4.15.1 Email & Web Browser Protection

Contents

Version	Adjustment Date	Approved By	Approval Date and signature
2.0	18/12/2025	Saud Alsulami	2/1/2025

1. Definitions

For purposes of this “Email & Web Browser Protection” the following definitions apply:

- **Phishing:** A deceptive practice of sending emails or creating fake websites to trick users into revealing personal information, passwords, or financial details.
- **Multi-Factor Authentication (MFA):** A security system that requires multiple methods of identification, such as a password and a unique code sent to a user's mobile device, to verify a user's identity.
- **URL Filter:** A security tool that blocks or allows access to websites based on the category or reputation of the URL, used to prevent users from accessing malicious or inappropriate content.

2. Purpose

The purpose of this policy is to define the requirements and mechanisms for ensuring the security and integrity of emails and web browser activities within Taqnyat. This policy aims to protect against unauthorized access, phishing, malware, and other cyber threats, while ensuring compliance with industry standards and regulations.

3. Scope

This policy applies to all employees, contractors, and third-party users who have access to the Taqnyat’s email systems and web browsers. It covers all devices and systems used to access emails and the internet, including desktops, laptops, mobile devices, and any network-connected equipment.

4. Policy

4.1. The NOC department must utilize the security features provided by Office 365 including email filtering and Data Loss Prevention (DLP).

4.2. Enforce MFA across all Office 365 accounts, particularly for administrative or privileged users.

4.3. Ensure that web browsers used to access Office 365 support HTTPS, SSL/TLS, and other security protocols to guarantee secure communication.

4.4. Use Office 365’s built-in archiving and backup capabilities, such as Exchange Online Archiving and retention policies, to ensure that emails are securely archived and recoverable.

4.5. Utilizing Kaspersky Antivirus to secure email communications and internet browsing on all employee devices.

4.6. Employing patch management software to ensure the latest versions of web browsers are in use, mitigating potential vulnerabilities.

4.7. Training employees to recognize phishing emails and inspect attached files for malicious software.

4.8. The NOC department should enforce restrictions on accessing suspicious websites to ensure secure browsing, mitigating potential risks.

4.9. Employees are responsible for their internet browsing habits and ensuring they do not engage in personal activities or conduct that may harm the company in any way.

4.10. Company Taqnyat reserves the right to monitor internet usage and block access to certain websites deemed inappropriate without seeking employee approval, ensuring a secure and compliant online environment.

4.11. Employees must apply the correct data classification when sending information via email, and they can refer to the cybersecurity officer for guidance in case of any uncertainties or issues.

5. Non-compliance

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

6. References

- SANS
- National Cybersecurity Authority's (NCA) ECC standards