

Email Policy

January 2026

TEMPLATE ONLY





[THIS PAGE IS INTENTIONALLY LEFT BLANK]





Contents

Email Policy	1
1. Introduction	4
2. Purpose	4
3. Scope.....	4
4. Policy.....	4
5. Policy Compliance	5
6. Related Standards, Policies and Procedures.....	5
7. Definitions and Terms.....	5
8. Revision History	5





1. Introduction

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organisation. At the same time, misuse of email can pose many legal, privacy and security risks, thus users need to understand the appropriate use of electronic communications.

2. Purpose

This policy defines how the organisation retains and securely deletes information to reduce cyber security risk and support the objectives of the **ACSC Essential Eight** mitigation strategies. Proper data retention and deletion limit the impact of cyber incidents, including malware, ransomware, and unauthorised access.

3. Scope

This policy applies to:

- All corporate email accounts and services provided and under the organisation.
- All devices (including personal) such as desktops, laptops, tablets and smartphones must undergo approval methods.
- All use of emails for sending, storing, receiving, forwarding or replying for internal or external communications.
- All content stored or archived email messages, attachments, embedded or stored via corporate email.

4. Policy

- 4.1 All use of email must be consistent with Peppermint IT's Policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- 4.2 Emails should primarily be used for official business purposes. Hence, there is a prohibited use for sending spam, sharing confidential or sensitive information and unauthorised commercial, political or illegal activities.
- 4.3 Peppermint IT's email account should be used primarily for Peppermint IT Business related purposes; personal communication is permitted on a limited basis, but non- Peppermint IT related commercial uses are prohibited.
- 4.4 All Peppermint IT data contained within an email message or an attachment must be secured according to Data Protection Standard.
- 4.5 Email should be retained only if it qualifies as a Peppermint IT business record. Email is a Peppermint IT Business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
- 4.6 Email that is identified as a business record shall be retained according to Peppermint IT's Record Retention Schedule.
- 4.7 Email systems may be monitored to ensure compliance with this policy, and it will follow applicable legal and regulatory requirements.





- 4.8 The I.T lady email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, or political beliefs, or national origin. Employees who receive any emails with this content from any Peppermint IT employee should report the matter to their supervisor immediately.
- 4.9 Users are prohibited from automatically forwarding Peppermint IT email to a third-party email system (noted in 4.8 below). Individual messages which are forwarded by the user must not contain Peppermint IT confidential or above information.
- 4.10 Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, MSN Hotmail etc. to conduct Peppermint IT business, to create or memorialise any binding transactions, or to store or retain email on behalf of Peppermint IT. Such communications and transactions should be conducted through proper channels using Peppermint IT-approved documentation.
- 4.11 Using a reasonable amount of Peppermint IT resources for personal emails is acceptable, but non-work-related emails shall be saved in a separate folder from work-related emails. Sending chain letters or joke emails from a Peppermint IT email account is prohibited.
- 4.12 Peppermint IT employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.
- 4.13 Peppermint IT may monitor messages without prior notice. Peppermint IT is not obliged to monitor email messages.

5. Policy Compliance

5.1 Compliance measurement

The Infosec team will verify compliance with this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any Exception to the policy must be improved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Procedures

6.1 Data Protection standard.

7. Definitions and Terms

7.1 None.

8. Revision History

None.



