NIST CSF Policies Document

1. Asset Management Policy (Identify - ID.AM-1 & ID.AM-2)

Purpose

To ensure all physical and digital assets are inventoried, tracked, and managed to reduce cybersecurity risks.

Scope

This policy applies to all hardware, software, systems, and data assets owned or managed by the organization.

Policy

- All assets must be documented in an asset inventory.
- Each asset must have an assigned owner.
- Inventories must be reviewed and updated quarterly.
- Asset records should include device type, location, assigned user, and classification (confidential, internal, public).

Responsibilities

- IT department: Maintain and audit inventory.
- Asset owners: Ensure updates when changes occur.

Enforcement

Non-compliance with this policy may result in corrective action, such as restricted access to systems or an internal review to ensure alignment with asset management procedures.

---

2. Access Control Policy (Protect - PR.AC-1)

Purpose

To ensure that access to information systems and data is limited to authorized users.

Scope

Applies to all employees, contractors, and third parties accessing company systems.

Policy

- Access rights must follow the principle of least privilege.
- All users must have unique user IDs.
- Multi-factor authentication (MFA) must be implemented for remote access.
- Access reviews are conducted quarterly.

Responsibilities

- System Administrators: Manage user accounts and permissions.
- HR Department: Notify IT of employee role changes or departures.

Enforcement

Failure to follow this policy may lead to temporary access suspension and a review by the IT or Security team to determine appropriate next steps.

---

3. Acceptable Use Policy – AUP (Protect - PR.AT-1)

Purpose

To define acceptable and unacceptable use of the organization’s information technology resources to protect data, networks, and reputation.

Scope

Applies to all employees, contractors, consultants, interns, and other authorized users who access or use the organization's IT assets.

Policy

3.1 Permitted Use

- IT resources are provided for legitimate business purposes.
- Occasional personal use is allowed if it does not:
  - ✓ Interfere with work duties.
  - ✓ Violate any other policies.
  - ✓ Consume excessive network resources.

3.2 Prohibited Use

Users must not:

- Access, transmit, or store offensive, pornographic, or illegal material.
- Attempt to bypass security controls or access unauthorized data.
- Use organization systems for personal profit, gambling, or political campaigning.
- Download or install unlicensed or unauthorized software.
- Connect personal devices to the corporate network without approval.

3.3 Email and Communication

- Organizational email must be used professionally.
- Users must not send bulk unsolicited emails (spam) or phishing messages.
- Confidential information should only be sent using secure methods (e.g., encryption).

3.4 Internet Usage

- Internet access must be used responsibly.
- Access to certain websites (e.g., adult content, torrenting, gaming) may be blocked or monitored.

3.5 Device and Password Use

- Devices must be password-protected and locked when unattended.
- Passwords must be complex and not shared.
- Users must report lost or stolen devices immediately.

3.6 Monitoring and Privacy

- The organization reserves the right to monitor all IT usage.
- Users should not expect personal privacy when using company systems.

Responsibilities

- All Users: Adhere to this policy and report violations.
- IT Department: Monitor usage, enforce policy, and provide guidance.

Enforcement

Violations of this policy may result in:

- Disciplinary action (including termination).
- Revocation of system access.
- Legal prosecution or other measures in line with HR and IT guidelines.

---

4. Security Awareness & Training Policy (Protect - PR.AT-1)

Purpose

To ensure all personnel are aware of cybersecurity threats and are trained to reduce risk.

Scope

Applies to all employees and contractors.

Policy

- All employees must complete cybersecurity training upon onboarding.
- Annual refresher training is mandatory.
- Phishing simulations will be conducted quarterly.
- Training records must be maintained for audit purposes.

Responsibilities

- Security team: Develop and deliver training materials.

- Managers: Ensure team participation.

Enforcement

Employees who do not complete mandatory training may have system access temporarily limited and may be required to attend follow-up sessions.

---

5. Incident Response Policy (Respond - RS.RP-1 & RS.CO-1)

Purpose

To define the organization's approach to detecting, reporting, responding to, and recovering from cybersecurity incidents.

Scope

Covers all systems and personnel involved in incident detection and response.

Policy

- All incidents must be reported to the security team immediately.
- A Computer Incident Response Team (CIRT) will be activated for major incidents.
- All incidents must be documented and reviewed.
- Lessons learned must be integrated into security processes.

Responsibilities

- Employees: Report suspected incidents immediately.
- CIRT: Manage the incident lifecycle and communication.

Enforcement

Failure to report or properly handle incidents may prompt a review by the Information Security team, and corrective steps will be taken as appropriate.

---

6. Backup & Recovery Policy (Recover - RC.RP-1)

Purpose

To ensure timely recovery of systems and data following a cybersecurity incident.

Scope

Covers backup, restoration, and business continuity practices.

Policy

- Critical data must be backed up daily.
- Backups must be tested monthly.
- Recovery procedures must be documented and available.
- Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) must be defined for critical systems.

Responsibilities

- IT Department: Manage and test backup systems.
- Department Heads: Define RTO/RPO for their systems.

Enforcement

Non-compliance may impact disaster recovery capabilities and result in disciplinary action.

Departments or teams found to be out of compliance with this policy may be subject to review and process adjustments to reduce future risk.

---

7. Business Continuity Policy – BCP (Recover – RC.RP-1)

Purpose

The purpose of this policy is to establish a framework for maintaining or restoring business operations during and after an unexpected disruption, such as cyberattacks, natural disasters, or critical system failures.

Scope

This policy applies to all departments, personnel, systems, and operations essential to the continuity of X Bank's services.

Policy

7.1 Business Impact Analysis (BIA)

- A BIA must be conducted at least annually to identify critical business processes and their dependencies.
- Each department must identify acceptable Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

7.2 Business Continuity Plans

- Every critical department must maintain a documented and approved Business Continuity Plan.
- Plans must define procedures for operating during outages and step-by-step instructions for recovery.
- Backup communication strategies (e.g., alternate email or phone systems) must be included.

7.3 Backup and Recovery

- Critical data must be backed up regularly according to the organization's data backup policy.
- Backup systems must be tested monthly for recoverability.
- Redundant infrastructure must be available where feasible.

7.4 Testing and Exercises

- BCP exercises (tabletop or simulation) must be conducted at least once a year.
- Gaps and lessons learned must be documented and used to update the BCP.

7.5 Roles and Responsibilities

- Each department head is responsible for maintaining their area's business continuity readiness.
- The BCP Coordinator oversees the enterprise-wide continuity planning and coordinates periodic reviews.

7.6 Documentation and Storage

- All BCP documentation must be securely stored both physically and digitally, with restricted access.
- Updated copies must be available to all relevant stakeholders during an incident.

Responsibilities

- Executive Management: Approve the BCP policy and ensure funding for resilience initiatives.
- IT Department: Maintain systems necessary for continuity (e.g., backup systems, failovers).
- BCP Coordinator: Develop and update plans, coordinate training and testing.
- Employees: Be aware of their roles in the BCP and participate in training and exercises.

Enforcement

Non-compliance with this policy may result in corrective action, including reassignment of responsibilities or additional training, to ensure resilience objectives are met.