# Security Policy Review and Enhancement

To effectively review and enhance an organization’s security policies and procedures, a structured approach is necessary. We can use a template of policies to review and enhance. It focuses on guiding employees on appropriate use of an organization's IT assets, data, and network resources. The policy outlines expectations for system usage, security, and compliance, ensuring that employees act responsibly to protect the organization from cyber risks.

## Analysis:

**Overview**:

- The document emphasizes protecting the organization's assets and systems while promoting a culture of openness and integrity.
- It covers a wide range of systems and technologies, including internet, intranet, devices, and network services.

**Purpose**:

- The purpose is to outline acceptable use to safeguard the company from risks like virus attacks, data breaches, and legal issues.
- There’s a clear intent to align the policy with security standards and minimize exposure to threats.

**Scope**:

- The policy applies to all employees, contractors, and third parties using company-owned or leased devices and resources.
- It also covers devices owned by employees but used to access company resources.

**Key Areas**:

- **General Use and Ownership**: Employees must protect proprietary information, avoid unauthorized disclosure, and ensure reasonable personal use.
- **Security and Proprietary Information**: Focus on password policies, securing devices, and preventing unauthorized access.
- **Unacceptable Use**: A comprehensive list of prohibited actions such as unauthorized copying of software, introducing malicious programs, and security breaches.
- **Email and Communication**: Addresses issues like unsolicited emails, harassment, and proper use of company communication channels.
- **Blogging and Social Media**: Covers restrictions on social media and blogging to prevent harm to the company's reputation and protect proprietary information.

**Compliance**:

- The policy includes regular audits, compliance checks, and strict penalties for violations.
- It aligns with related standards, such as data classification, password policy, and minimum access guidelines.

# 4. Policy

## 4.1 General Use and Ownership

4.1.1 <Company Name> proprietary information stored on electronic and computing devices whether owned or leased by <Company Name>, the employee or a third party, remains the sole property of <Company Name>. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard.*

4.1.2 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of <Company Name> proprietary information.

4.1.3 You may access, use or share <Company Name> proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within <Company Name> may monitor equipment, systems, and network traffic at any time, per Infosec's *Audit Policy*.

4.1.6 <Company Name> reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

## 4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the *Minimum Access Policy*.

4.2.2 System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected lock screen with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4 Postings by employees from a <Company Name> email address to newsgroups or other online platforms, should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of <Company Name>, unless posting is during business duties.

4.2.5 Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

### 4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of <Company Name> authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing <Company Name>-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

#### 4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

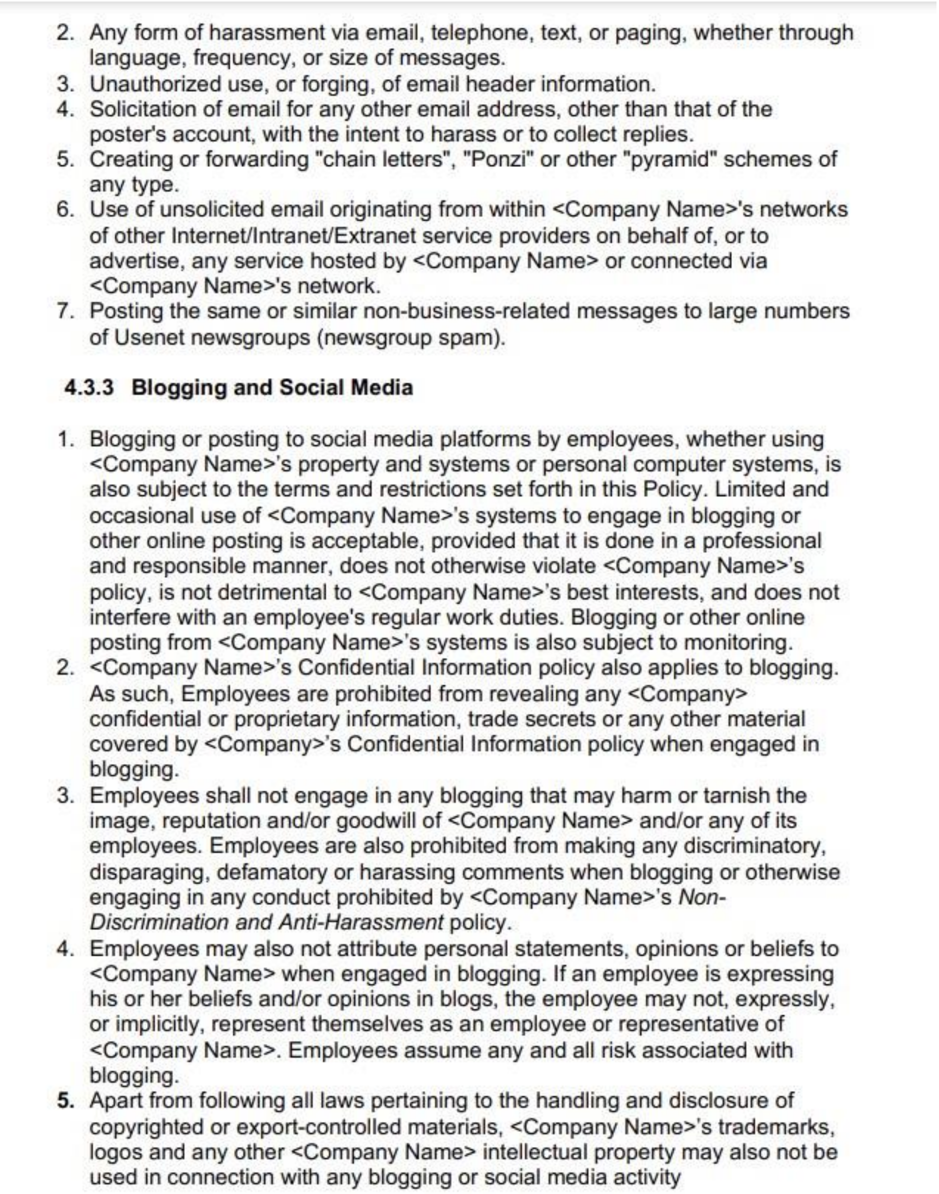
1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by <Company Name>.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which <Company Name> or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server, or an account for any purpose other than conducting <Company Name> business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, trojan horses, ransomware, etc.).

6. Revealing your account password/passphrase to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a <Company Name> computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any <Company Name> account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, brute-forcing accounts, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to the Infosec Team is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network, or account.
14. Introducing honeypots, honeynets, or similar technology on the <Company Name> network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, <Company Name> employees to parties outside <Company Name>.

### 4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).



2. Any form of harassment via email, telephone, text, or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within <Company Name>'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by <Company Name> or connected via <Company Name>'s network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

**4.3.3 Blogging and Social Media**

1. Blogging or posting to social media platforms by employees, whether using <Company Name>'s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of <Company Name>'s systems to engage in blogging or other online posting is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate <Company Name>'s policy, is not detrimental to <Company Name>'s best interests, and does not interfere with an employee's regular work duties. Blogging or other online posting from <Company Name>'s systems is also subject to monitoring.
2. <Company Name>'s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any <Company> confidential or proprietary information, trade secrets or any other material covered by <Company>'s Confidential Information policy when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of <Company Name> and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by <Company Name>'s *Non-Discrimination and Anti-Harassment* policy.
4. Employees may also not attribute personal statements, opinions or beliefs to <Company Name> when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of <Company Name>. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, <Company Name>'s trademarks, logos and any other <Company Name> intellectual property may also not be used in connection with any blogging or social media activity

## **Assessment and Enhancement**:

1. Access Control:

The policy includes basic password requirements and access control but does not mention advanced practices such as multi-factor authentication (MFA).
**Enhancement**: Strengthen the access control section by enforcing MFA for all employees accessing sensitive data and systems. Also, integrate role-based access control (RBAC) for enhanced user privilege management.

2. Data Protection:

The policy touches upon proprietary information protection but lacks details on encryption methods or compliance with data privacy regulations (GDPR, HIPAA).
**Enhancement**: Implement AES-256 encryption for sensitive data at rest and in transit. Include guidelines on complying with global privacy regulations and securing data backups.

3. Incident Response:
There’s no specific mention of an incident response plan.
**Enhancement**: Add a dedicated section on incident response to address how employees should report breaches, phishing attempts, or data loss. Align it with NIST SP 800-61 guidelines for effective incident handling, including roles, escalation procedures, and post-incident reviews.

This comprehensive approach will improve security measures, align policies with industry standards (e.g., NIST, ISO 27001), and better protect the organization from evolving cyber threats.

In addition to the initial areas of **access control**, **data protection**, and **incident response**, the policy can be further enhanced in the following ways:

### 1. Monitoring and Auditing

The current policy briefly mentions that authorized individuals can monitor systems and traffic, but it does not specify the methods or frequency of audits.
**Enhancement**:
Clearly define the scope, frequency, and type of monitoring (e.g., real-time monitoring, anomaly detection tools) to be used. Add periodic internal and external security audits, penetration tests, and vulnerability assessments to identify weaknesses in the system. Ensure logging is consistent with security best practices, capturing critical security events like failed login attempts, unauthorized access, and changes to user roles. Specify the tools and technologies used for monitoring (e.g., Intrusion Detection Systems

(IDS), Security Information and Event Management (SIEM)) and ensure compliance with legal and privacy requirements for monitoring employees.

## 2. Data Privacy and Compliance

While the policy covers data protection, it lacks specific references to **data privacy laws** and compliance requirements (e.g., GDPR, HIPAA, CCPA).
**Enhancement**:
Integrate policies that ensure compliance with global privacy regulations, including the protection of personally identifiable information (PII), data retention periods, and the legal basis for data processing. Provide specific data privacy controls and outline employee responsibilities for protecting customer and employee PII. Establish guidelines for data anonymization, pseudonymization, and secure deletion practices to further protect data in case of a breach.

## 3. Remote Work and Bring Your Own Device (BYOD) Policies

The policy mentions company-owned devices and includes general guidelines for personal use but lacks comprehensive rules for remote work and BYOD.
**Enhancement**:
Develop clear guidelines for remote work security, including: Use of company-approved Virtual Private Networks (VPNs) and encryption when accessing internal resources. Regularly updated security software, firewalls, and antivirus on personal devices used for work. Secure storage and handling of sensitive data when working remotely. Expand the BYOD policy to ensure that personal devices used for work comply with security requirements, such as:

- Mandatory installation of Mobile Device Management (MDM) software for remote device monitoring and security updates.
- Remote wipe capabilities in case of lost or stolen devices.
- Segregation of personal and work data to avoid unauthorized data exposure.

### 4. Password Management and Authentication

The current policy includes general password policies but lacks advanced practices like password complexity, expiration, and management tools.
**Enhancement**:
Strengthen password management by enforcing the use of password managers, encouraging complex password creation, and mandating regular password expiration (e.g., every 90 days). Introduce policies for Single Sign-On (SSO) and further strengthen authentication with biometric methods where possible. Implement Zero Trust Architecture principles, such as continuously validating user identity and behavior, particularly for privileged access accounts.

### 5. Security Awareness Training

Although the policy requires good judgment by employees, it lacks structured security awareness training for employees and contractors.
**Enhancement**:
Make security awareness training mandatory for all employees at onboarding and as part of ongoing annual training. Training should cover:

- Phishing attacks, social engineering, and how to identify malicious emails.
- Handling sensitive information, encryption basics, and secure communications.
- Incident response procedures and reporting mechanisms.

Include simulated phishing exercises to regularly test employee responses to phishing attacks and improve organizational readiness. Establish a recognition system for employees who demonstrate strong security practices.

### 6. Vendor and Third-Party Risk Management

The policy briefly mentions third-party workers but does not address the risks posed by vendors or contractors who have access to company systems and data.

**Enhancement**:
Implement a vendor management policy that requires third-party vendors and contractors to comply with the same security standards as internal employees. Conduct risk assessments for all third parties with access to sensitive data or systems, including:

- Regular security reviews of third-party practices.
- Mandating adherence to industry standards like ISO 27001 or SOC 2 for vendors.

Establish a vendor contract clause that includes data breach notification requirements, periodic audits, and a right to terminate contracts if security is compromised.

### 7. Physical Security

The policy focuses heavily on digital security, but there is limited mention of **physical security measures**.
**Enhancement**:
Define physical access control measures, such as **b**adge systems, biometric entry, and CCTV monitoring, to ensure only authorized personnel have access to sensitive areas like data centers. Specify rules for visitors and contractors to ensure they are monitored and restricted from accessing critical systems. Implement policies for the secure disposal of physical hardware (e.g., hard drives, USBs) to ensure no sensitive information is exposed through discarded hardware.

### 8. Cloud Security

The policy does not address **cloud computing** or how cloud services should be secured.
**Enhancement**:
Establish a cloud security policy that ensures data encryption both at rest and in transit within the cloud. Define roles and responsibilities between the organization and cloud service providers (shared responsibility model). Implement secure access control for cloud services using tools such as SSO and MFA for all cloud applications. Mandate regular security

assessments of cloud providers, ensuring they comply with SOC 2 and ISO 27001 standards.

### 9. Policy Version Control and Updates

The policy mentions updates but lacks a clear version control system or structured update process.

**Enhancement**:

Introduce a version control system that tracks updates and revisions to the policy, including who made the changes and why. Set a schedule for periodic reviews (e.g., annually or bi-annually) to ensure policies are updated based on evolving threats and new technologies. Implement a feedback mechanism so employees can report gaps or suggest improvements for future policy iterations.

### Conclusion:

By enhancing these areas, the organization's security posture will be strengthened, and the policy will become more comprehensive, covering both current and emerging risks. The enhancements ensure alignment with industry standards and will help the organization remain safe against internal and external threats.