PNY SABHA FINANCE LTD.
പാരമ്പര്യത്തിന്റെ വിശ്വാസം

PNY SABHA FINANCE LTD

IT AND IS POLICY

K.P. ANAND NAIR

Table of Contents

Revision History

Ver. No.	Prepared By	Revision Date	Reviewed/ Approved By	Approved Date	Remarks
1.	Anil.C Information Security Consultant–TuxCentrix Consultancy Pvt. Ltd.	28/03/2019	Board	09/05/2019	Base Version
2.	Anand Nair	30/07/2024	Board	06/08/2024	Renewed Version

Introduction

Information Technology (IT) at PNY Sabha Finance Limited (PNY) serves as a strategic enabler to the company's business operations. Therefore, PNY's IT policy is closely aligned with its overall business strategy, which emphasizes expanding into specific geographies, launching tailored products for targeted customer segments, and leveraging digital technology and electronic channels to extend customer outreach.

The IT policy of PNY encourages the practical and prudent use of technology to gain a competitive edge and maximize returns on IT investments. To achieve this, PNY follows the guiding principles outlined below for technology adoption:

- **Fit-for-purpose and value-for-money solutions** that are proven.
- **Standardization of technologies** and simplification of IT architecture.
- Avoidance of **technologies those are either too futuristic** or likely to become obsolete.
- Solutions those are **secure, scalable, and easy to maintain**, with straightforward integration options.
- Ensuring **best practices and information security** are integrated into the design, architecture, and processes.
- Readiness to adopt **open-source solutions** provided they meet the required standards of scalability and security.

PNY remains committed to protecting the confidentiality, integrity, and availability of all organizational, partner, and customer information assets. This policy ensures compliance with legal and regulatory standards, such as the Reserve Bank of India's (RBI) security guidelines.

These policies and guidelines apply to all PNY employees, contractors, and sub-contractors. The document will be reviewed bi-annually to remain relevant in the dynamic information security landscape.

1. IT Change Management Policy

1.1 Policy Statement

All changes to PNY's IT assets must be performed in a controlled manner to ensure that the risks associated with these changes are managed at an acceptable level.

1.2 Scope

This policy applies to:

- All critical IT assets.
- All personnel involved in administering or maintaining the IT infrastructure.
- Business or application owners responsible for the operation of their assigned IT assets.
- IT personnel responsible for carrying out approved changes.

1.3 Responsibilities

Role	Responsibility
IT Department (In-house IT Management)	Review and approve changes based on security impact analysis. Approve implementation plans in the test environment. Oversee movement from the test environment to production. Periodically review all changes.
IT Department (Outsourced IT Management)	For major changes in production, the IT service provider must notify PNY's IT department and explain associated risks, particularly regarding timelines. Maintain records of changes.
Users	IT Department is responsible for informing users of any major changes affecting them.

1.4 Procedures for Change Management

1. **Change Request (CR)**: A formal CR for business requirements must be submitted through the Department Head to the Change Management Committee (CMC). The CMC will assess feasibility and document the CR.
2. **Change Approval**: Minor changes are approved by the Change Manager; major changes require CMC approval.
3. **Implementation Planning**: An implementation team, including administrators, developers, operational personnel, and third-party vendors, will create a detailed plan.
4. **Testing**: The team will test changes in a test environment and ensure system functionality. Deviations from the plan must be recorded and approved.
5. **Implementation**: Approved changes will be carried out in the production environment, with a post-implementation report submitted.
6. **Monitoring and Verification**: Changes will be reviewed for effectiveness, ensuring objectives were met and the implementation adhered to the plan.

2. Backup and Archival Policy

2.1 Policy Statement

PNY will implement robust backup mechanisms to ensure that critical data is recoverable in the event of equipment failure, intentional destruction, or disaster.

2.2 Scope

This policy applies to:

- All critical IT assets owned by PNY.
- All critical information stored on PNY computing platforms.
- Backup administrators, application owners, and administrators responsible for server and network infrastructure.

2.3 Responsibilities

Role	Responsibility
Backup Administrators	Ensure that backups are performed according to the backup schedule. Confirm that backups are securely stored and easily recoverable. Regularly test the backups to ensure data integrity.
Application & Server Administrators	Ensure that all necessary files, including system software and critical databases, are backed up. Maintain the backup logs and recovery procedures.
Business Owners	Ensure the backup meets business continuity and compliance requirements.

2.4 Procedures

1. **Backup Scheduling**:
   - **Production Database (DB) Log Shipping**: Incremental backup every 15 minutes to a Disaster Recovery (DR) site.
   - **Production DB Full Backup**: Conducted after business hours and stored on external HDDs.
   - **Application Backup**: Carried out upon every change, and backup configuration files are updated accordingly.
2. **Data Retention**: Backup data will be retained according to business and compliance needs, and the recovery process will be tested periodically.
3. **Backup Monitoring**: A register will be maintained to log backup operations, including:
   - Application name.
   - Backup operator name and user ID.
   - Date of backup, backup status and comments.

3. IT Service Continuity Policy

3.1 Policy Statement

PNY will ensure that core IT services can be resumed after any severe disruption, within agreed-upon recovery objectives, to maintain business operations without major interruptions.

3.2 Scope

This policy applies to:

- All IT systems, including software, business data, and storage systems, which are essential to business continuity.

3.3 Responsibilities

Role	Responsibility
IT Service Continuity Manager	Develop and maintain the IT Service Continuity Strategy. Ensure alignment with business objectives and compliance requirements. Coordinate recovery activities in case of service disruptions.
IT Staff	Execute IT continuity procedures as documented and tested. Support the Continuity Manager in recovery efforts.

3.4 Procedures

1. **IT Service Continuity Strategy**:
   - **Recovery Point Objective (RPO)**: 30 minutes.
   - **Recovery Time Objective (RTO)**: 120 minutes.
   - Maintain detailed recovery plans for all critical business functions and potential disaster scenarios.
2. **Planning and Documentation**: All continuity plans, testing activities, and communication must be recorded and kept confidential. The IT Service Continuity Manager will ensure that the strategy is up to date with evolving internal and external requirements.

4. Password Policy

4.1 Policy Statement

PNY will ensure that access to its information systems is authenticated using strong passwords, and these passwords will be protected throughout their lifecycle.

4.2 Scope

This policy applies to:

- All information systems owned, leased, or outsourced by PNY.
- All personnel who have access to PNY data.
- All third-party service providers and sub-contractors with system access.

4.3 Responsibilities

Role	Responsibility
Users	Follow PNY's password policies and guidelines. Ensure password confidentiality at all times.
System & Application Owners	Ensure compliance with password requirements and procedures. Identify systems that cannot fully support the password policy and provide additional controls.
Head – IT	Review and enforce password policies. Maintain a list of systems unable to comply fully with password procedures and implement additional controls

4.4 Procedures

1. **Password Generation and Management**:
   - User IDs and passwords will only be generated upon formal request by authorized officials.
   - Users must change their password at first login.
   - Systems will enforce periodic password changes (every 50 days) and alert users 10 days before expiry.
   - Passwords must be at least 8 characters long, contain a mix of lower case, upper case, numbers, and special characters, and will not be stored or displayed in plaintext.
2. **Security Controls**:
   - Default passwords must be changed before any system moves to production.
   - Password history will retain at least the last three passwords.
   - Accounts will be locked after three failed login attempts and will require administrator intervention to reset.
3. **Compromise Protocol**:
   - Users suspecting that their password has been compromised must report it immediately and change the password without delay.

5. Anti-Virus Policy

5.1 Policy Statement

PNY will protect all its IT assets from malicious software using anti-virus solutions capable of early detection, efficient containment, and eradication of threats.

5.2 Scope

This policy applies to:

- All computer devices connected to PNY's network.
- All servers running on operating systems vulnerable to malware.

5.3 Responsibilities

Role	Responsibility
Anti-virus Administrators	Ensure anti-virus software is installed, updated, and configured on all PNY systems. Conduct regular system scans and submit status reports on anti-virus protection.
Head – IT	Review the implementation of anti-virus policies and address any deficiencies.

5.4 Procedures

1. **Selection and Installation**: Anti-virus software must be capable of detecting a wide range of malicious software, including viruses, Trojans, worms, and spyware. It should be installed on all systems before they are connected to PNY's network.
2. **System Scans**: Full system scans will be performed weekly, and real-time scans will be configured to detect threats whenever files are accessed, copied, or moved.
3. **Anti-Virus Reporting**: The anti-virus team will submit monthly reports covering the status of protection, including:
   - Number of systems lacking anti-virus protection.
   - Number of detected and quarantined viruses.
   - Actions taken to resolve infections.
4. **Incident Reporting**: Users must report any malware that is not automatically cleaned by the anti-virus agent to the Helpdesk for further investigation and resolution.

6. Access Control Policy

6.1 Policy Statement

Access to PNY's IT systems will be controlled to prevent unauthorized access, ensuring that information is protected from accidental or deliberate disclosure.

6.2 Scope

This policy applies to:

- All IT systems, including software, databases, file systems, storage systems, and removable media.

6.3 Responsibilities

Role	**Responsibility**
Users	Follow the access control procedures.
System/Network Administrators	Implement and monitor access controls. Communicate access policies to third-party vendors.
Head – IT	Oversee access control policy implementation and enforcement.

6.4 Guidelines

1. **Access Authorization**: Users will only be granted access following an approved business authorization request.
2. **Role Changes**: If an employee changes roles, their access rights must be reviewed and adjusted accordingly. Upon termination, all access rights will be revoked, and accounts will be disabled or deleted.
3. **Inactive Accounts**: User accounts inactive for a specified period will be disabled and later deleted.
4. **Annual Review**: Role-based permissions and individual user rights will be reviewed annually to ensure compliance with business needs.
5. **Privileged Accounts**: Privileged accounts (e.g., admin accounts) will be reviewed annually, and any changes must be approved and documented.
6. **Function-Specific Accounts**: Accounts used by teams for specific functions must be managed under strict access control policies; ensuring no unauthorized access occurs.

7. Cyber Security and Governance Policy

7.1 Policy Statement

PNY will ensure secure access to cloud services and maintain the confidentiality, availability, and integrity of data hosted in cloud environments.

7.2 Scope

This policy applies to:

- All information systems, assets, and applications hosted on public, private, or hybrid cloud platforms.

7.3 Responsibilities

Role	**Responsibility**
IT Head	Ensure compliance with cyber security and governance policies. Enforce security controls for cloud infrastructure.
Information System Steering Committee (ISSC)	Manage policy rollout and periodic reviews. Ensure cloud governance aligns with PNY's cyber security policies.

7.4 Guidelines

1. **Cloud Provider Agreements**: A master service agreement (MSA) must be maintained with the cloud service provider, including service level agreements (SLA) for security measures.
2. **Breach Notifications**: The cloud provider must notify PNY of any security breaches, regardless of data directly impacted.
3. **Data Location Awareness**: PNY must be aware of the data location and ensure compliance with local regulatory requirements, especially if multi-jurisdictional operations are involved.
4. **ISO/IEC Compliance**: The cloud provider must maintain ISO/IEC 27001 certification for data security.
5. **Data Encryption**: Data must be encrypted both at rest and during transit, complying with RBI guidelines for cryptographic protocols.
6. **Cloud Data Center Location**: As per RBI guidelines, PNY's data must be hosted in India, and the cloud provider must comply with these regulations.
7. **Remote Access Security**: Remote workers or service providers accessing cloud-hosted data must use encrypted channels such as VPN/IPSEC for secure access.

8. Incident Management Policy

8.1 Policy Statement

All information security incidents will be reported, promptly addressed, and steps will be taken to prevent recurrence.

8.2 Scope

This policy applies to:

- All PNY information assets, employees, and third-party personnel accessing company systems.

8.3 Responsibilities

Role	Responsibility
Users	Report any suspected incidents immediately.
IT Head	Validate and respond to incidents. Track incidents through closure and ensure corrective actions are implemented.

8.4 Procedures

1. **Incident Identification**: Any abnormal activity or event, such as unauthorized access attempts, system failures, or virus outbreaks, must be identified as a potential incident.
2. **Incident Reporting**: All users must report incidents immediately to the IT Helpdesk. The Helpdesk will log the incident and escalate it to the Incident Management Team.
3. **Incident Assessment**: The Incident Management Team will assess and validate the reported incident and determine the level of damage or disruption caused.
4. **Incident Recovery**: Recovery efforts will begin immediately to contain the incident and prevent further damage. This will include identifying and eliminating the root cause of the incident.
5. **Post-Incident Analysis**: The IT head will compile an incident report detailing the cause, impact, and corrective actions taken, which will be presented to management.

9. Batch Job Policy

9.1 Policy Statement

Batch jobs will be automated and scheduled to run without manual intervention, ensuring critical processes are performed regularly.

9.2 Scope

This policy applies to:

- All batch jobs involving PNY's IT assets, including databases and applications.

9.3 Responsibilities

Role	Responsibility
Database Administrator (DBA)	Ensure batch jobs are executed successfully. Address any exceptions with priority.
IT Head	Oversee the implementation and enforcement of the batch job policy.

9.4 Guidelines

1. **Batch Scheduling**: Critical batch jobs, such as database log shipping or real-time transaction integration, will be scheduled during office hours. Non-critical jobs (e.g., HR leaves updates) will be scheduled outside of office hours.
2. **Monitoring and Logging**: Any exceptions or errors in the batch job process must be logged and addressed immediately.
3. **Day-End and Day-Begin Jobs**: End-of-day processes (e.g., updating EMI charts) and beginning-of-day processes (e.g., moving settled loan files to history) must be clubbed together for efficiency.

10. Physical Access Control Policy

10.1 Policy Statement

PNY will implement stringent physical access controls to safeguard IT infrastructure hosted in data centers.

10.2 Scope

This policy applies to:

- All physical security measures and controls protecting information assets within PNY's data center.

10.3 Responsibilities

Role	Responsibility
IT Head	Ensure implementation of physical security controls at the data center. Maintain documentation on the physical infrastructure layout and security.
Users	Follow procedures for accessing physical IT assets and data center environments

10.4 Guidelines

1. **Role-Based Access**: Only individuals whose job roles require access to the data center will be authorized, with approvals documented.
2. **Authentication Mechanism**: Biometric verification or other secure mechanisms will be used to authenticate individuals entering the data center.
3. **Visitor Management**: All visitors, including contractors, must be pre-registered, escorted by authorized employees, and logged upon entry and exit.
4. **Surveillance**: CCTV cameras will be installed at all entry points and within the data center, with footage securely stored for at least 90 days.
5. **Physical Security**: All entry points will be monitored and environmental controls such as fire suppression and UPS systems will be in place to protect critical assets.

11. Enforcement

Compliance with this IT and IS policy will be subject to regular reviews by the IT department. Employees found violating the policy may face disciplinary actions, including termination, depending on the severity of the infraction, as determined by management and Human Resources.