Information Technology and Cyber Security Policy

1. Introduction

The vast development of Information and Communication Technology lead cyber space more vulnerable to a wide variety of challenges, risks and threats. Large-scale cyber-attacks experienced in financial sector highlighted the necessity of Information and Cyber Security Policy in order to provide safe and credible functioning of critical information systems.

KLM Axiva Finvest Limited ("KLM" or "Company") is committed to protect its information assets and ensuring the confidentiality, integrity, and availability of sensitive data. This information and cybersecurity policy is designed to implement the comprehensive framework designed by RBI for NBFC in managing information and cybersecurity risks and promoting a secure computing environment.

Information and Cyber Security Policy underscores several compelling priorities, the implementation of which is necessary to meet the objectives set out in Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023.

All employees, contractors, and third-party vendors shall acknowledge their understanding and compliance with this policy upon accessing the organization's ICT infrastructure and regularly thereafter. Violations of this policy may result in disciplinary actions, including the suspension or termination of access rights and legal consequences.

Vision: Build and enhance robust, effective, and secure information and Communication Technology infrastructure for KLM Axiva Finvest Limited, that sets the standard in the Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023.

Mission: Build capabilities to prevent and respond to information security threats, reduce vulnerabilities and minimize damage from cyber incidents, to protect information systems of the Organisation.

Scope:

This policy applies to all employees, contractors, vendors, and third parties who have access to KLM's information systems, networks, and data.

Objectives:

- Implement secure information security controls to enhance ICT infrastructure capabilities of the organization.
- Set up a system to design all documents necessary for information security implementation.
- To ensure documents to be in compliance with RBI guidelines and best practice.
- Establish and enhance information technology security incident response mechanisms to protect organisation's infrastructure.
- Carry out rapid identification of threats and risks, perform necessary responsive and preventive measures, in case of necessity provide crisis management through predictive, preventive, protective and recovery actions.

- ❖ Enhance the protection and resilience of functioning of the Organisation by operating mechanisms applying best practice on establishment, acquisition, development and operation of information resources.
- ❖ Create a workforce of professionals skilled in cyber security through capacity building, educational programs and training.
- ❖ Create a culture of cyber security users to act effectively in compliance with the defined rules.

Definitions:

Unless the context states otherwise, the terms herein shall bear the meanings assigned to them below:

(i) *'Cyber'* - Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems.
(ii) 'Cyber event' – Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring.
(iii) 'Cyber security' - Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.
(iv) 'Cyber incident' shall mean a cyber event that adversely affects the cyber security of an information asset whether resulting from malicious activity or not.
(v) 'Cyber-attack' - Malicious attempt(s) to exploit vulnerabilities through the cyber medium to damage, disrupt or gain unauthorized access to assets.
(vi) 'De-militarized Zone' or 'DMZ' is a perimeter network segment that is logically between internal and external networks.
(vii) 'Information Asset' - Any piece of data, device or other component of the environment that supports information-related activities. Information Assets include information system, data, hardware and software.

2. IT Governance

The organization's IT governance encompasses strategic alignment, risk management, resource management, performance management, and business continuity/disaster recovery management.

Board of Directors

The Board of Directors comprises senior authorities vested with the power to approve strategies and policies concerning IT, information assets, business continuity, information security, and cyber security, encompassing incident response, recovery management, and cyber crisis management of the organisation.

All Such strategies and policies shall be reviewed at least annually by the Board.

IT Strategy Committee of the Board

The organization has formed the Board-level IT Strategy Committee (ITSC) comprising members with strong technical expertise. The constitution and terms of reference of the Committee shall be as approved by the Board of Directors from time to time.

IT Steering Committee

Active involvement and leadership of senior management are critical for fostering a strong information security posture within the organization, ensuring protection of assets, maintaining trust with stakeholders, and mitigating risks effectively. IT Steering Committee is constituted with representation from senior management level from IT and business functions. ITSC should ideally be chaired by a IT Manager and comprise of representatives from Business, IT, Human Resource, Legal, Operation. CISO will be the secretary of this committee.

Senior Management

Senior management's proactive engagement and leadership are essential for cultivating a robust information security stance within the organization.

The senior management of the organisation shall ensure:

(i) Execution of the IT Strategy approved by the Board.
(ii) IT/ IS and their support infrastructure are functioning effectively and efficiently.
(iii) Necessary IT risk management processes are in place and create a culture of IT risk awareness and cyber hygiene practices in the organisation
(iv) Cyber security posture of the organisation is robust; and
(v) Overall, IT contributes to productivity, effectiveness and efficiency in business operations.

Head of IT Function

A senior-level, technically proficient, and experienced individual has been appointed as the Head of the IT function.

The Head of IT Function shall, be responsible for the following:

- Ensuring that the execution of IT projects/ initiatives is aligned with the organisation's IT Policy and IT Strategy;
- Ensuring that there is an effective organisational structure to support IT functions in the organisation; and
- Putting in place an effective disaster recovery setup and business continuity strategy/ plan.
- Head of IT Function shall ensure effective assessment, evaluation and management of IT controls and IT risk, including the implementation of robust internal controls to
  (i) secure the organisation's information assets
  (ii) comply with extant internal policies, regulatory and legal requirements on IT related aspects.

3. IT Infrastructure and Service Management

1. IT Services Management Policy

KLM relies on third-party service providers to deliver certain IT services. This policy ensures that these services are managed and delivered in a manner consistent with our IT service management framework and standards.

This policy applies to all third-party service providers delivering IT services to our Company.

Objectives:

Ensure third-party services meet our IT service management standards Establish clear roles and responsibilities for third-party service providers Manage third-party services to minimize risk and ensure compliance Ensure seamless integration with our internal IT services

IT service provider selection

The selection of IT service providers is crucial to ensuring that the services delivered align with KLM's business objectives, meet quality standards, and mitigate risks.

Selection Process

- Identify and document specific business requirements and objectives that the IT service provider must meet.
- Clearly define the scope, deliverables, and performance expectations for the IT services required.
- Evaluate potential providers based on initial criteria such as industry reputation, service offerings, and financial stability.
- Develop and issue a detailed RFP that outlines requirements, evaluation criteria, and submission instructions.
- Assess submitted proposals based on predefined criteria, including technical capability, cost, compliance, and references.
- Review financial statements and credit ratings to ensure the provider's long-term viability.
- Check references and customer reviews to assess the provider's track record and reliability.
- Verify compliance with relevant regulations, standards, and industry best practices.
- Where applicable, conduct site visits to evaluate the provider's facilities, operations, and security measures.
- Identify potential risks associated with the provider, such as operational risks, data security risks, and business continuity risks.
- Negotiate and finalize terms and conditions, including service levels, pricing, and compliance requirements.
- Define clear SLAs outlining performance metrics, reporting requirements, and remedies for non- performance.

- Ensure that the contract includes provisions for compliance with legal and regulatory requirements.

Vendor Risk Assessment

The Vendor Risk Assessment Process shall be established to identify, evaluate, and manage risks associated with third-party vendors. This process should ensure that vendors align with KLM's risk management standards and compliance requirements, protecting the organization from potential adverse impacts.

Vendor Risk Assessment Process

Risk Identification

- ***Vendor Profile Review:*** Collect and review information about the vendor, including business operations, financial stability, regulatory compliance, and history of past issues.

- ***Risk Categories*****:** Identify potential risk categories, including:
  - **Operational Risks:** Risks related to vendor performance, reliability, and service quality.
  - **Financial Risks**: Risks related to the vendor's financial stability and solvency.
  - **Compliance Risks:** Risks associated with regulatory compliance, data protection, and contractual obligations.
  - **Reputational Risks:** Risks that could impact KLM's reputation due to vendor activities or failures.
  - **Security Risks:** Risks related to data security, cybersecurity, and physical security.
  - **Concentration risk:** Risk is the risk associated with having a significant portion of your business's resources or operations dependent on a single source, such as a single vendor, customer, geographic area, or market.
  - **Conflict of interests risk: Ri**sk arises when an individual or organization has competing interests or loyalties that could impair their ability to make impartial decisions.
  - **Single point of failure risk:** Risk highlights the vulnerability of systems that lack redundancy or backup mechanisms.
  - **Data security:** risk refers to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of sensitive data.
  - **High availability:** risk refers to the potential for a system, application, or service to become unavailable or inaccessible
  - **Supply chain risks:** risk related to the potential for disruptions, failures, or vulnerabilities in the supply chain to impact an organization's ability to deliver products or services to customers.

Performance Monitoring: Continuously monitor the performance of the selected IT service provider against SLAs and service specifications.

2. Capacity Management Policy

The purpose of this policy is to ensure that information systems and infrastructure are able to

support business functions and ensure availability of all service delivery channels. This policy applies to all departments that are involved in the planning, allocation, and management of resources, including IT systems, human resources, and physical assets.

Definitions

Capacity: The maximum output or performance level that a resource or system can achieve.
Demand Forecasting: The process of estimating future resource needs based on historical data, market trends, and business plans.
Resource Utilization: The measure of how effectively resources are being used compared to their total available capacity.

Capacity Planning
Capacity planning must be conducted on a regular basis to anticipate and prepare for future resource needs.

Forecasts should be updated at least [frequency, e.g., quarterly] to reflect changes in business demands and market conditions.

Resource Allocation
Resources should be allocated based on priority and demand forecasts to ensure optimal utilization and minimize bottlenecks.

Departments must submit resource requests with sufficient lead time to allow for effective planning and allocation.

Monitoring and Reporting
Regular monitoring of resource utilization and performance metrics is required to ensure that capacity meets current demand.

Capacity reports should be reviewed monthly by the [Capacity Management Team/Department] to identify any potential issues or areas for improvement.

Scalability and Flexibility
Systems and resources should be designed to be scalable and flexible to adapt to changing business needs and unexpected demands.

Contingency plans should be developed to address potential capacity shortfalls or surpluses. Performance Optimization

Continuous improvement practices should be applied to optimize resource performance and efficiency.

3. Project Management Policy

Managing IT projects effectively requires a structured approach to ensure that goals are met, risks

are mitigated, and resources are used efficiently.

(i) Initiation

a. Define Project Scope and Objectives:

- Clearly outline the project's goals, deliverables, and boundaries.
- Identify stakeholders and their requirements. Enable appropriate stakeholder participation for effective monitoring and management of project risks and progress

b. Conduct Feasibility Study:

- Assess technical, operational, and financial feasibility.
- Consider risks and potential benefits.
- Any new IT application proposed to be introduced as a business product shall be subjected to product approval and quality assurance process.

(ii) Planning

a. Develop a Project Plan:

- Outline tasks, timelines, and milestones.
- Define resource requirements and allocate roles and responsibilities.

Outsourced Projects:

- Organisation shall ensure that maintenance and necessary support of software applications is provided by the software vendors and the same is enforced through formal agreement.
- Organisation shall obtain the source codes for all critical applications from their vendors. Where obtaining of the source code is not possible, REs shall put in place a
- Shall obtain a certificate or a written confirmation from the application developer or vendor stating that the application is free of known vulnerabilities, malware, and any covert channels in the code. Such a certificate or a written confirmation shall also be obtained whenever material changes to the code, including upgrades, occur.
- Source code escrow arrangement or other arrangements to adequately mitigate the risk of default by the vendor. Organisation shall ensure that all product updates and programme fixes are included in the source code escrow arrangement.

c. Develop a Schedule:

Use tools like Gantt charts to create a timeline with deadlines for each task.

d. Budgeting:

Estimate costs and develop a budget.
Include contingencies for unexpected expenses.

g. Quality Assurance Planning:

Define quality standards and procedures for ensuring deliverables meet expectations.

c. Monitor and Control:

Track progress against the project schedule and budget. Use tools and techniques to assess performance.

4. Change Management Policy

The purpose of this policy is to set out the KLM's process of change management. The objective of this process is to ensure that changes to IT services and their associated components are recorded and then evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner. This policy applies to all employees, departments, and projects within KLM.

Change Management Process
The change management process consists of the following stages:

Request for Change (RFC) Submission:
Submit a Change Request through the designated system or form.
Provide details including the description, impact, and implementation plan.

Initial Review:
The Change Management Team performs an initial assessment to ensure completeness and relevance. Minor changes may be approved at this stage.

Impact Assessment:
Evaluate the potential impact of the change on systems, processes, and stakeholders. Identify risks, benefits, and resource requirements.

Change Approval:
The Change Management Team reviews and approves significant changes.
Approval is based on the impact assessment, risk analysis, and alignment with organizational goals.

Change Planning:
Develop a detailed implementation plan, including timelines, resources, and communication strategies. Prepare a rollback plan in case the change needs to be reversed.

Implementation:
Execute the change according to the approved plan. Ensure all stakeholders are informed and prepared for the change.

Monitoring and Review:
Monitor the change implementation to ensure it is proceeding as planned.
Review the change post-implementation to evaluate its effectiveness and address any issues.

Documentation and Reporting:
Document the change process, including approvals, implementation details, and outcomes.
Report on the change's impact and effectiveness to the Change Management Team.

Roles and Responsibilities:
Change Management Team: Oversees the change management process, performs initial reviews, and coordinates with the Change Management Board.

Change Requester: Submits the Change Request, provides necessary details.
Change Implementer: Executes the change according to the approved plan and manages any issues during implementation.

Patch Management

The purpose of this Patch Management Policy is to establish a structured and proactive approach to patch management within KLM. This policy aims to minimize security vulnerabilities and maintain the stability and performance of the organization's IT systems.

This policy applies to all systems, devices, and software within the company IT infrastructure, including servers, workstations, laptops, network devices, and applications.

Patch Identification and Prioritization
Patches will be prioritized based on severity levels defined by severity rating and based on vendor recommendation.

Patch Deployment
The IT team will test patches in a controlled environment before deploying them in the production environment.

- Critical security patches will be deployed immediately of their release.
- Non-critical patches and updates will be deployed within 7 days of their release.

Patch Exceptions
In certain cases, where immediate patching is not feasible due to compatibility or operational concerns, the IT team may document and seek approval for temporary patch exceptions.

Patching Responsibilities

- The IT team is responsible for the overall management and deployment of patches and updates.

Patch Testing

- Patches and updates will undergo thorough testing to ensure they do not disrupt normal system functionality.

Patching Schedule

- Regular patching windows will be scheduled for different environments, such as development, staging, and production.
- Emergency patches may be deployed outside the regular schedule when deemed necessary.

5. Data Migration Policy

This policy outlines the guidelines and procedures for migrating data from one system, platform, or storage device to another. The policy ensures that data migration is done efficiently, securely, and with minimal disruption to business operations. Policy ensures the secure and efficient migration of data from legacy systems to new systems and platforms.

Roles and Responsibilities:

- Data Migration Team: Responsible for planning, executing, and testing data migration
- Data Owners: Responsible for ensuring data accuracy and completeness
- T Department: Responsible for providing technical support and infrastructure

Data Migration Process:

1. Planning:
    - Identify data to be migrated
    - Determine migration timeline and resources
    - Develop data migration plan and budget

2. Data Preparation:
    - Clean and validate data
    - Remove duplicates and inconsistencies
    - Ensure data compliance with regulations

3. Data Migration:
    - Transfer data from legacy system to new system
    - Use secure data transfer methods (e.g., encryption, secure FTP)

4. Data Testing:
    - Verify data accuracy and completeness
    - Test data integration with new system

5. Data Validation:
    - Validate data against business rules and requirements
    - Ensure data consistency and integrity

6. Deployment:
    - Deploy migrated data to production environment
    - Monitor data performance and address issues

7. Data Security and Privacy:
    - Ensure data encryption and access controls
    - Implement data backup and recovery procedures
    - Comply with data privacy regulations (e.g., GDPR, HIPAA)

8. Documentation:
    - Maintain detailed documentation of data migration processes and procedures
    - Update documentation as necessary

6. Audit Trails Policy

This policy is documented to ensure the integrity and security of systems and data by maintaining accurate and reliable audit trails. This policy applies to all systems, applications, and data under the control of KLM

Objectives:

- Maintain a complete and accurate record of all system and data transactions
- Provide a means to track and monitor user activity
- Support incident response and troubleshooting efforts
- Meet compliance requirements for data security and privacy Audit Trail Requirements.

All systems and applications must generate audit trails for all transactions, including:

- User logons and logoffs
- Data creations, modifications, and deletions
- System configurations and changes
- User access and permissions changes.

Audit trails must include:

- Date and time of transaction
- User ID and username
- Transaction type and details
- System or application name

Audit trails must be:

- Securely stored and protected from unauthorized access
- Kept in compliance with RBI regulations and other applicable legal requirements
- put in place a system for regularly monitoring the audit trails and system logs to detect any unauthorised activity.

Responsibilities:
System Administrators: Ensure systems and applications are configured to generate audit trails
Security Team: Monitor and review audit trails for suspicious activity
IT Management: Ensure compliance with this policy and provide resources for audit trail management.

Procedure:

1. Audit Trail Collection: Systems and applications will collect and store audit trails in a centralized repository.
2. Audit Trail Review: The Security Team will regularly review audit trails for suspicious activity.
3. Incident Response: Audit trails will be used to support incident response efforts.
4. Compliance: The audit trails shall satisfy a business requirements apart from regulatory and legal requirements. The audit trails must be detailed enough to facilitate the conduct of audit, serve as forensic evidence when required and assist in dispute resolution, including for non-repudiation purposes.

7. Cryptographic controls

The purpose of this Policy is to establish guidelines and procedures for the use of cryptographic mechanisms to protect information within KLM. This policy aims to ensure that cryptographic practices are consistent with applicable laws and regulations, as well as industry best practices. It covers all cryptographic activities, including encryption, decryption, key management, and cryptographic algorithm selection.

Cryptographic Algorithm Standards
Approved Algorithms: Only algorithms approved compliant with industry standards (e.g., AES-256, RSA- 2048) shall be used.
Prohibited Algorithms: Use of deprecated or insecure algorithms (e.g., DES, MD5) is prohibited.

Key Management
Key Generation: Cryptographic keys must be generated using secure methods and be of appropriate length as per current best practices.
Key Storage: Keys must be stored in secure hardware or software key management systems that provide protection against unauthorized access.
Key Distribution: Keys must be distributed securely using encryption and secure communication channels.
Key Rotation: Keys must be rotated regularly and whenever there is a suspicion of compromise. Key Destruction: Keys that are no longer needed must be destroyed securely to prevent recovery.

Encryption Practices
Data at Rest: All sensitive data stored on systems must be encrypted using approved algorithms and key management practices.
Data in Transit: All sensitive data transmitted over networks must be encrypted using approved protocols.
Backup Encryption: Backup data must be encrypted and stored securely to protect against unauthorized access.

8. Straight Through Processing (STP) Policy

The purpose of this Straight Through Processing (STP) Policy is to define the procedures and guidelines for implementing and maintaining STP within KLM. The goal of STP is to automate transaction processing, reduce manual intervention, minimize errors, and enhance operational efficiency.

This policy applies to all financial transactions and related processes within KLM that are subject to STP. It includes all systems, processes, and personnel involved in transaction processing, from initiation to settlement.

Definitions

Straight Through Processing (STP): A method of processing transactions automatically and

electronically without manual intervention. STP aims to streamline transactions from initiation to settlement by using technology to handle all processing steps.

Transaction: Any financial activity or trade that involves the transfer of funds or securities.
Manual Intervention: Any process or action performed by a person that is required to complete a transaction.

STP Implementation

System Integration:

- Integrate STP systems with internal and external systems to ensure seamless data flow and transaction processing.
- Use industry-standard protocols and APIs for system interoperability.

Transaction Handling:

- Ensure that all transaction data is captured accurately at the point of initiation.
- Implement validation checks and automated rules to verify data accuracy and completeness.

Exception Management:

- Define procedures for handling exceptions and errors that cannot be processed automatically.
- Ensure that exceptions are promptly reviewed, resolved, and documented.

9. Data Quality and Security

Data Accuracy:
Maintain high standards of data accuracy and completeness throughout the transaction lifecycle. Regularly audit and reconcile transaction data to identify and correct discrepancies.

Data Security:
Implement robust security measures to protect transaction data from unauthorized access and breaches.
Use encryption and secure communication protocols to safeguard data in transit and at rest.

10. Monitoring and Reporting

Performance Monitoring:
Continuously monitor STP performance to identify and address any issues or bottlenecks. Use performance metrics and reports to assess the effectiveness of STP processes.

Reporting:
Generate regular reports on STP performance, including transaction volumes, exception rates, and processing times.

Ensure that reports are reviewed by relevant stakeholders to identify areas for improvement.

11. Compliance and Governance

Regulatory Compliance:
Ensure that STP processes comply with applicable financial regulations and industry standards. Regularly review and update STP procedures to align with regulatory changes.

12. Physical and Environmental Controls

The purpose of this policy is to establish guidelines and procedures to protect the organization's physical assets, facilities, and personnel from potential threats, ensuring the safety and security of all stakeholders.

This policy applies to all employees, contractors, visitors, and third-party personnel accessing the organization's premises or facilities.

Access Control:

a. Identification and Authentication: Access to the organization's premises will be granted based on identification and authentication mechanisms, such as access cards or biometric authentication.

b. Access Levels: Access privileges will be granted based on job roles and responsibilities, with different access levels assigned to employees, contractors, and visitors.

c. Visitor Management: A visitor management system will be implemented to track and monitor visitor access to the premises. All visitors must register and obtain appropriate identification while on-site.

d. Access Monitoring: Access logs will be maintained to track entry and exit times, helping to monitor and investigate any suspicious activities.

Physical Security Measures:

a. Perimeter Security: Physical barriers will be implemented to secure the organization's perimeter and prevent unauthorized access.

b. Building Security: Security cameras, alarms, and security personnel will be strategically placed throughout the building to monitor and respond to security incidents effectively.

c. Data Centre Security:
   - Shall implement suitable physical and environmental controls in Data Centre and Disaster Recovery sites used by them.
   - The DC and DR sites should be geographically well separated so that both the sites are not

affected by a similar threat associated to their location.

- Shall ensure that their DC and DR sites are subjected to necessary e- surveillance mechanism.

d. Equipment Protection: Critical equipment and assets will be physically secured and marked with identification to prevent theft and unauthorized relocation.

13. Access Controls

The purpose of this policy to control access to software, information assets and business processes on the basis of business and regulatory security requirements.

Access Control Methods

Access to data is variously and appropriately controlled according to the data classification. Access control methods include explicit logon to devices, Windows share and file permissions to files and folders, user account privileges, server and workstation access rights, firewall permissions, network zone and VLAN ACLs, IIS / Apache intranet / extranet authentication rights, login rights, database access rights, encryption and other methods as necessary.

Access control applies to all Organisation owned networks, servers, workstations, laptops, mobile devices and services run on behalf of Organisation.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within organisations Active Directory domains.

Access Approval

All access by any user or system (employee, contractor, third party service vendor) must be justified by a business reason for why the access is necessary, along with the parameters of access (what classification level, times/dates, from what locations, etc.) Access cannot be simply given to 'everything'. Justifications shall be kept on file for review, as well as forensic purposes.

Access Request

Users will request access in the following way:

- *A formal access control request is made using an approved form and documentation.*
- *A valid business justification for the access is documented.*
- *Access requests will specify particular systems or information (no general access to all) commensurate with the person's access level.*
- *Access requests must be correctly approved*
- *Request forms should be stored by the administrators and retained until at least 90 days after the person has left the company*

Changes in access must be requested and documented in the same way as original access requests (may be accomplished on the original form as notations and subsequent approval signatures)

Access Request Form

All access must be requested through an Access Request Form and routed through IT Department. Log register is to be maintained in IT Department server or related systems.

User registration

A registration and re-registration procedure shall be used for granting access to all information asset of the company. User should not get access without registration process and in case of violation of being a valid user; user rights should be de-registered with immediate effect.

User IDs

Each user must have a unique ID that only they should use for logical access. This ID may be used to access several systems but will not be used by anyone else. Employees should not share their unique ID or security access cards to secured areas. Users are responsible for all actions taken with their unique user ID, whether or not they are the ones who took the actions. Thus, it behoves the user to protect their IDs and passwords. Never give your password to anyone, including your supervisor. User IDs for users who have left the company must be deactivated or deleted. It is permissible to retain a user account for access to the user's data once they have left, but the password must be changed to prevent the user from accessing their account. Data will be recovered and moved as soon as possible, and the account disabled or deleted in this case.

Password

Password issuing, strength requirements, changing and control will be managed through formal processes.

Password issuing will be managed by the IT department for employees, associates, contractors, partners, and vendors. Password length, complexity and expiration times will be controlled through Group Policy Objects in operation system.

Privilege management

The allocation and use of privileges shall be restricted and controlled. Inappropriate use of system privileges may become a major contributory factor to the failure of systems hence access to critical systems should be filtered in such a way that nobody will be able to take disadvantage of the rights.

User Account Review

Administrators will conduct periodic (at least monthly) audits of all user accounts and disable/delete any accounts that have not been used in the past month. If the user is known to be away from the office (maternity leave, sabbatical, etc.) then the account must be disabled and a notation made as to why and the person's expected return. User accounts that have never been used in the month period must be deleted.

Review of user access rights

User access rights should be reviewed at regular intervals for effective control over access to data and information. User access to data and information should be reviewed on regular basis to keep updated access control. Transferred or left employees account gets removed in such periodic access audit.

User Access Termination

Users who leave, the organisation will have their access to all systems terminated on their last day, or as soon as possible if they are being terminated for cause. All access must be terminated (through disabling, deleting, or changing the password), including physical access to facilities, and remote access. The user access request form and associated documentation must be used as a reference to ensure that all systems and networks are addressed. The access request form must be annotated that access has been terminated and how, (e.g., disabling).

Remote Access

It is the responsibility of employees, contractors, vendors and agents with remote access privileges to company's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection.

When accessing the network from a personal computer, Authorized Users are responsible for preventing access to any computer resources or data by non-Authorized Users. Performance of illegal activities through network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access.

Authorized Users will not use networks to access the Internet for outside business interests.

Remote Access Requirement

- Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases.
- Authorized Users shall protect their login and password, even from family members.
- While using owned computer to remotely connect to corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
- Ensure that the systems used and the remote access from alternate work location to the environment hosting organisation's information assets are secure.
- Implement multi-factor authentication for enterprise access (logical) to critical systems
- Put in place a mechanism to identify all remote-access devices attached/ connected to the organisation's systems
- Ensure that data/ information shared/ presented in teleworking is secured appropriately.

All hosts that are connected to internal networks via remote access technologies must use the most up-to- date anti-virus software this includes personal computers.

Personal equipment used to connect to networks must meet the requirements stated in the Hardware and Software Configuration Standards for Remote Access to Networks.

It is the policy of the Organisation., that mobile computing and storage devices containing or accessing the information resources at the DBFS must be approved prior to connecting to the information systems. This pertains to all devices connecting to the network at the >, regardless of

ownership.

Mobile computing and storage devices include, but are not limited to: laptop computers, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, modems, handheld wireless devices, wireless networking cards, and any other existing or future mobile computing or storage device that may connect to or access the information systems at DBFS. A risk analysis for each new media type shall be conducted and documented prior to its use or connection to the network unless the media type has already been approved by the CSTC.

Physical access to information technology processing equipment, media storage areas, and media storage devices and supporting infrastructure (communications, power, and environmental) must be controlled to prevent, detect, and minimize the effects of unauthorized or unintended access to these areas.

Branches / Departments are required to establish physical and environmental controls for assets under their physical control. Requirements within this policy extend to self-contained facilities such as external data centers, as feasible, and should be considered prior to entering into a contract with an external data center, workplace, or facility. In conjunction with the Asset Management Policy, physical and environmental controls must follow the minimum requirements established within this policy.

14. System Metrics Policy

The purpose of this System Metrics Policy is to establish guidelines for monitoring, measuring, and managing the performance and health of the organization's critical IT systems. This policy aims to ensure system reliability, optimize performance, and support proactive incident management and continuous improvement.

Metrics Definition

Key Performance Indicators (KPIs)
Performance Metrics:
Response Time: Average time taken to process a request.
Throughput: Number of transactions or requests processed per unit time.
System Load: Average system load measured over time.

Availability Metrics:
Uptime: Percentage of time the system is operational and available.
Downtime: Amount of time the system is non-operational.

Capacity Metrics:
CPU Utilization: Percentage of CPU capacity being used.
Memory Utilization: Percentage of memory being used.
Storage Utilization: Percentage of storage capacity being used.

Error Metrics:
Error Rate: Number of errors occurring within a specific period.
Failure Rate: Frequency of system failures or outages.

Security Metrics:
Intrusion Attempts: Number of unauthorized access attempts.
Authentication Failures: Number of failed login attempts.

Measurement Methods
Metrics shall be collected using tools such as Nagios, Prometheus etc. Data will be captured in real-time where possible, and aggregated for analysis as needed.

4. Information Security and Risk Management

1. Periodic review of IT related risks

This policy aims to protect its information assets from cyber threats and IT risks. This policy outlines the approach to manage cyber and IT risks by establishing a framework for identifying, assessing, managing, and mitigating risks associated with the organization's information technology assets and services.

Definitions

Risk: The potential for loss, damage, or destruction of an asset or the impact of a threat exploiting a vulnerability.
Risk Assessment: The process of identifying, analyzing, and evaluating risks to IT assets and services.
Risk Management: The systematic process of managing risks through identification, assessment, response, and monitoring.

Risk Management Framework
The organization will adopt a risk management framework that includes the following steps:

Risk Identification: Regularly identify and document potential risks to IT assets, including threats, vulnerabilities, and potential impacts.
Risk Assessment: Analyze identified risks to determine their likelihood and potential impact on the organization. Risks will be prioritized based on their severity.
Risk Response: Develop and implement risk response strategies, including risk avoidance, mitigation, transfer, or acceptance, based on the risk assessment results.
Risk Monitoring: Continuously monitor risks and the effectiveness of risk management strategies, making adjustments as necessary.

2. Roles and Responsibilities

Risk Management Committee of the Board (RMCB): Responsible for overseeing the risk management process, conducting risk assessments, and developing risk management strategies. RMCB in consultation with the ITSC shall periodically review and update the policy at least on a yearly basis.

3. Risk Management Tools and Techniques

The organization will utilize appropriate tools and techniques for risk management, including risk assessment frameworks (e.g., NIST, ISO 31000), Security audits and assessments.

5. Business Continuity and Disaster Recovery Management

KLM Axiva Finvest Ltd. recognizes the critical importance of maintaining uninterrupted access to our Core Banking System (CBS) application, Prosper, and related banking services for our customers. The dynamic nature of today's financial environment necessitates a comprehensive Business Continuity Plan (BCP) to ensure that our operations can withstand and quickly recover from any disruptions. Our BCP policy is designed to safeguard our banking services, protect customer data, and minimize any potential impact on our operations, ensuring that we continue to deliver reliable and secure banking services under all circumstances.

The BCP procedure outlines detailed strategies and protocols to be followed in the event of various potential disruptions, including natural disasters, cyber-attacks, technical failures, and other emergencies. By implementing these procedures, KLM Axiva Finvest Ltd. aims to ensure the rapid restoration of the CBS application, Prosper, and other critical services, thereby maintaining operational resilience.

1. Scope
    a. Applications & Services: Core banking application, Prosper, hosted in the cloud.
    b. Locations:
        i. Primary Data Centre (DC): KLM Axiva Finvest Limited, KLM Grand Estate, Bypass Road, Edapally Ernakulam, Kerala - 682024.
        ii. Disaster Recovery (DR) site: KLM Tower, College Road, Opp. Vimalagiri School, Kothamangalam, Ernakulam, 686691.
    c. Access: HO and branches access via VPN tunnel to HO.
    d. Redundancies: Dual ISP connections, dual firewalls, and UPS for power backup.

2. Objectives
    a. Ensure availability of core banking services during disruptions.
    b. Minimize operational impact.
    c. Provide a framework for quick recovery.
    d. Safeguard data and IT infrastructure.
3. Roles and Responsibilities
    a. CIO: Oversee BCP implementation and maintenance.

b. IT Team: Ensure IT infrastructure availability and security.
    i. Branch Managers: Ensure HO and branch compliance and coordination during disruptions.

4. Risk Assessment
    a. Identify potential risks and their impact.
    b. Prioritize critical functions and processes.
    c. Develop mitigation strategies.

5. Recovery Objectives

Recovery Time Objective (RTO): The maximum acceptable length of time that an application, system, or process can be down after a failure or disaster occurs.

- Normal: 4 to 24 hours
- High Availability Systems: Less than 1 hour
- Mission-Critical Systems: Minutes to a few hours
- Non-Critical Systems: Up to several days

Recovery Point Objective (RPO): The maximum acceptable amount of data loss measured in time.

- Normal: 4 to 24 hours
- High Availability Systems: Less than 1 hour
- Mission-Critical Systems: Seconds to minutes
- Non-Critical Systems: Up to several days

6. Recovery Strategies

Data Centre and DR:

- Synchronize DC and DR: Ensure that the Primary Data Centre (DC) and Disaster Recovery (DR) site are continuously synchronized. This includes regular updates and data replication to ensure that both sites have the latest information.
- Regularly test failover procedures: Conduct periodic failover tests to ensure that the transition from the DC to the DR site can be done seamlessly and within the defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). These tests should include complete simulations of potential disaster scenarios to verify the effectiveness of the failover process.

VPN and ISP:

- Maintain dual ISP connections: To prevent network outages, maintain two separate Internet Service Providers (ISPs) for redundancy. This ensures continuous network connectivity even if one ISP fails.
- Regularly test VPN failover: Conduct regular tests of the Virtual Private Network (VPN) failover systems to ensure that access from branches to the Head Office (HO) remains uninterrupted during an ISP failure.

Firewalls:

- Ensure high availability and redundancy: Implement firewall configurations that provide

high availability and redundancy. This involves setting up multiple firewalls in active-passive or active- active modes to ensure continuous protection and connectivity even if one firewall fails.

Power Backup:

- Regularly test and maintain UPS systems: Conduct regular maintenance and testing of Uninterruptible Power Supply (UPS) systems to ensure they are functional and capable of providing power during outages. This includes checking battery health, load testing, and ensuring proper configuration for seamless power transition.

DR Drills:

- Conduct disaster recovery drills twice annually: Perform comprehensive disaster recovery (DR) drills twice a year. These drills should simulate different disaster scenarios and test the entire recovery process, including data restoration, system failover, and operational continuity. The drills help identify any gaps or weaknesses in the DR plan and ensure that all personnel are familiar with their roles and responsibilities during a disaster.

6. Incident Response Plan

Identification

i. General Incident Response

a. Continuous Monitoring: Implement continuous monitoring tools and practices to detect any anomalies, suspicious activities, or breaches. This can include network traffic analysis, endpoint monitoring, and application logs.
b. Logging: Ensure that all relevant events are logged comprehensively. This includes access logs, system logs, and application logs. Logs should capture essential details such as timestamps, user activities, error messages, and system responses.
c. Alerting: Configure alert mechanisms to notify the incident response team immediately when potential incidents are detected. This can be done through automated alerts via email, SMS, or integrated incident response platforms.

ii. Communication

Notify Stakeholders Internally:

- Internal Communication Plan: Develop a communication plan that outlines the roles and responsibilities of team members in the event of an incident. This should include a clear escalation path and contact information.
- Incident Reporting: Ensure that all team members know how to report an incident. This can be done through a dedicated incident reporting system or a designated contact person.
- Regular Updates: Keep internal stakeholders informed with regular updates on the status of the incident, actions taken, and next steps.

Communicate with Customers Externally:

- External Communication Plan: Develop a plan for communicating with customers and external stakeholders. This should include predefined templates and key messages to be delivered during an incident.
- Transparency: Maintain transparency with customers regarding the incident's nature, potential impact, and steps being taken to resolve the issue. This helps in maintaining trust and managing customer expectations.
- Support Channels: Provide customers with support channels where they can seek assistance or clarification during an incident. This can include customer support hotlines, email, or a dedicated incident response web page.

iii. Response

Address Minor Incidents Locally:

- Immediate Action: For minor incidents that do not have a widespread impact, the incident response team should take immediate action to contain and resolve the issue locally.
- Documentation: Document the incident details, actions taken, and resolution to ensure lessons are learned and to improve future incident response efforts.
- Root Cause Analysis: Conduct a root cause analysis to understand the underlying factors that caused the incident and implement measures to prevent recurrence.

Invoke DR Procedures for Major Incidents:

- Disaster Recovery (DR) Plan: For major incidents that significantly impact operations, invoke the organization's disaster recovery procedures. This should include predefined steps for system failover, data recovery, and business continuity.
- Coordination: Coordinate with all relevant teams, including IT, security, and business units, to ensure a smooth execution of the DR plan.
- Escalation: Escalate the incident to senior management and external partners as necessary to mobilize additional resources and expertise.

iv. Recovery

- System Restoration: Restore affected systems and data from backups or alternate sites as per the DR plan. Ensure that all critical services are brought back online in a prioritized manner.
- Validation: Conduct thorough validation and testing of restored systems to ensure they are functioning correctly and securely. This includes running integrity checks, performance tests, and security assessments.
- Post-Incident Review: Perform a post-incident review to assess the effectiveness of the response and recovery efforts. Identify any gaps or areas for improvement and update the incident response plan accordingly.
- Communication: Inform internal and external stakeholders about the successful recovery and any residual actions that may be required. Provide a detailed incident report that outlines the incident, response actions, and lessons learned.

Specific Scenarios

i. Network Outage

- Identification: Detect loss of connectivity.
- Response: Switch to backup ISP. Notify IT team and affected branches.
- Recovery: Ensure network stability, validate VPN connections.

ii. Data Center Failure

- Identification: Monitor for DC failures through automated alerts.
- Response: Trigger failover to DR site in Kothamangalam.
- Recovery: Validate data integrity and service availability at DR site. Plan and execute restoration of the primary DC to meet RTO and RPO.

iii. Cybersecurity Breach

- Identification: Detect through security monitoring systems.
- Response: Isolate affected systems, notify IT and security teams, engage external cybersecurity experts if needed.
- Recovery: Conduct a thorough investigation, patch vulnerabilities, restore secure operations, and communicate with stakeholders.

iv. Power Outage

- Identification: Detect power failure at HO or branches.
- Response: Switch to UPS power. Notify facilities and IT teams.
- Recovery: Restore primary power, validate UPS functionality, ensure all systems are operational.

v. Application Failure

- Identification: Detect through monitoring tools and user reports.
- Response: Restart application services, notify IT team.
- Recovery: Diagnose and fix the root cause, validate application functionality, and communicate resolution to users.

Training and Testing

a. Conduct regular training sessions and simulations.
b. Test BCP through drills, failover tests between DC and DR, and ISP connections.
c. Conduct disaster recovery (DR) drills twice annually to ensure readiness and effectiveness of the DR plan.

7. Information System (IS) Audit

1. Information Systems (IS) Audit

The purpose of this Information System Audit Policy is to establish a framework for conducting audits of information systems within KLM. This policy applies to all information systems owned or operated by KLM including hardware, software, networks, and data.

A. Definitions

Audit: A systematic examination of information systems, processes, and controls to assess their effectiveness, compliance, and security.

Information System Audit: An assessment of the information systems and related controls to evaluate their reliability and security.

Auditor: An individual or team responsible for conducting the audit, which may include internal staff or external parties.

B. Objectives of Audits

The objectives of conducting information system audits include:
Assessing the effectiveness of security controls and risk management practices.
Evaluating compliance with applicable laws, regulations, and policies.
Identifying areas for improvement in information systems and controls.
Ensuring the accuracy and reliability of information processed by the systems.

C. Responsibilities

- The Audit Committee of the Board (ACB) shall be responsible for exercising oversight of IS Audit of the KLM.
- The ACB shall review critical issues highlighted related to IT / information security/ cyber security and provide appropriate direction and guidance to the Management.
- KLM shall have a separate IS Audit function or resources who possess required professional skills and competence within the Internal Audit function.
- Use of external resources for conducting IS audit in areas where skills are lacking within the organisation, the responsibility and accountability for such external IS audits would continue to remain with the competent authority within Internal Audit function.

D. Audit Frequency

KLM shall carry out IS Audit planning by adopting a risk-based audit approach. Information system audits will be conducted once in every 2 years or more frequently as necessary based on:

- Changes in technology or business processes.
- Identified risks and vulnerabilities.
- Regulatory requirements.
- Previous audit findings.

E. Audit Planning

Audits will be planned and conducted in accordance with the following steps:

- Define Audit Scope: Identify the systems, processes, and controls to be audited.
- Develop Audit Objectives: Establish specific objectives for the audit based on organizational goals and risk assessments.
- Create Audit Plan: Outline the methodology, resources, timeline, and responsible parties for the audit.

F. Compliance and Governance

This policy aligns with applicable laws, RBI regulations, and industry standards, including but not limited to:

d. RBI regulations
e. ISO/IEC 27001
f. NIST SP 800-53

Approved by the Board of Directors on August 26, 2021;
Revised by the Board of Directors on January 17, 2025.