals.
   - Personal data in any quantity where its protection is justified because of the nature of the individuals, source of the information, or extent of the information.

   Data as described above must be encrypted:

   - Where it is stored on a computing device or any computer storage medium which may be exposed to a significant risk of being lost or stolen. (Computers used to access remotely stored data or to process locally stored data may create cache files. Depending on the technology in use persistent and unencrypted cache files may be created.) Any such device when outside a secure Company location is considered to be at significant risk, including home computers.
   - Where it is to be transmitted via a computer network using a mechanism that does not itself incorporate encryption. Depending on the specific technology being used this could refer to: sending data by email either within or outside the Company, transferring files offsite, remotely accessing files or Web pages. The risk is that unencrypted data in transit may be intercepted.
   - Where the data is being sent using a postal service such that the data media could be lost, stolen or intercepted and read whilst in transit.

C. Where data being handled by the Company is subject to an agreement with an external organization specifying use of encryption, the agreed handling procedures, encryption technologies and standards must be used.

D. Where personal data is to be encrypted and no overriding requirements (from an external body) apply, the recommended minimum Company encryption standards (or better) must be applied. For further details refer below to the “Cryptography implementation” section.

E. Individuals must be authorized by the Head of Department before taking or sending confidential information out of a secure Company location. Optionally the Head of Department may elect to authorize specific individuals to routinely undertake a particular activity involving a specific type of data. A departmental record of such authorizations is to be established and maintained recording the following details:
   - The data name or description.
   - Who has been authorized to remove the data.
   - Purpose for which the data is being removed.
   - Date of data removal or an indication where removal is routine, e.g. “advisor resignation”.
   - Where the data is being taken or sent.
   - Any agreed external security requirements that apply to the data.
   - Confirmation that the data will be encrypted and handled securely.
   - Encryption technology used e.g. name of encryption hardware or software.

F. Company Web transactions that involve the transfer of personal, sensitive or confidential data or funds must use encryption, for example, Hypertext Transfer Protocol over Secure Socket Layer or Transport Security Layer (HTTPS).

18. Management of encryption keys

18.1 Departmental procedures must be in place:

- To manage encryption keys in a way that ensures encrypted stored data will neither become unrecoverable nor accessible by an unauthorized person.
- To facilitate authorized officers of the Company to obtain prompt access to the encrypted information in the case of an emergency or investigation.
- To ensure that encryption keys are stored and always communicated securely.
- To record who holds encryption keys relating to important information.
- To revoke encryption keys when key holders leave.

18.2 Where practical, an unencrypted backup copy of critical Company data should be securely maintained. Critical backup data should be stored where there are appropriate physical security measures in place (e.g. on resilient computer servers in an alarmed computer room or on backup tapes stored in a fire safe preferably in a different building).

18.3 Where Company information received as email has been encrypted for secure transit, and is information which may be needed again later, it should be securely stored in a form which does not rely on ongoing accessibility of the senders public key.

19. Required use of digital signatures

Significant Company business information being communicated electronically should be authenticated by use of digital signatures; information received without a digital signature should not be relied upon. Staff involved must assess the level of risk and decide whether to require use of digital signatures or whether to use an alternative means to authenticate the communication.

20.Unsupported use of encryption

20.1. Staff and staffs should:

- Not store encrypted data on Company systems except where they are able to justify doing so for legitimate purposes.
- Be aware that the Company reserves the rights to request sight, at any time, of the unencrypted version of any data stored on its systems and the option to remove any data.

21.Cryptography implementation

a. All encryption products, standards and procedures used to protect sensitive Company data must be ones which have received substantial public review and have been proven to work effectively.
b. Where a department elects to undertake an activity that would incur a cost, in order to remain compliant with security policy, then that cost should normally be found from the departmental budget. For example, where a research project requires measures for secure data handling it is appropriate that costs for any necessary additional security measures are factored into the tender.

1. Objective

The Objective of this mobile computing policy is to define the controls that need to be implemented and maintained to protect information assets against unauthorized access that poses substantial risk to the organization. The policy intends to establish adequate controls for using mobile devices at DBL.

2. Scope

This Policy applies to DBL' IT Systems and all DBL information assets, including those in both electronic (e.g., information systems, applications, systems platforms, and computer operations) and physical (e.g., vendor contracts, loan documentation, client files, and personnel information) formats regardless of the location.

3. Policy

1. This information security policy document sets out additional principles and expectations relating to using mobile computing devices and using computers away from the office. It is a sub-document of Information Security Policy.

1. Definitions:

- Confidential information - information which if improperly disclosed or lost could cause harm or distress to individuals, or financial loss or reputational damage to the Company. This includes personal data, as defined by the Data Protection Act, and other valuable or sensitive information not in the public domain, such as information that is commercially confidential for the Company or a third party, and information related to intellectual property.
- Mobile computing device – a portable computing or telecommunications device that can execute programs or store digital data. Examples: laptop, tablet computer (including iPad), personal digital assistant (PDA), smart phone, smart watch and other wearable computers, digital camera, external/removable hard drive, USB memory stick or flash drive.

Mobile computing and telecommunications devices make it easy to work away from the office and thereby expose information to different and probably increased security risks. In particular, mobile devices are prone to loss or theft.

Use of mobile computing to work securely with confidential data may involve additional cost and effort; this may be an unnecessary expense where suitable centrally administered services are already available. The business need should justify committing additional resources to mobile computing.

This document includes statements on:

- Mobile Computing.
- Information handling requirements.
- Mobile computing equipment - purchase, suitability and support.
- Management of mobile computing devices.
- Reassignment, repair and disposal of equipment.
- International transfer of personal data and the Data Protection Act.

2. Policy scope

2.1. This policy relates to storing and accessing Company information:

- Using mobile computing devices.
- Using computers away from the office.

3. Mobile Computing

3.1.The Company does not require staff to store or access confidential information using computing devices that it does not own or manage. Should the Company require one of its members to use a mobile or home computing device to store or access confidential data, then a suitably configured Company owned device must be provided.

3.2.Staff are strongly advised not to store or access any confidential information from: privately owned home computers, public computers in libraries, cyber cafes, hotels etc. This is because the Company has no control over the specifications, operation or administration of such devices and therefore cannot be confident of their security.

3.3.Staff nevertheless electing to store or access confidential information from devices not owned by the Company should take appropriate security precautions based on a risk assessment that takes into account the nature and quantity of the data involved. They should be aware that certain data supplied by external bodies may be subject to specific security requirements. In the event of loss or disclosure of confidential information, individuals responsible for handling that data will be expected to give an account of the security precautions in use.

3.4. Individuals must not allow any access to, or use of, equipment that may put confidential information at risk of loss or disclosure. Examples:

- Individuals must not permit others, including family or friends, to use or modify any equipment provided by the Company to carry out their professional duties.
- Individuals, electing to take personal responsibility for storing or accessing confidential information using privately owned home computers, must ensure that others do not have access to or see that information. In addition, they must ensure that unauthorized persons do not have privileges to install software or otherwise put the security of the system at risk.

3.5. Individuals who opt to use a mobile computing device not owned by the Company to store or access confidential information are fully responsible for ensuring that the device features adequate security provisions in order to protect the information (see Management of mobile computing devices).

3.6.Any loss, or possible unauthorized disclosure, of confidential information must be reported to the relevant Head of Department and IT.

4. Information handling requirements

4.1. Individuals must be authorized by the Head of Department to remove or send confidential information outside a secure Company location, and a record must be kept of this by the department. Depending on the specific nature and quantity of the information it may also be necessary also to encrypt it.

4.2.Unencrypted confidential information must not be transmitted via a network where traffic may be subject to snooping or interception. (Unless there is reason to believe otherwise assume this is the case.) Where it is uncertain that encrypted network protocols are in use from source to destination then encryption of data files before sending them is required. The data will then be secure regardless of whether all, none or only some of the stages in the network link use an encrypted protocol.

4.3.Where confidential information is being handled using a mobile device also:

- Where possible anonymous personal data.
- Handle the minimum amount of data necessary for the work in hand.

- Hold the data for the minimum time.
- Make backups. Mobile computing devices can fail, be damaged or stolen so have an appropriate backup regime for any important data stored on the device. Also ensure that backups are held securely, where possible on the Company network.
- Use a password protected screen saver / screen lock. Should the device be left unattended this may help to avoid unauthorized access.
- Use strong passwords for all accounts which have access to the device. Weak passwords have been a major cause of compromised systems and data.
- Actively manage physical security and do not leave the device unattended where there is a significant risk of theft. Examples: do not leave it in a parked car, lock it in an office draw when not in use, lock the door when leaving it in an office etc.
- Do not leave the device logged in and unlocked where there is a significant possibility that it may be accessed by an unauthorized person.
- Do not work with confidential data where there is a risk of “shoulder surfing” i.e. someone looking over your shoulder at the screen or keyboard.

5. Mobile computing equipment – purchase, suitability and support

5.1.When considering use or purchase of a mobile computing device, that may be used to manage any confidential information, it is essential to ensure that:

- Where the device is to be used to handle data provided to the Company by external bodies or vice versa, it is capable of meeting any specific security requirements demanded.
- The device is technically capable of providing acceptable security for data whether that data is being stored, downloaded or uploaded to the device.
- There will be adequate technical support available to ensure that the device can be configured and used in a way that keeps confidential data secure.

5.2.Advice and support for approved Company devices and software may be requested from departmental computing staff or IT Services.

6. Management of mobile computing devices

6.1.To help ensure security, even on devices with full disk encryption, they must be actively managed in terms of configuration and maintenance. Encryption may not prevent access to data if a running full disk encrypted system is infected or hacked.

6.2.Ensure that devices have current and automatically updated anti-virus software installed. The presence of malware such as viruses or worms would be a threat to security of data on the device.

6.3.Ensure that the device remains up to date with security patches for both the operating system and any software applications installed.

6.4.Ensure that devices have correctly configured firewall software installed where applicable. Vulnerable network services would be a threat to security of data on the device.

6.5.Ensure user privileges are configured on the basis of “least privilege”. For example under Windows ensure that users that do not need administrator privileges are not in the “Administrator” or “Power Users” group.

6.6.Ensure that for normal business activities the user does not work with administrative rights. Administrative rights should be used only when it is necessary to perform specific system administration or configuration tasks.

6.7. Installing software from untrusted sources must be avoided. Such software is far more likely to harm security than tried and tested software obtained from well known legitimate sources.

6.8 Employees

a) Prior Issuance of devices

- Post approval from management, IT Department does system hardening of laptops.

b) Checklist:

  - BIOS Setup password
  - Disable External Storage Devices
  - Disable Unused ports
  - Approval from Management
  - NDA to be signed

- All laptop computers must have a machine/boot up password and/or user id that is required (in the set up) when powered up to avoid tampering of operating system and programs.
- Encrypt user Data and Email storage folder using windows encryption, where ever possible encrypt whole disk.
- Once the laptop is hardened as per the check list, the IT team updates the system inventory detailing to which employee it is assigned to and the laptop details like (make, configuration , MAC address, software, connectivity to wireless)

7.0 Maintenance

All laptops / smart phone users are required to return laptops to Network Team to facilitate updates to antivirus and general review on security aspects and vulnerabilities quarterly.

8.0 User Responsibility:

- Users are responsible for all data stored / created and backup requirement.
- In case data created on the system be stolen, lost user are required to report the incident within 30 mins.
- Users are responsible for equipment under their and will be held accountable for any loss or damage to such equipment and may be required to make good any loss.
- Laptops should not be left unattended in any public places nor be left unattended in open offices.
- If employee needs to use laptop in a public place, meeting room or other unprotected area, care must be taken to avoid unauthorized access or disclosure of information. A screensaver with password must be used.

9.0 Return of Laptop to the IT Department

- On leaving the employment, employees must return all portable equipment to the Network department.
- If the equipment is to be re-assigned to another employee of the organization it will normally be necessary to upload and/or delete the information as per check list.

10. IT Teams Responsibility – consultants / third party user carrying their own laptops

- External laptop users are required to enter the details of laptop in inward register.
- No external consultants / third party users of laptops will be given permission to access enterprise systems (file servers, database servers)

11. Reassignment, repair and disposal of equipment

11.1 HODs must ensure that data is removed as appropriate before a loan mobile computing device is reassigned to another person. Preferably this should be done routinely at the time the device is returned.

11.2. Data must be securely deleted when disposing of mobile computing devices. Either a suitably effective in-house procedure may be used, or another organization may undertake the work provided that they are subject to a contractual agreement stipulating secure data handling and deletion. (Note that simple file deletion is often inadequate for ensuring that files cannot be recovered. Staff needing to ensure that confidential data has been deleted are advised to seek assistance from their departmental Computer Officer or IT Services.)

11.3 Where a mobile computing device is to be repaired by another organization there are two options relating to personal or confidential data stored on the device:

- Remove the data from the device before the repair or maintenance work is undertaken.
- Use a company that is subject to a suitable contractual agreement stipulating secure data handling.

1. Objective

To establish and maintain policy for managing and, where appropriate, governing the technology that is used to process the Company's information assets in a secure, reliable and cost effective manner.

2. SCOPE

Applicable to all DBL cloud services

3. POLICY

3.1 This policy is to ensure that the DBL makes the best possible decisions regarding its use of Cloud based services. Cloud based services store information on remote servers, i.e. servers that don't belong to the Company. These can be generic services such as Dropbox and Google Drive but also major corporate systems such as the Amazon Web Services and Digital Ocean etc. The central principle is that we only engage with these services when we understand the implications of doing so. It is vital that the benefits, opportunities and risks have been assessed and that we have an evidential basis on which to make the decision.

The policy outlines what we should evaluate from a technology perspective when looking at a new Cloud based service. The key areas for evaluation are:

A. Data protection and information security: The Company's data is at the heart of everything we do. As such it needs to be treated with care. The Company has to comply with data protection laws and we must ensure we have assessed any risks to our data from engaging with Cloud based services.

2. CONTEXT

Information is the key asset of the Company. The Company's information assets and the technology used to process, transmit and store it, needs to be appropriately and cost effectively managed, secured and governed to protect against consequences arising from the breaches of confidentiality, failures of integrity, interruption to availability and failure to comply with legal, statutory or regulatory requirements. Failure to do so may result in the Company being unable to deliver its core services, while incurring significant financial costs as well as having legal implication and liability, and may also result in lasting reputational damage.

The Company is governed by important regulations and working practices, particularly regarding the procurement and use of Information Technology (IT) systems and services.

The relevant regulations and governance considerations for procuring and using externally provided Information Technology (IT) systems and services are covered in number of ways:

The legal, statutory and contractual aspect covered by Legal Services and the Procurement Unit. The Procurement Regulations stipulates that the Company's Standard Terms and Conditions must be used for any supplier contract, unless agreed otherwise with the Procurement Unit (IT Category Manager).

• The Information Security aspects covered under the Company's Information Security Policies overseen by IT Department

3. PURPOSE

IT Services is made accountable and responsible for managing and, where appropriate, governing the technology that is used to process the Company's information assets in a secure, reliable and cost effective manner, irrespective of whether they are provided by IT Services or departments; delivered using the Company infrastructure or by third party outsourcing or cloud services provider.

This document covers the guidelines and governance policy related to Information Technology capability provided by the third party outsourcing or cloud services provider.

It is acknowledged that the cloud services offer number of benefits including agility, cost reduction, flexibility of scale and remote access. However there are a number of relevant policies which need to be considered carefully when using "Cloud Services" for the information assets and technology capability:

• that involves sensitive, personal or confidential information

• that involves contracts which may be above certain financial threshold

• that involves unapproved technology and/or integration considerations not aligned to Company technology strategy

• where poor service quality and capability may impact on Company commitments to its stakeholders

It should be noted that the Procurement Regulations, IT Policies and standard Legal/Contractual compliance terms also covers facets of the selection and use of Cloud Services. These are administered by the respective teams and are not covered here even though there may be some technical input required for those aspects.

This document covers the IT Services technology & service considerations for the Selection and Use of Cloud Services.

4. DEFINITION OF TERMS

The definitions of the key terms relevant to the scope of this policy document are given below.

Cloud Services: In the context of this policy document 'Cloud services' is a general term for anything that involves delivering hosted technology services or cloud based products over the internet. It includes:

• The traditional definition of Cloud Services including all currently known and any new service models (IaaS – Infrastructure as a Service, PaaS – Platform as a Service, SaaS – Software as a Service), and all currently known and new deployment models (Public; Private; Community; and Hybrid cloud deployments) where there will be a formal contractual agreement between the provider and the Company.

• Hosted technology or application services provided by third parties with systems hosted in either dedicated or co-located infrastructure or cloud IaaS or PaaS, or as part of shared service offerings or collaborative initiatives or any combination of the above.

• Technology elements which are part of business process outsourcing, even though the contract may be just for business processes with no explicit mention of technology.

• Cloud based services or products used to process, store or transmit Company information assets, where there is a contractual agreement

5. Roles and Responsibility

5.1. IT Department will be responsible for creating and updating this policy.

5.2. IT Department will be responsible for governance and implementation of this policy in conjunction with associated stakeholder in this area, viz. Procurement, Legal etc.

5.3. The Service User/Procurer commissioning and planning the use of the cloud services is responsible for ensuring full compliance with this policy. Failure to comply with any Company policy may lead to disciplinary action.

5.4. The final decision on non-compliance with this policy will rest with the CIO.

6. Policy Details

6.1. This policy applies to the procurement, selection and use of all type of cloud services irrespective of the financial contract value for such service provision (including free, freemium, any type of subscription model, annual charges or part of a multiyear contract).

6.2. This policy supplements the regulation and policy directives covered by the Procurement Regulations and the Information Security policies. Hence aspects covered in those regulations and policies will not be repeated here.

6.3. The Service User/Procurer must contact IT Department via their IT business partner in the initial instance to ensure compliance with Cloud Service Policy when the works, services or goods to be procured are to be provided by Cloud Services as defined above, irrespective of the financial contract value of such services.

6.4 The Information risk assessment is to be carried out on the advice and guidance of IAS when the Cloud Service provider will process, transmit or store Company information asset that is of sensitive, personal or confidential nature.

6.5 IT Department will assess and consider whether the proposed service is acceptable, covering the following areas (but not limited to this list):

• Technical standards, in particular compliance with Authentication, Authorization, Integration, web domain and end user devices standards

• Relevant non-functional requirements, in particular technical security, availability, resilience, scalability, interoperability and technology life span and viability etc.

• Service management and support aspects, especially if the Service is going to be used by a large number of Company users.

• Technical aspects of Business Continuity and Disaster Recovery

• Technical considerations for end of service scenarios (Exit strategy)

• The requirement for management information and reporting

6.6 IT Department may also liaise with Procurement and other relevant functions to ensure that appropriate account is taken of technical and service aspects in the procurement exercise and ultimate contract, including the specification, tender evaluation criteria, terms and conditions and service level agreement.

1. Objective

To establish and maintain policy for reporting Software faults in time for ensuring availability of IT Assets as per Information Security Policy.

2. SCOPE

Applicable to all DBL Employees

3. Policy

Software faults on Company IT systems must be reported, logged and dealt with in an appropriate way.

Reporting software faults

Where a software fault has been identified, a detailed description of the problem should be reported to, and logged by, someone who is responsible for handling problems relating to the software system

Software users should be provided with information about what level of support they can expect; preferably this information should be documented and readily available. It is important that those supporting software, or operating a fault logging service, are able to advise software users of the level of support available.

A person who has logged a software fault should be kept informed, or be able to find out, how management of the fault is progressing. Where it is impossible to rectify a fault, that fact should be logged and the person who reported the fault should be informed.

It is important that an escalation procedure should be brought into play where a reported fault is serious, e.g. represents a significant security risk, and cannot be rectified immediately. A decision to remove a software system with a severe problem from service may be needed.

Problems with Central Service software systems supported by IT Services should be reported to the IT Department help desk (email ITCO@dilipbuildcon.co.in). The IT Service Desk will log details of the fault, manage investigation of the problem and report back to the person that has logged the fault.

1. Objective

To establish and maintain policy for managing Software Licenses to ensure Company's information assets in a secure, reliable and cost effective manner.

2. SCOPE

Applicable to all DBL Software applications

The Software Regulations apply to all DBL employees and staff and all those who are granted use of a Company IT account including but not limited to external collaborators.

It should be noted that the Software Management Policy is still applicable to all software, including Freeware, Shareware and Public Domain Software, irrespective of whether it is included within the scope of the Software Regulations.

They cover software procured for use in all DBL environments, including home use. All software acquired on behalf of the Company shall be deemed to be Company's property and governed by the Financial Regulations currently in force.

3. Policy

This document sets out the regulations and controls that apply to the use of software in compliance with the above policy as determined and approved by the Top Management

The purpose of the Software Regulations is to ensure that all software in use within the Company is licensed in order to prevent copyright infringement and to ensure proper software asset management. There is also a requirement to ensure value for money in relation to software purchasing.

4. Definition

Software can be defined as "A set of instructions that causes a computer to perform one or more tasks". Software types include Commercial, Freeware, Shareware and Public Domain Software. This is not an exhaustive list and not all these types are necessarily approved by the Company .

5. Security Risk

a) DBL licenses the use of computer software from a variety of third parties. The software developer normally copyrights such software and, unless expressly authorized to do so, the DBL has no right to make copies of software except for backup or archival purposes. Copyright laws protect software against copying and distribution, even in the absence of a license agreement.
b) Under the Copyright, Design & Patents Act 1988 the illegal reproduction of software can be subject to civil damages and to criminal penalties including fines and imprisonment.
c) If the use of illegal software were discovered, both the person who made the illegal copy and the Company could be liable to prosecution. Such action would damage the Company's credibility and reputation as well as potentially resulting in significant legal costs.

6. Exclusions

a. Software written by Company staff where the Company owns the intellectual property rights.
b. Software purchased as part of equipment purchases.
c. Freeware, Shareware and Public Domain Software
d. Mobile apps purchased for use on a particular tablet or smart phone device

7. Changes

Changes to the Software Regulations are subject to IT Procedures and require the approval of the IT Department

8. Particulars

The Software Regulations outline the required framework for acquisition, registration and installation of all software controlled and used by, or on behalf of, the Company and its departments.

9. Approval of Software Purchase

a) All software purchases must be approved by the CIO prior to purchase. This enables software to be tested to ensure it is fit for use and compatible with other systems currently in use within the Company. It also ensures that the software effectively supports the user needs within the constraints of Company Policy, License conditions and total cost of ownership.
b) In granting approval to purchase specific consideration must also be given to compliance with the Software Management Policy and in particular:
   - whether the software incorporates adequate security controls for its intended purpose;
   - whether the proposed software is known to have any outstanding security vulnerabilities or issues;
   - the need for assurances that suppliers will provide updates to correct any serious security vulnerabilities discovered in the future;
   - the need to enter into a software escrow agreement for mission-critical applications.

c) IT department will only provide support for software that has been acquired in accordance with the Software Regulations.
d) The support level for a specific piece of software will be agreed when approval for the software purchase is granted. This will be a sliding scale of support from full support including installation, supporting infrastructure and training.
e) Software purchased personally must not be installed on equipment purchased using Company funds. Exceptions to this rule must be approved by CIO.

10.Registration of Software

a. All software installation media will be stored by IT Department. If staff are in possession of software they must ensure that it is passed to IT department without delay.
b. IT Department must complete the registration and inventory requirements for all software including completing registration details and returning these to the supplier. All software must be registered in the name of the Company. A copy of all license agreements (electronic or hard copy) must be held by IT Department.
c. Manuals, tutorials and other user materials should be made available to the users.

d. IT Department will maintain software asset register and record the software assets the Company holds. This will be a register of all software assets, including application software, system software, development tools and utilities.

e. The minimum detail that must be documented within the register is:
   - Detailed description of the software
   - Date and source of software acquisition
   - Asset number of each hardware item on to which each copy is installed
   - Reference to install location within Definitive Software Library (DSL)
   - Software product serial or licence number(s)
   - Details of any upgrades or modifications applied to the software
   - Where the software is applied to third parties as part of a contract, the contract details and if appropriate the validity period
   - Record of media storage location
   - The party responsible for maintaining the software who has accepted the responsibility

11. Installation of Software

a) Software installation will be carried out by IT department unless an end User has been granted enhanced privileges. In this case the User takes on the responsibilities.
b) A User may request enhanced privileges by submitting a case to the IT Head or a Software Approver. Where such requests are granted, the User will sign that they accept the responsibilities for software installation, registration and maintenance.
c) Where Software is installed for evaluation purposes this must be carried out in line with any license restrictions, with IT evaluation carried out by the IT Department and functional evaluation by the User. Once the evaluation is passed the software should then be approved for purchase by the Top Management and registered.
d) Once evaluated no software will be installed for use without it having first been recorded on the Company software asset register and without clear proof of license. Installation will then be authorized and the software deployed using the most efficient method. Following installation, the designated installer will ensure that the Software Asset Register is updated to reflect the usage of the software.

12. Software Maintenance

a. Software must be actively maintained to ensure that all fixes and patches, needed to avoid significant emerging security risks, are applied as promptly as possible.
b. Systems running software, including the operating system, which are clearly not being maintained adequately and which may be presenting a wider risk to security are liable to have their Company network connectivity withdrawn. This decision may be made by the concerned IT Department personnel..

13. Removal or Transfer of Software

a) The Software Asset Register must be updated should software be removed or transferred; thus all removals or transfers must be undertaken either by IT department personnel unless an end User has been granted enhanced privileges. In this case the User takes on the responsibilities

b) Software must only be transferred between different computers in line with the software license agreement and these Regulations.
c) Software must be removed from any information processing equipment that is earmarked for disposal according to the Company's disposal policy. In most cases this will be via the Company's disposal vendor.

14. Monitoring

To monitor compliance with the Software Regulations, random audits will be carried out.

1. Objective

To establish and maintain policy for managing the software applications to protect the Company's information assets in a secure, reliable and cost-effective manner.

2. SCOPE

Applicable to all DBL Software applications

3. Policy

This information security policy document contains high-level descriptions of expectations and principles for managing software on DBL

Software is very important to the Company because it is used extensively to enhance, or enable, performance of many key activities. Software management decisions taken across the Company influence efficiency, economy and information security. This document is primarily concerned with security aspects of software management.

This document includes statements on:

- General software management principles
- Managing security risks relating to software
- Permitted, regulated and prohibited use of software

Definitions:

Software management - any procurement, development, installation, regulation, maintenance or removal of software that takes place on Company owned computers or computers permitted connection to Company networks.

4. General software management principles

a) All software, including operating systems and applications must be managed correctly.
b) There must be an identifiable individual or organization taking current responsibility for every item of software deployed.
c) Those responsible for software must monitor relevant sources of information which may alert them to a need to act in relation to new security vulnerabilities.
d) Software is to be patched as soon as possible to remove security vulnerabilities.
e) Staff involved in managing software must have experience, training or qualification commensurate with the importance of the software and risk levels involved. At the minimum all staff involved must be aware of, and proactive in managing, information security related risks associated with software. Company departments must support this policy by ensuring that permission and responsibility for systems and software management is delegated accordingly.
f) Company software management procedures must incorporate measures for controlling these information security risks:

    - Illegal use of software
    - Use for of software for illegal purposes
    - Software copyright infringement
    - Inadequate control over data access by software
    - Insecure software design, configuration or usage procedures

- Software network services vulnerable to attack
- Software causing operational problems to systems or network
- Untrusted mobile code, viruses, “Trojans”, worms and spyware

5. Managing security risks relating to software

5.1 Software procurement

- When business requirements for new systems or enhancements are being specified, the specification documents should describe any special or essential requirements for security controls.
- When software for use by the Company is being procured there must be an assessment of whether the software incorporates adequate security controls for its intended purpose.
- It must be investigated and taken into account whether proposed new software or upgrades are known to have outstanding security vulnerabilities or issues.
- At the time of software procurement, the basis of future support and the expected supported lifetime of the product should be established. It may be important to have assurance that manufacturers will provide updates to correct any serious security vulnerabilities discovered in future.
- Consideration should be given to software escrow for mission critical applications. In a software escrow agreement the software source code is deposited into an account held by a third party escrow agent. Escrow is typically requested by a software licensee to ensure maintenance of the software. The software source code is released to the licensee if the licensor fails to maintain and update the software as promised in the software license agreement.

5.2 Software development

- Software developed at the Company must be assessed for its potential to introduce information security risks and any such risks must be adequately addressed.
- Upgrades or other changes to locally developed software must be assessed in terms of whether they may introduce an increased risk to information security. Any risks identified must be suitably addressed.

5.3 Software modification

In-house customization of externally written software should be avoided where it may lead to future difficulty for the Company in obtaining external support. Only strictly controlled essential changes should be permitted and all changes made should be fully documented.

5.4. Software installation

- For each item of software managed by a department a master copy of any media, enabling codes and installation instruction must be stored safely in accordance with procedures.
- Software must not be put into user service on Company systems unless a department or group has assessed and committed to providing sufficient resourcing for its ongoing management. (Software applications and systems utilized by the Company vary widely in cost, relative importance, user numbers, complexity, maintenance requirements and code quality. These factors must be taken into account when evaluating the ongoing resourcing commitment that will be required.)

5.5. Software regulation

- Use of illegal software and using software for illegal activities could be construed to be gross misconduct.
- Use of software which tests or attempts to break Company system or network security is prohibited unless the Head of IT has been notified and given authorization.
- Use of software which causes operational problems that inconvenience others, or which makes demands on resources which are excessive or cannot be justified, may be prohibited or regulated.
- Software found on Company systems which incorporates malware of any type is liable to automated or manual removal or deactivation.

5.6 Software maintenance

- Change control procedures, with comprehensive audit trails, must be used for all changes or upgrades to software of importance. Where correct operation of the software is itself important, or of importance to a wider system, changes must be authorized and tested before being applied to the live environment.
- Software must be actively maintained to ensure that all fixes and patches, needed to avoid significant emerging security risks, are applied as promptly as possible.
- Changing software of critical importance that is in service may sometimes be judged too risky. For example the risk of something going wrong as a result of installing a patch may seem greater than the risk associated with not installing it. It is good software management practice to assess such risks, make an informed judgement and document the reason for the decision. When it is necessary to defer installing a security fix, a less risky way or time to proceed with the installation must be sought.
- Systems running software, including the operating system, which are clearly not being maintained adequately and which may be presenting a wider risk to security are liable to have their Company network connectivity withdrawn

5.7 Software removal

- Software that is not licence compliant must be brought into compliance promptly or uninstalled.
- Software that is known to be causing a serious security problem, which cannot be adequately mitigated, should be removed from service.
- Operating systems and application software must not be abandoned or otherwise left unmaintained for extended periods. Systems and application software that are no longer required should be decommissioned; where they will not be managed for an extended temporary period they should be removed from service.
- When decommissioning a computer system, for disposal or re-use, appropriate measures must be taken in relation to any software and data stored on it. Software must be removed, where not doing so could lead to breaking the terms of its licence

6. Permitted, regulated and prohibited use of software

The Company must comply with its overriding legal and contractual obligations.

IT Head has responsibility for IT at the Company and on behalf of the Company is permitted to regulate or prohibit use of particular software or types of software for the overall benefit of the Company

1. Objective

The objective of Clear Desk and Clear Screen Policy is to establish the guidelines to reduce the risks of unauthorized access, loss of and damage to information during and outside normal working hours for DBL information and information systems (operating systems, applications, databases, network equipment and others information handling systems – collectively "**IT Systems**") is implemented.

2. Scope

This Policy applies to DBL's IT Systems and all DBL information assets, including those in both electronic (e.g., information systems, applications, systems platforms, and computer operations) and physical (e.g., vendor contracts, loan documentation, client files, and personnel information) formats regardless of the location.

This policy applies to all employees, contractors, consultants, temporary workers and any person utilizing any form of DBL's information technology or having responsibility for institutional information stored in an alternate format, such as paper. This policy covers any papers, and any computing devices that contain or display DBL's information regardless of location.

3. Policy

A clear desk and clear screen policy reduce the risks of unauthorized access, loss of and damage to information during and outside normal working hours. DBL's Information Security Policy requires the protection of unauthorized access to sensitive data. Additionally, much of the DBL's data must be protected according to legal and contractual requirements.

The purpose of this policy is to establish acceptable and unacceptable use of computer screens and work desks at DBL in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

- Documents or folders must be saved in the C:\Users\<username/profile>\data folder. Laptop screen must not contain any document or folder.
- Employees need to lock the system if they leave their workstation more than 5 minutes.
- Do not keep any confidential information on the desk and the screen must have a password screen saver.
- Employees need to keep all documents in one drive / SharePoint
- Employee's In/Out logs are Accessed through facial HID.

Requirements

Whenever unattended or not in use, all computing devices must be left logged off or protected with a screen or keyboard locking mechanism controlled by a password or similar user authentication mechanism (this includes laptops, tablets, smartphones and desktops).

When viewing sensitive information on a screen, users should be aware of their surroundings and should ensure that third parties are not permitted to view the sensitive information.

Sensitive or critical business information, e.g. on paper or on electronic storage media, must be secured when not required, especially when the office is vacated at the end of the work day.

Paper containing sensitive or classified information must be removed from printers immediately. Printers used to print sensitive information should not be in public areas. Any time a document containing

sensitive information is being printed the user must make sure they know the proper printer is chosen and also go directly to the printer to retrieve the document.

Sensitive information on paper or electronic storage media that is to be shredded must not be left in unattended boxes or bins to be handled at a later time and must be secured until the time that they can be shredded.

Any papers containing sensitive or critical information should not be left on the desk/cubical unattended.

1. Objective

The Objective of this BYOD policy is to define the controls that need to be implemented and maintained to protect information assets against unauthorized access that poses substantial risk to the organization. The policy intends to establish adequate controls for using mobile devices at DBL.

2. Scope

This Policy applies to devices owned or provided by DBL with terms and conditions as per HR Policy

3. Policy

DBL grants some of its employees the privilege of using tablet computers, palmtops, mobiles, tablets, etc at work for marketing purposes. DBL reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of DBL's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

DBL employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

Acceptable Use

- The company defines acceptable business use as activities that directly or indirectly support the business of DBL.
- The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.
- Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the company. Such websites include, but are not limited to social networking sites, job portals, any sites considered illegal.
- Devices' camera and/or video capabilities are not disabled while on-site.
- Devices may not be used at any time to:
    - Store or transmit illicit materials
    - Store or transmit proprietary information belonging to another company
    - Harass others
    - Engage in outside business activities
- The following apps are allowed: (include a detailed list of apps, such as weather, productivity apps, Facebook, etc., which will be permitted)
- The following apps are not allowed:
  (apps not downloaded through iTunes or Google Play, etc.)
- Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc.
- DBL has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

Devices and Support

- Smartphones including iPhone, Android, Blackberry and Windows phones are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.).
- Tablets including iPad and Android are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.).
- Connectivity issues are supported by IT; employees should/should not contact the device manufacturer or their carrier for operating system or hardware-related issues.

- Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

Reimbursement

- The company will be procuring the device as per HR Policies.
- The company will
  a) pay the employee an allowance,
  b) cover the cost of the entire phone/data plan,
  c) pay half of the phone/data plan, etc.
- The company will/will not reimburse the employee for the following charges: roaming, plan overages, etc.

Security

- In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network.
- The company's Password Policy must be followed.
- The device must lock itself with a password or PIN if it's idle for one minutes.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Employees are automatically prevented from downloading, installing and using any app that does not appear on the company's list of approved apps.
- Smartphones and tablets that are not on the company's list of supported devices are/are not allowed to connect to the network.
- Smartphones and tablets belonging to employees that are for personal use only are/are not allowed to connect to the network.
- Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.
- The employee's device will be remotely wiped if

  a) The device is lost,
  b) The employee terminates his or her employment,
  c) IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure

Risks/Liabilities/Disclaimers

- While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- The company reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to the company within **24** hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- DBL reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

1. Objective

This policy is to ensure the confidentiality, authenticity / integrity, and availability of the information by applying appropriate levels of cryptographic controls. The encryption technique is applied to ensure the security for critical removable media, laptop hard-drives, portable devices, mobiles, and remote access should be allowed to the terminal services, and Wi-Fi protected encryption is mandatory for all the wireless networks.

2. Scope

The scope of this procedure is establishing keying techniques which are applicable to protect physical and data access at DBL premises and the information assets. If any unauthorized access or breach of the information security management system, it should be reported to IT Team and the respective incidents will be recorded and reported.

3. Policy

At DBL, policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.

Key management is a set of techniques and procedures for establishing and maintaining keying authorized party.

At DBL, the objective of Key management is to establish key relationship of keying material in a manner that counters relevant threats.

The objectives of Key management are

- Supporting the users with an existing domain.
- Generating distribution and installation of keying.
- Controlling set of Keying material.
- Storage backup and archival of Keying.

The key management techniques are

- Symmetric.
- Key Encryption.
- Public Key Encryption.
- Accessed through facial HID.

1. Objective

In the dynamic landscape of IT operations, maintaining the security and integrity of data is paramount. Data leakage policy ensures a robust mechanism w.r.t data to be controlled, monitored, and tracked to mitigate risks and vulnerabilities.

2. Scope

This Policy applies to DBL' IT Systems and all DBL information assets, including those in both electronic (e.g., information systems, applications, systems platforms, and computer operations) and physical (e.g., vendor contracts, loan documentation, client files, and personnel information) formats regardless of the location.

3. Policy

Data Leakage Prevention: Security Policy for IT Department: In an era of heightened data security concerns, the prevention of data leakage is a top priority for IT Team. This document outlines the strategic approach we adopt to mitigate data leakage risks, focusing on the implementation of key tools such as Microsoft Intune, as well as from our roadmap and examples of implementations like Data Leakage Prevention (DLP) and Privileged Access Management (PAM).

Implementation of Microsoft Intune: One of the cornerstones of our data leakage prevention strategy is the use of Microsoft Intune. This versatile tool empowers us to manage PCs, and applications, enabling us to enforce security policies and configurations across our IT ecosystem. By implementing Intune, we can achieve the following:

- Device Management: Intune allows us to configure and secure devices, ensuring they meet the required security standards before accessing sensitive data.
- Application Control: We can manage application access and permissions, preventing unauthorized apps from accessing confidential information.
- Data Encryption: Intune enables us to encrypt data on devices, safeguarding it from potential breaches.

Handling Data Leakage: In our commitment to data leakage prevention, we have established stringent procedures:

- Access Control: Access to sensitive data is restricted based on role-based permissions. Users are granted access only to the data necessary for their tasks.
- Monitoring and Auditing: We employ advanced monitoring tools to track data movement and access patterns. Suspicious activities trigger alerts for immediate investigation.
- Encryption: Confidential data is encrypted both at rest and in transit. This prevents unauthorized access even if the data is compromised.
- Employee Training: Through training programs, email form IT Helpdesk, and new letters we raise awareness about all areas related to IT security such as threat intelligence, cloud services, planned BCP drills, data leakage risks and best practices for preventing inadvertent breaches.

- IT Team Roadmap Implementations: IT team operates under a proactive roadmap that anticipates security challenges and adopts measures to counteract them. A few examples of implementations within this roadmap include:

    - Data Leakage Prevention (DLP): We plan to implement DLP policies to identify and prevent the unauthorized sharing of sensitive data. This involves monitoring data flow across networks, endpoints, and cloud environments.
    - Privileged Access Management (PAM): To mitigate insider threats, we plan to employ PAM solutions to control and monitor access to critical systems and sensitive data. This minimizes the risk of unauthorized access.

1. Objective

The purpose of this Data Masking policy is to use data masking as a technique to protect sensitive data by obscuring or replacing the original data with fictitious but realistic data. At DBL data masking will be applied to various types of data, including text, numbers, and dates, and will be done using a variety of methods, such as encryption, substitution, and redaction.

2. Scope

This Policy applies to DBL's IT Systems and all DBL information assets, including those in both electronic (e.g., information systems, applications, systems platforms, and computer operations) and physical (e.g., vendor contracts, loan documentation, client files, and personnel information) formats regardless of the location.

3. Policy

a. Data masking technique will be used to protect sensitive data – usually any data that could be deemed personally identifiable information (PII) – over and above an organization's standard information security protocols such as access control etc.
b. Data masking is a complex technical process that involves altering sensitive information and preventing users from identifying data subjects through a variety of measures.
c. At DBL data masking will be done through two main technique pseudonymization and/or anonymization. Both of these methods are designed to disguise the true purpose of PII through disassociation – i.e. hiding the link between the raw data, and the subject (usually a person).
d. As an organization DBL will take great care to ensure that no single piece of data compromises the subject's identity.
e. When using either of these techniques, organization will should consider:
    - The level of pseudonymization and/or anonymization required, relative to the nature of the data.
    - How the masked data is being accessed.
    - Any binding agreements that restrict use of the data to be masked.
    - Keeping the masked data separate from any other data types, to prevent the data subject being easily identified.
    - Logging when the data was received, and how it has been provided to any internal or external sources.
f. Other methods that can be used to bolster data security (will be implemented as scope):
    - Key-based encryption.
    - Voiding or deleting characters within the dataset.
    - Varying numbers and dates.
    - Replacing values across the data.
    - Hash-based value masking

Data Masking Principals

a) Data masking is an important part of an organization policy towards protecting PII and safeguarding the identity of the individuals whom it holds data on.

b) As well as the above techniques, organization should consider the below suggestions when strategizing their approach to data masking:

    - Implement masking techniques that only reveal the minimum amount of data to anyone who uses it.

- 'Obfuscating' (hiding) certain pieces of data at the request of the subject, and only allowing certain members of staff to access the sections that are relevant to them.
- Building their data masking operation around specific legal and regulatory guidelines.
- Where pseudonymization is implemented, the algorithm that is used to 'de-mask' the data is kept safe and secure.

1.Objective

DBL recognizes that the efficient management of its many different data records (including personally identifiable data records) is essential to ensure full compliance with all applicable legislative, regulatory, and contractual obligations. This Data Retention Policy will also contribute to the effective overall management of all data processing activities within DBL.

2. Scope

This Policy applies to DBL's IT Systems and all DBL information assets, including those in both electronic (e.g., information systems, applications, systems platforms, and computer operations) and physical (e.g., vendor contracts, loan documentation, client files, and personnel information) formats regardless of the location.

3. Policy

3.1 General

"Records" shall be defined as any evidential material which supports DBL in management and delivery of its various organizational functions. Once data records have been created, or have otherwise passed into the control of DBL, they must be securely retained for a pre-defined period (as per the DBL Data Retention Schedule) to provide evidence of the completed activity. It is acknowledged that data records are likely to exist in hard-copy or in a variety of electronic formats.

Dependent on the specific data processing activities being undertaken, and in line with applicable legislation or regulations, certain records may be identified as having a requirement to be permanently archived, or subject to subsequent statistical analysis or historical research purposes.

The DBL Data Retention Policy has been compiled with reference to:

- Applicable legislative and regulatory requirements identified by DBL
- Documented contractual requirements from DBL's customers and stakeholders

3.2 Data Retention

DBL shall:

Ensure that it maintains complete and accurate inventory of all the data it holds, including its format, location, any special considerations or handling requirements, and the legal basis under which it is being held (where applicable). All new data record types shall be promptly classified and recorded within the inventory upon their first discovery.

Ensure that it identifies and understands the retention period for each category of data being held and has communicated this to all employees, contractors, and any other interested parties. Data retention periods shall adhere to the principle of data minimization, which ensures that data is only retained for as long as is necessary to deliver the declared purpose.

Specify data retention periods, with full consideration being given to (a) legislative, regulatory, or contractual requirements, (b) value of the data concerned, (c) costs, risks and liabilities associated with its retention, and (d) ease or difficulty of making sure that the information remains both accurate and current.

Ensure that any person identifying data records which have been retained for longer than their declared retention period, and which do not have a valid justification for their continued retention, shall notify DBL immediately so that the matter can be promptly investigated and resolved.

Consider, when a lengthy retention period has been identified by DBL, how the data is to be securely stored in the most appropriate way to preserve its integrity and minimize physical storage space – e.g. it may be beneficial to scan large quantities of paper records onto digital media. The stability and longevity of any digital media selected by the DBL, as well as the availability of technical resources needed to create and retrieve the contents, shall be fully assessed in advance to ensure that the required retention periods can be achieved.

Carefully check, where data is being passed into or out of DBL's possession, that this is only undertaken having determined any periods of retention which have already passed and how this information is to be communicated or accommodated.

Ensure that all data which is held shall be afforded appropriate levels of physical and technical protection, as specified within the DBL's security policies and related documentation. All employees shall be provided with training to ensure that they understand information security, data protection and data retention requirements, and their role in supporting them.

3.3 **Data Disposal**

Once data records have been identified as requiring disposal, they shall be promptly destroyed in a secure and permanent manner. All paper records, regardless of any protective markings or sensitivity notices they carry, shall be destroyed using a cross-cut shredder.

Electronic records shall be permanently erased using acceptable technology which has the capability to prevent the data's subsequent recovery. This shall typically be by selecting and using appropriate data destruction software tools, or alternatively may require the physical destruction of the hardware asset (e.g. hard drives or backup media) which contains the data.

Records of the disposal activity, whether arising from shredding, physical destruction, or technical means, shall be maintained to demonstrate compliance with this Data Retention Policy and the applicable legislative, regulatory, or contractual requirements. Such records shall identify the individual who authorized and/or undertook the disposal activity.

Where an individual data subject has requested that their personal data is deleted, then DBL shall retain supporting records to validate that the erasure activity has indeed taken place within the specified timeframe.

3.4 General Guidelines

Data Classification: Data should be classified based on its sensitivity and importance. Categories may include "Restricted," "Confidential," "Internal," and "Public."

Data Retention Periods: Define data retention periods for each data category based on legal, regulatory, and business requirements. Retention periods should consider the purpose of data collection and the organization's operational needs.

Data Access Controls:

Implement access controls to ensure that only authorized individuals have access to data, especially data with longer retention periods. Use role-based access control (RBAC) and enforce the principle of least privilege.

Backup and Archive Retention: Determine how long backups and archives are retained, considering their purpose and data retention requirements. Ensure that data subject to legal holds or investigations is not prematurely deleted.

Data Subject Rights:

Ensure compliance with data subject rights, including the right to access, rectify, delete, or restrict the processing of their data. Implement procedures for handling data subject requests related to data retention.

Legal Holds and Litigation Holds:

Establish procedures for identifying and suspending data disposal in cases of legal holds, pending litigation, or regulatory investigations.

Compliance and Reporting: Maintain records of data retention activities, including disposal and legal hold processes, and generate compliance reports to demonstrate adherence to data retention requirements.

1. Objective

The purpose of this policy is to make users aware of the usage of the information deletion: disposal and destruction policy implemented by the DBL.

2. Scope

This Policy applies to DBL's IT Systems and all DBL information assets, including those in both electronic (e.g., information systems, applications, systems platforms, and computer operations) and physical (e.g., vendor contracts, loan documentation, client files, and personnel information) formats regardless of the location.

This policy is applicable to organizational-wide information deletion, disposal, and destruction. It describes how disposal of hardware we will handle in future, answer questions from Pollution Control Board during audit / review w.r.t disposal of hardware devices, scrap management for hardware, policy followed for deletion of the information of an employee who exits the company or changes project / department.

3.Policy

a) In our commitment to maintaining data security and environmental responsibility, we have established a comprehensive Information Disposal and Destruction Policy. This policy encompasses the disposal of both digital media and hardware devices while addressing potential inquiries from regulatory bodies such as the Pollution Control Board during audits or reviews.

b) Digital Media Disposal:
   - Data Sanitization: Before disposal, all digital media (e.g., hard drives, solid-state drives, USB drives) will undergo thorough data sanitization using industry-standard methods. This includes secure data erasure or physical destruction as appropriate.
   - Verification: The effectiveness of data sanitization will be verified through audits and checks to ensure that no recoverable data remains.

c) Hardware Disposal:
   - Environmental Compliance: All hardware disposal will strictly adhere to local and national regulations, including those set forth by the Pollution Control Board. Our organization is committed to minimizing the environmental impact of hardware disposal.
   - E-Waste Management: Hardware that is no longer usable will be categorized as electronic waste (e-waste) and handled in accordance with authorized e-waste recyclers. This includes devices such as computers, monitors, printers, and other electronic equipment.
   - Documentation: Detailed records of hardware disposal, including dates, methods, and relevant regulatory approvals, will be maintained to provide evidence of compliance during audits or reviews.

d) Addressing Pollution Control Board Inquiries: Our organization is prepared to address questions related to hardware disposal.
   - Regulatory Compliance: We provide documentation demonstrating our adherence to e-waste regulations and guidelines set by the Pollution Control Board.
   - Authorized Partnerships: Details of our partnerships with authorized e-waste recyclers will be presented, highlighting our commitment to responsible hardware disposal.
   - Environmental Impact Mitigation: We implement measures to minimize the environmental impact of hardware disposal, including proper recycling, material reclamation, and pollution prevention.

- **Documentation Access:**

  Relevant disposal records and certifications will be made available for review to showcase our transparent approach to hardware disposal. Project teams maintain information security plan which details the implementation of information security policies and procedures defined at DBL.

e) Information Deletion w.r.t Employee
   - Effective management of employee information is crucial for organizations to maintain data integrity and comply with privacy regulations. When an employee leaves the organization, a structured information deletion process should be in place to safeguard sensitive data. This process typically involves removing access to company systems, revoking credentials, and deleting or archiving relevant records. In DBL we will follow the below two conditions for Information deletion.

f) Exits the Company
   - The HR Team will send a formal email to the IT Team anytime a user leaves the company. As soon as we have the email, we will notify the reporting manager of the departing user via email that any information from his email or One Drive, etc., is needed if needed, we will take a backup of the employee's information and forward it to his/her manager. if we hear back from the manager about the information. if not, we will erase the employee's data and terminate their access.

1. Objective

The purpose of this policy is to establish a standard for creation of strong passwords, protection of those passwords, and frequency of change. It also describes what guidelines to be followed while creating the passwords.

2. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any DBL facility which has access to the DBL network or stores any non-public DBL information. Service accounts that are used to support and manage infrastructure are excluded from this.

3. Policy

3.1 General

a) All system-level passwords (e.g., root, NT admin, application administration accounts, etc.) must be changed quarterly**.**

b) All user-level passwords (e.g., email, web, etc.) must be changed at least every quarter. For laptops password should change for every 90 days and 5 days prior intimation is given to users.

c) User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.

d) All user-level and system-level passwords must conform to the best practices described below.

3.2 Best Practices

1) Passwords should not be written down, emailed or spoken.
2) Passwords must be kept confidential and not shared with colleagues. This does not apply to generic departmental passwords, where a group manages the password.
3) Your username or variations of the username should not be embedded in your password.
4) Passwords must not be blank.
5) Passwords should not be typed or saved in electronic documents.
6) Passwords must not be based on personal information (e.g. names of families, Date of Birth, pets, and name of your street, car registration numbers, and telephone numbers).
7) Passwords must not be revealed to your manager.
8) Passwords must not be revealed to anyone over the phone even if the recipient is a member of a group.
9) Passwords must not include words from a dictionary in any language.
10) Passwords must not be included in any automated login process.
11) New passwords must not bear any relation to the old. For instance, if the old password is August, the new password must not be August1 or 1gustAu or any variation of August.
12) Once passwords have been changed by IT Team, new password must be created immediately by user.
13) Passwords must be unique from 3 previous passwords. The previous passwords should not be re-used.

3.3 Password Composition

Passwords must meet the following criteria:

- Passwords must be at least eight characters long.
- Password must have at least one capital letter and one numeric.
- Passwords must be composed of alphanumeric characters (alphabets – A..Z, a...z and numbers – base 10 digits – 0..9) and must include special characters (e.g. !; £; $;); (; %; &; *; #; @; ?; {; }; [;]; =; +; >; <; “;). ex: august@123 or @ugust123

Here are some methods for making strong passwords:

- You can choose one or two lines from a poem or song and use the first letter of each word. For example, ‘Always look on the bright side of life becomes alotbsol
- Passwords are case sensitive: using the above example, the passwords alotbsol, AlotbsoL and aLotBsol are different and the security of passwords can be increased if mixed case passwords are used.
- One strategy for creating strong passwords is to replace letters with numbers or characters. For example, Alotbsol becomes A10tbs01 where the letter “l” has been replaced with the digit “1” and the letter “o” has been replaced with the digit ‘0’.
- Choose a minimum of two short unrelated words and concatenate them together with special symbols or numbers. For example, awn, crat, it is three unrelated words which become awn+crat=it? When the words are joined together.

3.4 System based Password Requirements

Privileged and administrative passwords must be subject to stringent composition and frequency of change. Privilege passwords include passwords of root account for routers, switches, firewalls, network operating systems, office 365 and Servers

1. Objective

The purpose of this is to manage Information Security within the organization during development for internal use or as part of development activities performed for the client. Security requirements of development and support processes, and covers issues such as system change control procedures, outsourced development, and system security testing.

2. Scope

This Policy applies to DBL' IT Systems and all DBL information assets, including those in both electronic (e.g., information systems, applications, systems platforms, and computer operations) and physical (e.g., vendor contracts, loan documentation, client files, and personnel information) formats regardless of the location.

3. Policy

a) A secure development policy is a set of rules and best practices that help organizations mitigate the risk of security vulnerabilities in development environments and to ensure the secure development of software– i.e., the virtual workspaces where organizations make changes to software and web applications without affecting the live product or page.
b) Secure development policy establishes guidelines and best practices for secure development, ensuring that all software development activities prioritize security at every stage.
c) The primary goal of a Secure Development Policy is to embed security measures throughout the software development lifecycle, from the initial design phase to deployment and maintenance. This helps in identifying security vulnerabilities early in the development process and mitigate the risk of security breaches and data compromises.
d) As part of secure development practices, DBL Engineering teams shall ensure that:

- Define security requirements of all projects and standards that all engineers should adhere to
- Define secure design principles to be used.
- Define secure coding, review, and deployment standards.
- Define how to react when security vulnerability is identified in the project.
- Development & test environment shall be protected as per IT controls.
- Development & test environment shall be separated from each other.
- Only baselined versions of software should be installed for the test environment.
- Only authorized personnel shall install the baselined versions.
- Outsourcing partner personnel shall not install the software baselined versions.
- Access permissions shall be granted to project team members only after a business justification is provided by Delivery Manager or BU Head.
- Every software project shall define and maintain a Project Information Security Plan.
- IT team shall perform vulnerability assessment of all nodes. If any vulnerability is identified, analysis shall include the actions to assess the risks and decide for treatment.
- Software configuration management shall be planned and performed for every software project.

e) The secure development activities include:

- Adherence to security requirements as stated in project scope / requirements.
- Software design shall address IS requirements.
- Source code review shall be performed applying suitable sampling criteria to ensure that information security features are designed and implemented in the code.

- QA team shall perform the IS requirements as needed.
    - Development team to follow secure coding standards related to Microsoft, Java, IOS, Mobile or related technology.
- Under service management projects, the information security of any live data or test data shall be protected.
- IT shall also ensure that the requirements under supplier agreement (ex. AWS) for the projects are met. IT shall report any security breach or weakness to the supplier.
- Access permissions for the service management team shall be supervised by IT Manager.
- All related ISMS policies shall be adhered to by the Engineering team members.
- Whenever any security breach/ weakness is observed, IT Team / IT Manager shall be immediately informed.
- Continuous improvement plan to be defined based on incidents and update the plan as per need. It could be updated either in the project management plan or project information security plan.

1. Objective

The purpose of this policy is to provide a framework within which DBL information accessed by suppliers is safeguarded and that information security is considered as key in supplier agreements and contracts.

2. Scope

This policy applies to all suppliers associated with DBL, IT Systems and all DBL information assets, including those in both electronic (e.g., information systems, applications, systems platforms, and computer operations) and physical (e.g., vendor contracts, loan documentation, client files, and personnel information) formats regardless of the location.

3. Policy

3.1 Information Security in Supplier Relationship

3.1.1 Information Security Policy for Suppliers

- Information security requirements for mitigating the risks associated with supplier's access to DBL assets shall be agreed with the supplier and documented in the form of agreements or contracts;
- DBL shall identify and mandate information security controls to specifically address third party/ vendor/ supplier access to the information in the policy;
- Suppliers/ third parties like IT services, HR services, logistics utilities, and IT infrastructure components shall be identified.
- Resilience and, if necessary, recovery and contingency arrangements to ensure the availability of the information or information processing provided by either party shall be defined.

3.1.2 Addressing Security within Supplier Agreements

a) All agreements with Contract Partner that access, process, communicate or manage DBL information or information processing facilities, or provide products or services shall have relevant security requirements embedded in them;
b) DBL shall ensure that suitable agreement clauses include the following but not limited to:
   - Clear definition of supplier/vendor responsibilities;
   - Description of product/service being provided;
   - Adherence to relevant sections of DBL Information Security Policies and Procedures;
   - Arrangements for reporting, notifying and investigating information security incidents if any through any channel (Oral / Mail / Tool);
   - Agreed service levels and performance monitoring and reporting criteria;
   - Escalation procedures for problem resolution;
   - Creating awareness among supplier/vendor employees and contract staff regarding relevant sections of Information Security Policies and Procedures;
   - Conditions for termination, re-negotiation of agreements;
   - Provisions for ensuring that applicable legal, contractual and immigration requirements are met;
   - Service continuity and availability requirements;
   - Independent assurance, i.e. the right to audit responsibilities defined in the agreement, to have those audits carried out by DBL management or supplier/vendor identified by the DBL;
   - Providing confirmation to DBL that background verification has been performed for all contractors and supplier/vendor personnel having access to information;
   - Defining and clearly communicating security roles and responsibilities of contractors and supplier/vendor staff;
   - Restricting access to sensitive information;

- Requirements for involvement of the supplier/vendor with subcontractors, and the security controls these subcontractors need to implement.

3.1.3 Information and Communication Technology Supply Chain

- All agreements with the vendors/contractors will include details on the DBL Information security requirements that they need to comply with
- The contractors and sub-contractors need to abide by the clauses that they have agreed with DBL
- DBL will ensure that NDA's have been signed with all the vendors

3.2 Supplier Service Delivery Management

3.2.1 Monitoring and Review of Supplier Services

- Service reports and evidences provided by the third parties shall be reviewed at regular intervals;
- Review of third-party audit trails and records of security incidents, operational problems, failures, fault logging and disruptions shall be done regularly; and
- Key Performance Indicator (KPI) framework shall be defined for monitoring effectiveness of Information Security. Depending on the nature of engagement with the Supplier, following shall be agreed with the Supplier to monitor Information Security effectiveness and ensure compliance to Information Security terms and conditions within agreements:
  - Reports and Key Performance Indicators (KPIs) to be shared by the Supplier; and
  - Frequency of sharing agreed reports and KPIs.
- Periodic audits / Reviews for critical vendors shall be carried out to ensure compliance to Information Security terms and conditions within agreements with the supplier;
- Supplier operations shall be monitored through a security governance program including all the above aspects.

3.2.2 Managing Changes to Supplier Services

- Significant changes to supplier services (e.g. enhancement to networks, new technologies, new products or newer versions, change of vendors, change of physical location etc.) shall be informed to the IT team;
- Such changes shall:
  - Take into account criticality of business systems and processes involved; and
  - Be accompanied by re-assessment of risks.

---END--