Security Policy Review Report

1. Introduction

This report presents a review and enhancement of three fundamental security policies essential to any organization's cyber security framework:

- **Access Control Policy**
- **Data Protection Policy**
- **Incident Response Policy**

These policies were selected based on their critical role in protecting data, regulating user access, and managing security incidents. The review process involved comparing the existing policies against globally recognized standards and best practices — primarily **NIST Cyber security Framework** and **ISO/IEC 27001** — to identify gaps and areas of improvement.

Templates and references from the **SANS Security Policy Library** and **Infosec Institute** were also used to guide the structure and content of each updated policy.

2. Policy Scope and Importance

Access Control Policy

Defines how users gain access to organizational systems, data, and resources. It ensures that only authorized individuals can access specific systems or information, based on roles and responsibilities.

Data Protection Policy

Outlines how the organization collects, stores, processes, and protects sensitive and personal data. It ensures compliance with legal requirements and defends against data breaches.

Incident Response Policy

Provides a formal process for detecting, reporting, and responding to security incidents to minimize their impact and prevent recurrence.

3. Assessment of Existing Policies

Access Control Policy

Strengths:

- Role-based access defined
- General authentication requirements in place

Weaknesses Identified:

- No multi-factor authentication (MFA)
- No periodic access reviews
- Weak password complexity standards

Action Needed:

- Update with stronger authentication requirements.

Reference Standard Used:

- **NIST SP 800-53 Rev. 5 (AC Family)**
- **ISO/IEC 27001:2022 – Annex A.9: Access Control**

Data Protection Policy

Strengths:

- Data classification levels defined
- Basic encryption mentioned

Weaknesses Identified/Gaps:

- No mention of data retention or disposal policies
- Missing BYOD (Bring Your Own Device) rules
- Lacks cloud data security measures

Action Needed:

- Add rules for Bring Your Own Device (BYOD) and data access logs.

Reference Standard Used:

- **NIST SP 800-171 (Protecting CUI)**
- **ISO/IEC 27001 – Annex A.8: Asset Management, A.18: Compliance**

Incident Response Policy

Strengths:

- Defined incident types
- Initial incident reporting process present

Weaknesses Identified/Gaps:

- No incident response team roles defined
- No post-incident review process
- Lacks communication and escalation steps

Action Needed:

- Add steps for notifying teams and learning from incidents.

Reference Standard Used:

- **NIST SP 800-61r2: Computer Security Incident Handling Guide**
- **ISO/IEC 27001 – Annex A.16: Information Security Incident Management**

4. Enhancements Based on Industry Best Practices

Access Control Policy (Updated)

- Enforced **multi-factor authentication** across all critical systems
- Updated password requirements to follow **NIST SP 800-63B**
- Implemented **bi-annual user access reviews**
- Added principle of **least privilege** enforcement

Data Protection Policy (Updated)

- Introduced **data retention and disposal policy**
- Added secure use policies for **personal and mobile devices**
- Required encryption for data **at rest and in transit**
- Introduced classification labels for internal, confidential, and public data

Incident Response Policy (Updated)

- Created **Incident Response Team (IRT)** with defined roles
- Added a 4-phase incident response lifecycle: **Preparation, Detection & Analysis, Containment/Eradication, and Recovery** (per NIST 800-61r2)
- Included **incident communication plan** for internal and external notifications
- Required **post-incident reports and corrective actions**

5. Implementation Plan

Each updated policy was rewritten using a blend of:

- **SANS Security Policy Templates**: Provided ready-made frameworks
- **Infosec Institute Templates**: Offered industry examples
- **NIST & ISO 27001 Standards**: Guided security control language and technical accuracy

Actions Taken:

- Created 3 updated policy documents in DOC and PDF formats
- Shared policies with IT and compliance teams for internal review
- Scheduled quarterly training to enforce the new rules
- Added policy reviews to annual audit checklist

---

6. Recommendations

1. **Review all policies every 12 months** to ensure compliance and relevance
2. **Train staff twice per year** on security awareness and policy changes
3. **Audit user access** and data use quarterly
4. **Conduct mock incident drills** to test the new Incident Response Policy
5. Monitor updates from **NIST**, **ISO**, and **cyber security advisories**

7. References

NIST Cyber security Framework – https://www.nist.gov/cyberframework

ISO/IEC 27001 – https://www.iso.org/isoiec-27001-information-security.html

SANS Security Policy Templates – https://www.sans.org/information-security-policy/

Infosec Institute Policy Templates – https://resources.infosecinstitute.com/
