< Organization Name>

Email Cybersecurity Policy With NIST Framework

V0.1 2025-04-04

This document is based on a cybersecurity policy with NIST frameworks provided by Ok TECH Solutions.

Ok TECH Solutions grants permission for the template document to be modified in any manner < Organization Name> wishes, provided this acknowledgment remains in place.

Document Owner: <Person's Name>

Contact: <Person's email and/or mobile telephone>

Document Approval

Role	Job title	Name	Date	Signature
Choose Role	Insert Job Title	Insert Individuals full personal name	Click here to add date	Insert Signature

Mail Policy Review

Electronic Mail policy					
Policy		Effective Date	March/03/31	Email	Mail@Companyx.com
Version	12.0	Contact	0976992323		

How To Use This Document

This is an Email policy document. It contains suggestions or recommend content. It is content that can be freely added to, moved, modified or deleted. Do not feel obliged to use the content as is if it does not suit your organization. You should read and adopt, adapt or remove as appropriate.

What to do:

1. This document uses generic text for certain items that need to be updated by the organization. These template text items are formatted in red with angle brackets (e.g. <Organisation Name> representing the organization's name), and should be updated to replace the template text with appropriate text specific to the organization.
2. Using global replace, change <Organisation Name> to the organization's name
3. On the front page and in the page headers, change the Document Title to remove " [Template]" from the title, if present
4. On the front page and in the page footers, update the <Document Version & Date> to a new version of this document after your editing, and as you edit it in the future; e.g. V1.5 2025-05-05
5. Edit the document header to include the organization's logo, or remove the <Organisation Logo> template text
6. Find any other template text items and update them with the appropriate text for the organization
7. Review all the content and change anything as required to meet the organization's requirements and circumstances-sections and text can be modified, moved, deleted or added
8. Update the Contents table after updates by clicking on "Contents" and "Update Table…"; you may occasionally be prompted and can "Update entire table"
9. When ready, delete these instructions on this page and update the Contents again
10. Save the updated document

Contents

Definitions

1. Phishing: A fraudulent attempt to obtain sensitive information by masquerading as a trustworthy entity in electronic communications.

2. Unauthorized Access: Gaining access to systems, networks, or data without permission.

3. Spam: Unsolicited and often irrelevant or inappropriate messages sent over the internet, typically to a large number of users.

4. Encryption: The process of converting information or data into a code to prevent unauthorized access.

5. Authentication: The process of verifying the identity of a user or system.

6. Cybersecurity: is the set of technologies, processes, and practices designed to safeguard information and systems from cyber threats such as hacking, malware, phishing, ransomware, and data breaches.

7. Access control : is a security technique that determines who is allowed to access or use information and resources, and under what conditions.

8. Incident response: is the process of identifying, managing, recording, and analyzing security threats or incidents in real time, with the goal of minimizing damage and reducing recovery time and costs.

9. Risk assessment: is a systematic process used to evaluate the potential risks that may affect an organization ' s assets, operations, or individuals, with the goal of implementing appropriate safeguards or controls.

10. Framework: A framework is a conceptual structure used to support or guide the creation of something complex, such as policies, strategies, or systems—especially in areas like cybersecurity, project management, or software development.

11. NIST(National Institute of Standards and Technology): NIST Cybersecurity Framework is a voluntary, risk-based framework that provides a common language and structured approach for organizations to assess and improve their ability to prevent, detect, and respond to cyber threats.

Literature Review

Email remains a primary communication channel in organizations but also a significant vector for security threats such as phishing, malware, data leakage, and impersonation attacks. Email security policies are essential components of broader cybersecurity frameworks, designed to establish standards for secure email use, employee responsibilities, and technical controls.

1. **Evolution and Importance of Email Security Policies**

Several studies underscore the growing need for robust email security policies due to increasing cyberattacks. According to Hadnagy (2018), email is the most exploited attack vector, often serving as the entry point for social engineering and phishing schemes. The literature emphasizes that security policies must evolve with threats, adopting a dynamic, proactive stance (Alshaikh et al., 2020).

2. **Components of an Effective Email Security Policy**

Key elements commonly identified in the literature include:

- Access Control: Guidelines on authentication, authorization, and identity verification (ISO/IEC 27001:2013).
- Content Filtering and Encryption: Use of spam filters, malware detection, and encryption protocols (SANS Institute, 2021).
- User Training and Awareness: Regular training to recognize phishing attempts and suspicious behavior (Abawajy, 2014).
- Acceptable Use Policies (AUP): Clear instructions on appropriate and inappropriate use of email systems.
- Incident Response: Steps to follow in the event of a security breach involving email.

3. **Challenges in Policy Implementation**

Implementation gaps are often due to a lack of awareness, inadequate enforcement, or insufficient executive support (Knapp et al., 2009). Literature points out that many organizations have policies on paper that are poorly communicated or understood by employees.

4. **Regulatory and Compliance Considerations**

Email policies must align with regulations such as GDPR, HIPAA, and others, which impose strict rules on data handling and confidentiality. Compliance-driven policy design is a major theme in recent research (Cavusoglu et al., 2015).

5 **Emerging Trends in Email Security Policy**

- Zero Trust Models: Policies increasingly favor zero-trust principles, minimizing implicit trust in email communications.
- AI and Automation: Incorporating AI to detect phishing and automate policy enforcement is gaining ground (Symantec, 2022).
- Cloud-Based Email Security: The shift to cloud services like Microsoft 365 and Google Workspace introduces new policy challenges and solutions.

1. Introduction

Email is a critical communication tool for organizations but also a primary target for cyber threats such as phishing, malware, business email compromise (BEC), and data leaks. This Email Security Policy establishes guidelines to protect email communications, ensuring data confidentiality, integrity, and availability while mitigating security risks.

This policy aligns with the NIST Cybersecurity Framework (CSF) and industry best practices by implementing security controls across five core functions: Identify, Protect, Detect, Respond, and Recover.

2. Objectives

The primary objectives of this policy are to:

- Prevent unauthorized access, data breaches, and cyber threats targeting email systems.
- Ensure compliance with NIST 800-53, NIST 800-171, ISO 27001, GDPR, HIPAA, and other regulatory requirements.
- Define security measures to protect email communication from phishing, malware, and unauthorized data sharing.
- Establish a framework for email monitoring, incident response, and recovery.
- Promote user awareness and secure email usage practices.

3. Scope

This policy applies to all employees, contractors, third-party vendors, and any individuals who use the organization's email system. It covers:

- Corporate email accounts (e.g., owentromy50company@gmail.com).
- Personal email usage for business communications (if applicable).
- Webmail, mobile access, and third-party email services integrated with corporate systems.
- Email clients, cloud-based email solutions, and security configurations.

4. Policy Statement

General Requirements

1-1 The necessary technologies to protect the confidentiality, integrity, and availability of email messages during transmission and storage must be used and updated constantly.

1-2 Email protection, analysis, and filtering technologies must be used to block suspicious email messages, such as spam and phishing email messages.

1-3 The necessary technologies, such as Data Leakage Prevention(DLP), must be used to protect data against leakage via email from inside or outside <organization name>.

1-4 Technologies must be used to protect email servers against Advanced Persistent Threats (APTs) and zero-day malware.

1-5 Technologies must be used to inspect email message attachments and links in a sandbox before they reach the user's mailbox, whether such email messages are sent from inside or outside

1-17 Open mail relay services must be disabled on the server.

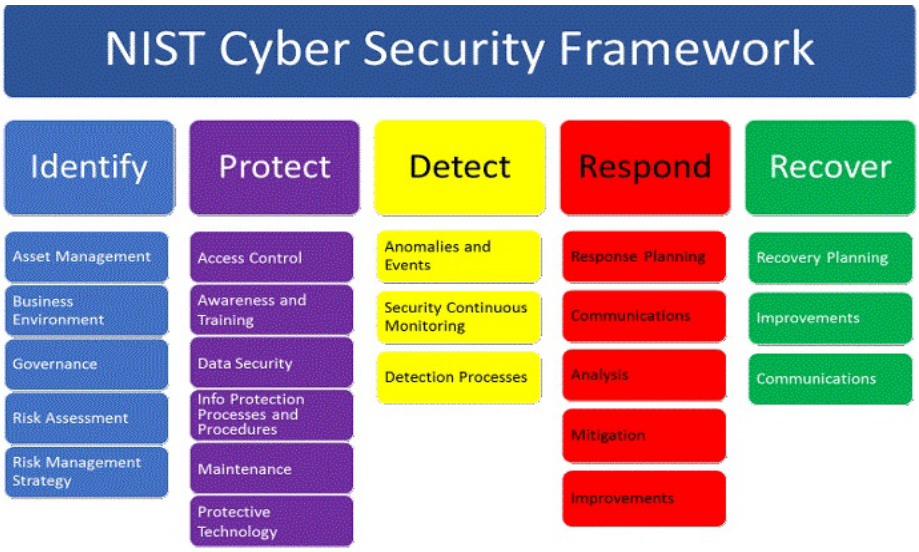
1-18 The use of email must be prohibited for privileged accounts.

1-19 Connections between email gateways must be encrypted to prevent inactive man-in-the-middle attacks.

1-20 <cybersecurity function> must ensure the cybersecurity awareness of all personnel and educate them to handle secure email services and detect phishing emails.

1-21 Key Performance Indicators (KPIs) must be used to ensure the continuous improvement and efficient and effective use of email protection requirements.

This policy is designed in line with NIST Cybersecurity Framework and its core functions which are Identify, Protect, Detect, Respond and Recover. Below is an illustration of NIST framework.



A. Identify (Asset & Risk Management)

- Maintain an inventory of email accounts, users, and associated access rights.
- Classify email data based on sensitivity (e.g., public, internal, confidential, restricted).
- Conduct regular risk assessments to identify email-related threats (e.g., phishing, spoofing, insider threats).

B. Protect (Access Control & Security Measures)

- Authentication & Access Control:
- Enforce Multi-Factor Authentication (MFA) for all email accounts.
- Implement role-based access control (RBAC) to limit email access.
- Email Encryption & Data Protection:
- Encrypt emails containing sensitive information in transit and at rest.
- Use Data Loss Prevention (DLP) tools to detect and block unauthorized sharing of confidential data.
- Anti-Phishing & Anti-Malware Measures:

- Deploy email filtering solutions (e.g., spam filters, attachment scanning, URL filtering).
- Block emails from known malicious domains and IP addresses.
- Train employees on identifying phishing attempts and business email compromise (BEC) attacks.
- Device Security:
- Enforce email security policies on company-owned and personal devices.
- Require automatic security updates for email clients.

C. Detect (Threat Monitoring & Incident Detection)

- Use SIEM (Security Information and Event Management) for email log monitoring.
- Enable alerts for suspicious login activity (e.g., unauthorized access, foreign IP logins).
- Conduct regular vulnerability scans and penetration testing on email infrastructure.

D. Respond (Incident Response & Reporting)

- Implement an Email Security Incident Response Plan (ESIRP) to address email-based threats.
- Establish an email reporting mechanism for employees to report phishing emails.
- Quarantine and analyze suspected phishing or malware-laden emails.
- Notify affected users and take remedial actions (e.g., password reset, email blocking).

E. Recover (Business Continuity & Backup Policies)

- Ensure email backups are encrypted, stored securely, and tested regularly.

- Have a Business Continuity Plan (BCP) to restore email services in case of cyber incidents.
- Conduct post-incident reviews to improve security measures.

* Email Encryption?

Email encryption is the process of converting plain text email content into a coded format that can only be read by authorized recipients. This is achieved using encryption algorithms and key pairs, which consist of a public key and a private key. The public key is shared with anyone who needs to send an encrypted email, while the private key is kept secret by the recipient to decrypt the messages.

Types of email encryption

There are several common types of email encryption, each designed to meet different security needs and requirements. Below are some of the most widely used solutions:

1. S/MIME (Secure/Multipurpose Internet Mail Extensions)

S/MIME uses digital certificates to encrypt and sign emails. It is widely supported by email clients like Outlook and Apple Mail.

Pros:

- Provides both encryption and digital signatures.
- Ensures message authenticity and integrity.

Cons:

- Requires a public key infrastructure (PKI) and management of digital certificates.

- Can be complex to set up for smaller organizations.

2. Microsoft 365 Message Encryption

This feature allows users to send encrypted emails from Microsoft 365 to any email address.

Pros:

- Integrated into the Microsoft ecosystem, making it easy to use.
- Recipients can access encrypted messages using a secure web portal.

Cons:

- Limited features compared to other encryption methods.
- May not be compatible with non-Microsoft email clients.

3. End-to-end encryption

This method ensures that only the sender and recipient can read the email content, with no access granted to intermediaries.

Pros:

- Provides maximum security and privacy.
- Reduces the risk of data breaches.

Cons:

- Requires both parties to use compatible encryption tools.

- May involve additional steps for users unfamiliar with the process.

*** Roles and Responsibilities**

1- Policy Owner: <head of cybersecurity function>

2- Policy Review and Update: <cybersecurity function>

3- Policy Implementation and Execution: <information technology organization> and <cybersecurity function>

4- Policy Compliance Measurement: <cybersecurity function>Update and Review <cybersecurity function> must review the policy at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

*** Compliance & Legal**

1- <Head of cybersecurity function> will ensure the compliance of <organization name> with this policy on a regular basis.

2- All personnel of <organization name> must comply with this policy.

3- Any violation of this policy may be subject to disciplinary action according

to <organization name>'s procedures.

Individuals involved may be held liable for:

- Sending or forwarding e-mails with any libelous, defamatory, offensive, racist, or obscene remarks
- Sending or forwarding confidential information without permission
- Sending or forwarding copyrighted material without permission

- Knowingly sending or forwarding an attachment that contains a virus
- Ensure compliance with regulatory requirements (e.g., GDPR, HIPAA, CMMC, PCI-DSS).
- Regularly audit and update email security policies.

*** Training & Awareness**

- Conduct regular cybersecurity awareness training on email threats (e.g., phishing, ransomware).
- Simulate phishing attacks to test employee awareness and response.

*** Enforcement & Penalties**

- Unauthorized use of email for malicious activities may result in disciplinary action.

- Employees must immediately report any suspected email security incidents.