**Security Policy Review and Enhancement Report**

**InternIntelligence Task 4**

**1. Introduction**

Security policies are essential for ensuring the protection of an organization's digital assets, data, and IT infrastructure. This report evaluates existing security policies, identifies gaps, and proposes enhancements based on industry best practices such as **ISO 27001, NIST Cybersecurity Framework, and GDPR compliance**.

**2. Security Policy Assessment**

A review of existing policies was conducted, focusing on key areas such as:

**✔ Information Security Policy**

* Ensures protection of sensitive organizational data.
* **Issue Identified:** Lack of clear data classification guidelines.
* **Improvement:** Introduce a **data classification framework** (Confidential, Internal, Public).

**✔ Access Control Policy**

* Manages user access to critical resources.
* **Issue Identified:** No multi-factor authentication (MFA) enforcement.
* **Improvement:** Implement **MFA for all privileged accounts**.

**✔ Incident Response Policy**

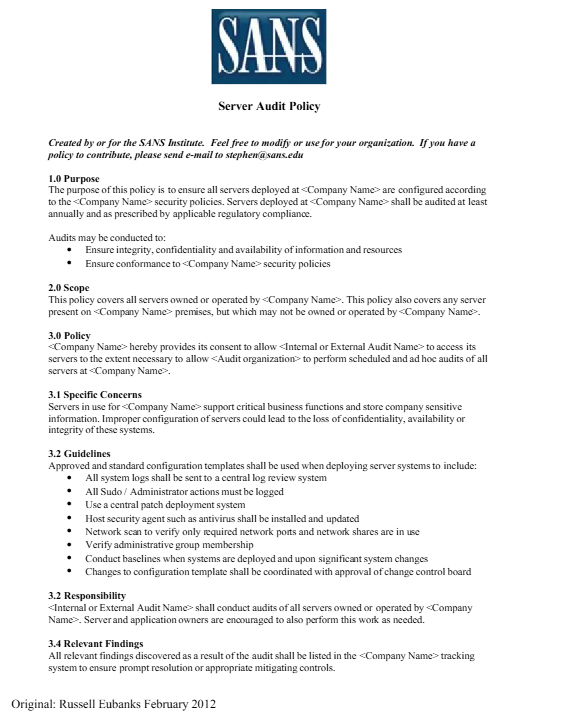
* Defines how security incidents are managed.
* **Issue Identified:** No structured incident response playbook.
* **Improvement:** Develop **a detailed incident response plan** following **NIST SP 800-61 guidelines**.

**✔ Network Security Policy**

* Ensures secure access to internal and external networks.
* **Issue Identified:** Weak firewall and intrusion detection rules.
* **Improvement:** Strengthen firewall configurations and implement **Intrusion Detection/Prevention Systems (IDS/IPS)**.

**✔ Data Protection Policy**

* Ensures compliance with data protection laws (GDPR, ISO 27001).
* **Issue Identified:** No clear **data retention policy**.
* **Improvement:** Define **data retention & deletion periods** based on legal requirements.

****