# INFORMATION TECHNOLOGY / INFORMATION SECURITY POLICY

# OF

# WELKIN COMMERCIALS PRIVATE LIMITED

# SUMMARY OF THE POLICY

| | |
|---|---|
| **Document Name** | Information Security Policy |
| **Issue and Effective Date** | 22/04/2025 |
| **Date of Next Review** | 21/04/2026 |
| **Periodicity of Review** | Annual |
| **Owner/Contact** | IT Department |
| **Approver** | Board of Directors |
| **Annexure** | - |

# TABLE OF CONTENTS

## 1. INTRODUCTION

This Policy shall be termed as IT Framework and security Policy of **WELKIN COMMERCIALS PRIVATE LIMITED ("The Company" or "Welkin").** The terms in this policy shall be considered as defined by the Reserve Bank of India in its Master Direction on NBFC-Scale Based Regulation,2023 (DoR.FIN.REC.No. 45/03.10.119/2023-24 dated Oct 19, 2023 and DoS.CO.CSITEG/SEC.7/31.01.015/2023-24 dated November 7, 2023

These Guidelines aim to enhance safety, security, efficiency in processes leading to benefits for NBFCs and their customers. NBFCs, pursuant to these Guidelines, are required to conduct a formal gap analysis between their present status and stipulations as set out in the Guidelines and put in place a time-bound action plan to address the gap.

This IT Framework falls within the scope of Section B of the Guidelines i.e. NBFCs with asset size of below INR 500 crores (Indian Rupees Five Hundred Crores only).

IT governance is an integral part of the corporate governance of **Welkin** and effective IT governance is the responsibility of the Board of Directors of **Welkin** ("Board") and its Executive Management.

**Welkin** Designated a Senior level executive as the **Chief Technical Officer (CTO)** who is heading the complete IT department and responsible for the effective implementation of IT Policy involving IT strategy, value delivery, risk management, and IT resource management. To ensure technical competence, periodic assessments should be formulated to ensure that sufficient, competent, and capable human resources are available. The board of directors exercises oversight over the **Chief Technical Officer (CTO).**

The CTO will also ensure implementation of this IT Framework which, inter alia, includes

(i) Security aspects;

(ii) User Role;

(iii) Information Security and Cyber Security;

(iv) Business Continuity Planning Policy;

(v) Back-up Data.

For the purpose of effective implementation of this IT Framework, the CTO shall ensure technical competence at senior/middle level management of **Welkin**. The CTO is also responsible for periodic assessment of the IT training requirements to ensure the availability of sufficient, competent and capable human resources in "**Welkin**".

## 2. SECURITY STANDARDS

Adopting new technology exposes the business to the risk of unauthorized access of data. Unavailability of technology support may lead to a breakdown in business. With this, users & customers must have confidence that the information system will operate without unanticipated failures or problems. This will ensure that technology is optimally utilized and IT enhances future growth.

The company implements basic security standards - such as physical/logical access controls and a well-defined password policy.

**Here are the following basic creeds of the board-approved IT Policy–**

1. **Confidentiality –** Ensuring access to sensitive data to authorised users only;
2. **Integrity –** Ensuring accuracy and reliability of information by ensuring that there is no modification without authorization;
3. **Availability –** Ensuring that uninterrupted data is available to users as and when required;
4. **Authenticity –** It is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine for information security.

## 3. SECURITY ASPECTS

1. **Password Policy**

All users are responsible for keeping their passwords secure and confidential. The password credentials of the users must comply with the password parameters ("Complexity Requirements") and standards laid down in this IT Framework. Passwords must not be shared with or made available to anyone in any manner that is not consistent with this IT Framework.

The Complexity Requirements for setting passwords are as follows:

- A strong password must be at least 8 (Eight) characters long.
- It should not contain any of the user's personal information—specifically his/her real name, user name, or even company name.
- It must be very unique from the passwords used previously by the users.
- It should contain characters from the four primary categories i.e. uppercase letters, lowercase letters, numbers, and characters.
- To ensure that a compromised password is not misused on a long-term basis, users are encouraged to change the password every 90 (Ninety) days.
- Passwords must not be stored in readable form in computers without access control systems or in other locations where unauthorized persons might discover them.
- Passwords must not be written down and left in a place where unauthorized persons might discover them. Immediately upon assignment of the initial password and in case of password "reset" situations, the password must be immediately changed by the user to ensure confidentiality of all information.
- Under no circumstances, the users shall use another user's account or password without proper authorization.
- Under no circumstances, should the user share his/her password(s) with another user(s), unless the said user has obtained from the concerned branch manager/IT head the necessary approval in this regard. In cases where the password(s) is shared in accordance with the above, the user shall be responsible for changing the said password(s) immediately upon the completion of the task for which the password was shared.

2. **Access Controls**

- Access to the **Welkin's** electronic information and information systems, and the facilities where they are housed, is a privilege that may be monitored and revoked without notification. Additionally, all access is governed by law and **Welkin's** policies including but not limited to requirements laid down in this policy.

- Persons or entities with access to **Welkin's** electronic information and information systems are accountable for all activities associated with their user credentials. They are responsible to protect the confidentiality, integrity, and availability of information collected, processed, transmitted, stored, or transmitted by **Welkin's**, irrespective of the medium on which the information resides.
- Access must be granted on the basis of least privilege - only to resources required by the current role and responsibilities of the person.
- Requirements:

  a. All users must use a unique ID to access **Welkin's** systems and applications.

  b. Alternative authentication mechanisms that do not rely on a unique ID and password must be formally approved.

  c. Remote access to **Welkin's** systems and applications must use a two-factor authentication where possible

  d. System and application sessions must automatically lock after 10 (Ten) minutes of inactivity.

Our Information Security Policy shall ensure the following:

- Confidentiality, integrity and availability of information across the company.
- Protection of all data from unauthorised physical and logical access.
- Protection of information from fraud, corruption or loss during input, processing, transmission and storage.

- Protection of critical information to ensure continuation of its day-to-day operations with minimal breakdowns.
- Educating its users to ensure that they comply with relevant legislation relating to the maintenance, protection, retention and withholding of information.
- Appropriate management of Information Security related incidents.

## 4. INFORMATION SECURITY AND CYBER SECURITY

### 1. Information Security:

**Welkin** has an information security framework with the following principles:

- **Identification and classification of information assets: Welkin** maintains detailed inventory of information assets with distinct and clear identification of the asset.
- **Functions**: The information security function is adequately resourced in terms of the number of staff, level of skill and tools or techniques like risk assessment, security architecture, vulnerability assessment, forensic assessment, etc. Further, there is a clear segregation of responsibilities relating to system administration, database administration and transaction processing.
- **Role based access control** – Access to information is based on well-defined user roles (system administrator, user manager, application owner.) **Welkin** has a clear delegation of authority to upgrade/change user profiles and permissions and also key business parameters.
- **Personnel Security** - A few authorized application owners/users may have intimate knowledge of financial institution processes and they pose a potential threat to systems and data. **Welkin** has a process of appropriate checks and balances to avoid any such threat to its systems and data. Personnel with privileged access like system administrator, cyber security personnel, etc are subject to rigorous background checks and screening.
- **Physical Security** - The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. **Welkin** has created a secured environment for physical security of information assets such as secure location of critical data, restricted access to

sensitive areas like data centers etc. and has further obtained adequate insurance to safeguard such data.

- **Maker-checker –** Maker checker is one of the important principles of authorization in the information systems of financial entities. It means that for each transaction, there are at least two individuals necessary for its completion as this will reduce the risk of error and will ensure the reliability of the information. **Welkin** ensures that it complies with this requirement to carry out all its business operations.
- **Audit Trails - Welkin** ensures that audit trails exist for IT assets satisfying its business requirements including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required and assisting in dispute resolution. If an employee, for instance, attempts to access an unauthorized section, this improper activity is recorded in the audit trail.
- **Mobile Financial Services – Welkin** has a mechanism for safeguarding information assets that are used by mobile applications to provide services to customers. The technology used by **Welkin** for mobile services ensures confidentiality, integrity and authenticity and provides for end-to- end encryption.
- **Social Media Risks – Welkin** uses social media to market their products and is well equipped in handling social media risks and threats in order to avoid any account takeover or malware distribution. **Welkin** further ensures proper controls such as encryption and secure connections to mitigate such risks.
- **Digital Signatures** - A Digital signature certificate authenticates an entity's identity electronically. **Welkin** protects the authenticity and integrity of important electronic documents and also for high value fund transfer.
- **Regulatory Returns – Welkin** has adequate systems and formats to file regulatory returns to the RBI on a periodic basis. Filing of regulatory returns is managed and verified by the authorized representatives of **Welkin**.

**2. <u>Cyber Security</u>**

- **Welkin** takes effective measures to prevent cyber-attacks and to promptly detect any cyber intrusions to respond / recover / contain the fall out. Among other things, **Welkin** takes necessary preventive and corrective measures in addressing various types of cyber threats which includes denial of service, distributed denial of services

(DDoS), ransom-ware / crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds and password related frauds. **Welkin** realizes that managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This requires a high level of awareness among staff at all levels.

- **Welkin** ensures that the top management and the Board have a fair degree of awareness of the fine nuances of the threats. Further, it also proactively promotes, among their customers, vendors, service providers and other relevant stakeholders an understanding of their cyber resilience objectives, and ensures appropriate action to support their synchronised implementation and testing.

**3. Confidentiality**

- **Welkin**, along with preservation and protection of the security (as set out in detail above), also ensures confidentiality of customer information in the custody or possession of the service provider.
- Access to customer information by employees of the service provider to **Welkin** is on 'need to know' basis i.e., limited to those areas where the information is required in order to perform the outsourced function.
- **Welkin** further ensures that the service provider isolates and clearly identifies **Welkin's** customer information, documents, records and assets to protect the confidentiality of the information. **Welkin** has strong safeguards in place so that there is no commingling of information / documents, records and assets.
- **Welkin** ensures that it immediately notifies RBI in the event of any breach of security and leakage of confidential customer related information.

## 5. BUSINESS CONTINUITY PLANNING (BCP)

- BCP forms a significant part of any organisation's overall Business Continuity Management plan, which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes. BCP at **Welkin** is also designed to minimise the operational, financial, legal, reputational and other

material consequences arising from a disaster. **Welkin** has a Board approved BCP Policy. The functioning of BCP shall be monitored by the Board by way of periodic reports.

- **Welkin** requires its service providers to develop and establish a robust framework for documenting, maintaining and testing business continuity and recovery procedures. **Welkin** ensures that the service provider periodically tests the Business Continuity and Recovery Plan and occasionally conducts joint testing and recovery exercises with its service provider.

- In order to mitigate the risk of unexpected termination of the outsourcing agreement or liquidation of the service provider, **Welkin** retains an appropriate level of control over their outsourcing and the right to intervene with appropriate measures to continue its business operations in such cases without incurring prohibitive expenses and without any break in the operations of **Welkin** and its services to the customers.

- **Welkin** ensures that service providers are able to isolate **Welkin's** information, documents and records and other assets. In appropriate situations, **Welkin** can remove all its assets, documents, records of transactions and information given to the service provider, from the possession of the service provider in order to continue its business operations, or delete, destroy or render the same unusable.

- The CTO is responsible for formulation, review and monitoring of BCP to ensure continued effectiveness including identifying critical business verticals, locations and shared resources to prepare a detailed business impact analysis.

- After the vulnerabilities and inter relationships between various systems, departments and business processes are identified, there should be a recovery strategy available with the CTO to minimise losses in case of a disaster. **Welkin** also has the option of alternate service providers and would be able to bring the outsourced activity back in-house in case of an emergency.

- **Welkin** also has in place necessary backup sites for their critical business systems and Data centers.

These plans will also be tested by **Welkin** on a regular basis. The results along with the gap analysis will be placed by the CTO before the Board.

## 6. ARRANGEMENT FOR BACKUP OF DATA

**1.** By regular backups, data will be protected. Appropriate IT team will perform backup for responsible data. All backup data will be stored in an encrypted manner and backup copies will be stored in an environmentally protected and access controlled secure location. Stored copies will be stored with a short description that includes the following information:

a. Backup date / Resource name / type of backup method
b. Stored copies shall be made available upon authorised request:

The request for stored data shall be approved by an authorised person nominated by a Director/Manager in the appropriate department.

**2. Requests for stored data will include:**

a. Completion of a form that outlines the specifics of the request, including what copy is being requested, where and when the requester would like it delivered and why they are requesting the copy;
b. Acknowledgment that the backup copy will be returned or destroyed promptly upon completion of its use;
c. Submission of a return receipt as evidence that the backup copy has been returned.
d. A record of the physical and logical movements of all backup copies shall be maintained. Physical and logical movement of backup copies shall refer to:

1. The initial backup copy and its transit to storage;

2. Any movement of backup copies from their storage location to another location;

e. The record of physical and logical movements of backup media shall include:

1. all identification information relating to the requested copies;
2. purpose of the request;
3. the person requesting the copy;
4. authorization for the request;
5. where the copy will be held while it is out of storage;
6. when the copy was released from storage;
7. when the copy will be returned to storage.

f. Media in transit and store shall be protected from unauthorised access, misuse or corruption, including sufficient protection to avoid any physical damage arising during transit and store. All personnel responsible for data backup processing shall have:

1. Relevant identification;
2. Relevant authorization.

g. All relevant department backups shall be verified periodically and report on its ability to recover data. On a daily basis, information generated from each backup job will be reviewed for the following purposes:

1. To check for and correct errors;
2. To monitor the duration of the backup job;
3. To optimise backup performance where possible;

**h.** The IT team will identify problems and take corrective action to reduce any risks associated with failed backups.

## 7. PROVISIONS PERTAINING TO INFORMATION AND CYBER SECURITY

1. The risk assessment shall be brought to the notice of the Chief Risk Officer (CRO), CTO and the Board and serve as an input for Information Security Auditors. The

technology which will be used for mobile facilities shall ensure confidentiality, integrity, authenticity & deliver end-to-end encryption.

2. For using Social Media to market products, the marketing team shall be well equipped in handling social media risks and threats. As measures against account takeovers and malware distribution, proper controls, encryption and secure connections will be utilised.

3. The management will define, implement and monitor information security for the information assets on a real-time basis.

4. The information security committee will consist of senior executives along with the top management participation. This committee will be responsible for security related activities in the organization.

**7.1 Information received from applicant will be categorised as:**

**Secret:** Data concerning identity and access shall be classified as secret.

**Confidential:** System programmes and changes thereto shall be classified as confidential.

**Internal:** Information in relation to dispute resolution purposes shall be treated as internal.

**Public:** Non-Sensitive information available for external release.

## 8. Regulatory Returns To RBI (CIMS PORTAL)

**Welkin** shall ensure that adequate IT infrastructure arrangement is available to file regulatory returns to RBI (XBRL Returns).

## 9. CONFIDENTIALITY / NON-DISCLOSURE AGREEMENTS

This Policy has been prepared and implemented to ensure that all the users and staff are aware of their responsibilities towards the IT Resources of **Welkin**. It details the end users of their responsibilities and the acceptable use of the IT Resources.

### 9.1 Human Resources Security Policy

**1. Prior to employment**

**Personnel Screening**

- At the time of job applications verification checks should include the following:
    - Proof of the person's identity (e.g. passport);
    - Proof of their academic qualifications (e.g. certificates);
    - Proof of their work experience (e.g. résumé/CV and references);
    - Criminal record check;
    - Credit check.

- In the case of third parties, a similar screening process should be carried out. In case contractors and temporary staff are provided through an agency the contract with the agency should clearly specify the agency's responsibility for screening and notification procedures they need to follow if screening has not been completed or if the results give cause of doubt or concern.
- Authorization given to access sensitive systems by new and inexperienced staff should be supervised and management should evaluate this process.

**2. Terms and Conditions of Employment**

Terms and conditions of employment should include:

- Information security related roles and responsibilities.
- Action to be taken if the employee disregards security requirements
- Legal responsibilities and rights, e.g. regarding copyright laws and should be clarified within the terms and conditions of employment

- Indemnification clause against any loss, claim or damage to a third party caused by the employee
- Responsibility for classification and management of data
- It should state that these responsibilities are extended outside the organisation's premises and outside normal working hours, e.g. in case of home working.
- Roles and responsibilities related to information security should be documented in job descriptions and definitions. It should include:
    - Any general responsibilities for implementing or maintaining the Information Security policy
    - Any specific responsibilities for the protection of particular assets
    - Any specific responsibilities for the protection of particular security processes or activities
- All employees shall sign Confidentiality / Non-Disclosure Agreements at the time of joining.

**3. During employment**

**Management Responsibilities**

- Ensure that all users are properly briefed on their information security roles and responsibilities prior to being granted access to sensitive information or information systems.
- Provide guidelines to state security expectations of their role within the organisation.
- Ensure that the employees, contractors and third-party users conform to the terms and conditions of their employment / agreement.
- Ensure that all employees with information security responsibilities continue to have appropriate skills and qualifications.

**4. Information Security awareness, education and training**

- Training programs should be conducted to make users aware of new security threats. Periodic training calendar should be maintained.
- Employees should also be issued alerts whenever required through emails by the IT Team
- Copies of training and security education related manuals should be made available to all the employees.
- Users should be fully trained in the correct use of IT facilities like logon procedures, use of software packages etc.
- User training should include the following:
  - Reporting security incidents
  - Virus protection controls
  - Physical access
  - Internet usage
  - Email usage
  - Password usage
  - File sharing
  - Remote access

**5. Disciplinary Process**

- There should be a formal disciplinary process for employees who have committed a security breach subject to prior verification that a security breach has indeed occurred.
- The formal disciplinary process should ensure correct and fair treatment for employees who are suspected of committing breaches of security.
- The formal disciplinary process should provide for a response that takes into consideration factors such as the nature and gravity of the breach and its impact

on business, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required.

- In serious cases of misconduct, the process should allow for instant removal of duties, access rights and privileges, and for immediate escorting out of the site, if necessary.

## 6. Termination or Change of Employment

**Terminations and Job Changes**

- The communication of termination responsibilities should include ongoing security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement and the terms and conditions of employment continuing for a defined period after the end of the employee's, contractor's or third-party user's employment.
- The Human Resources function is generally responsible for the overall termination process and works together with the supervising manager of the person leaving to manage the security aspects of the relevant procedures.

**Return of Assets**

- Upon receiving communication from HR Department about terminations or job changes, IT Team shall ensure that
    - All assets (hardware, software assigned to the employee) are returned, including policy and procedure manuals and technical documentation,
    - Keys, passes and other access devices are returned,
- IT shall intimate to the HR Department through mail or any other mode of written communication that all access devices and keys have been returned.

**Removal of access rights**

- In case of terminations, IT shall ensure that access to information systems is revoked by deactivation or deletion of the person's access identifiers and the removal of the access authorities granted to them.

- In case of job changes, IT shall modify rights of the employee in line with the access control policy.
- IT shall send communication of removal of access rights to HR Department.

9.2 **Third Party Confidentiality or non-disclosure agreements**

- Third Party operations and work involving access to organizational information processing facilities should be based on formal contract specifying compliance with all information security controls through confidentiality or non-disclosure agreements
- Confidentiality or non-disclosure agreements should include:
    - General policy on information security - i.e. the Third-party is bound by the principles of **Welkin's** Information Security policy.
    - Involvement by the third party or subcontractors and other participants.
    - The right to audit contractual responsibilities.
    - Notice, notification and other conditions for termination of contracts.
    - A description of each IT service to be made available.
    - Times and dates when the service is to be made available - Service Level Agreements (SLAs) (including contingency arrangements, if appropriate).
    - The respective liabilities of the parties to the agreement.
    - Responsibilities regarding hardware and software installation and maintenance.
    - Responsibilities with respect to legal matters e.g. data protection, copyright legislation.
    - Restrictions on copying and disclosing information.
    - Procedures regarding protection of **Welkin's** assets.
    - Measures to ensure the return and processing of information and other assets at the end of the contract.

- The authorization process for user access.
- The right to monitor and revoke user access.
- A requirement to maintain a list of individuals authorised to use the service.
- Permitted access methods and the control and use of user identifiers and passwords.
- Measures to provide protection against the spread of computer viruses.
- Any required physical protection measures.
- User training in methods, procedures and security.
- Arrangements and responsibilities for reporting and investigating security incidents.
- Mechanisms to ensure that security measures are followed.

- Each third-party employee shall sign the Confidentiality and Non-Disclosure agreements, which shall be kept in a file by the ISM.
- Third-party employees are responsible for immediately informing the manager responsible for the contract, of any security breaches, including unauthorized access to or compromise of the data or information technology resources of **Welkin**. However, any **Welkin** employee who is aware of security violations by vendors shall also report them to the concerned information owner as well as security administrator.

## 10. USER ACCESS MANAGEMENT

### 1. User Registration & De-registration

**User Registration**

- Users should follow the formal registration and de-registration process adopted by **Welkin** for access to be granted to the information processing facilities.
- Access to all information services and facilities should be controlled through a formal registration process which should include using unique user IDs. Use of

group IDs should only be permitted where they are suitable and approved for the work to be carried out.

- Checks should be performed by the ISM / IT Manager on access requests to confirm they are appropriate for the business purpose and are consistent with the security policy e.g. to confirm that they do not compromise segregation of duties.
- Users should be given a written statement of their access rights.
- Users should be required to formally accept an undertaking to indicate that they understand and accept the conditions of access.
- Access for new users or users with changed rights should be denied by the Information Owner / Custodian until all authorisation procedures have been completed.
- A formal record should be maintained by the Information Owner / Custodian of all persons registered to use the service.
- Procedures should be established to notify the Information Owner / Custodian of users who leave **Welkin** or change responsibilities internally, and their accounts should be removed or changed immediately.
- There should be periodic (at least monthly) checks for, and removal of, redundant user-IDs and accounts that are no longer required.
- There should be procedures to ensure that redundant user IDs are not re-issued to other users.
- There should be periodic (at least monthly) checks to detect low or no use by registered users. There should be procedures to remove inactive accounts on a periodic basis.

**User De-registration**

Where an employee is leaving the organisation, the following guidelines should be followed:

- As soon as an employee resigns or is terminated, his network account shall be disabled so that access to confidential information is prohibited.
- Collect back all the security IDs, proximity devices, access badges, smart cards and any other identification, authentication and access devices that the employee has been granted.
- It is important to retain the contents of the system exactly as they are at the moment the previous employee was terminated or chose to leave. Thus, before decommissioning a computer as a workstation for another employee, an image of the hard drive has to be made and it shall be verified that the image is complete and accessible. In case of sensitive workstations, a second form of backup onto typical backup media shall also be made. It is important to create a copy of the data exactly, so it can be used in the future to locate information, corroborate stories or provide evidence in the event a crime is detected.
- Look through the desk, cubicle, work area and locker for any type of storage device or media and for documentation and printouts. If anything is found that contains data from a security classification other than that assigned to the ex-worker, further investigation as to how that data was obtained is necessary.
- This shall allow them to monitor the user accounts and commonly accessed resources of the ex-employee to look for unauthorized access. Co-workers should be informed about the person's work status and that they should not grant electronic or physical access or provide any confidential information to the ex-worker under any circumstances.

## 11. LOGGING AND MONITORING

### 1. Event Logging

- The ISM should decide on the conditions for logging. Audit logs should include:
  - User ID's

- Dates and times for log-on and log-off
- Terminal identity or location if possible
- Records for successful and rejected system attempts
- Records of successful and rejected data and other resource access attempts

- The following are the major audit events that need to be logged in a server / desktop:
  - Audit account logon events – Success, Failure
  - Audit logon events – Success, Failure
  - Audit policy change – Success, Failure
- All faults reported by users shall be logged by the IT Team.
- Similarly, faults displayed by systems/ servers pertaining to information processing or communication systems shall be logged by the IT Team and the respective vendor shall be notified
- IT Team shall record the corrective action taken for resolution of these faults in the said log.
- IT team shall on a monthly basis submit a report to the ISM regarding the faults logged during the current month, the actions taken and the current status. This shall include faults reported to all third-party vendors
- The ISM shall review the corrective measures taken to ensure that controls have not been compromised, and that the action taken is fully authorised.

**2. Protection of log information**

- Access to edit or delete log files shall not be allowed to anyone.
- All log files shall be backed up and made available to the monitoring authority.
- Log backups shall be done on a server different from the device that is being logged.

- **Welkin** shall retain user access logs for a minimum period of two years and periodic backup shall be conducted.
- Backup logs to be stored in an encrypted format.

**3. Administrator and operator logs**

- Logs shall be enabled to capture details of all activities done by the IT Manager / System administrator.
- Logs should include the following information:
    - System starting and finishing time
    - System errors and corrective action taken
    - Confirmation of correct handling of data files and computer output
    - Name of the person making the log entry
- These logs shall be subjected to regular, independent checks against operating procedures. These checks shall be performed by IT team.

## 12. CLOCK SYNCHRONISATION

The real-time clocks on workstations should reflect the accurate current time at their physical location. This should be enforced at the system level through clock synchronization protocols like Network Time Protocol (NTP).

## 13. IT SECURITY REVIEWS / PERIODIC IT SECURITY AUDITS

- IS Policy will be reviewed annually or at the time of any major change in the existing information technology environment affecting policies and procedures, whichever is earlier, by ISM. These changes will however be made as distinct version changes and will be tracked. Annual reviews shall be recorded in the Review / Version control table of the document. IT Security audits shall be carried out at six-monthly intervals.

- Any deviation in implementation of IS Policy shall only be allowed upon approval from the Board. The reason for deviation shall be presented to the board. All

deviations shall be valid for a fixed term, with a maximum term of 12 months. The same can be extended upon approval from the Board.

## 14. REGULAR REVIEWS OF RISK ASSESSMENT

The review is conducted at least once a year, or more frequently in the case of:

1. Significant Organizational Changes
2. Significant Change In Technology Architecture
3. Change of Business Objectives.
4. Changes In The Business Environment
5. Acquisition of A New Major Client
6. Addition of A New Business Line / Division
7. Change in the Legal / Regulatory Environment.

## 15. REVIEW

The Board approves of this IT Framework and has overall charge of the operational functions of **Welkin**. The Board is further responsible for timely amending this IT Framework pursuant to its operations and/or any change in the regulations or new regulations issued by the RBI in relation to this IT Framework.

**********