

P2021 - Email Policy

Contents

Purpose:.....	3
Scope:.....	3
Statement:.....	3
Policy Sections:.....	5
.....	5
Policy References:.....	6

Purpose:

The purpose of this policy is to outline the acceptable use of corporate emails at Integrity. These rules are in place to protect Integrity. Inappropriate use exposes our organization to risks, data loss, and legal issues. We want to ensure that we understand the limitations of using and accessing corporate email accounts on various personal and Integrity issued devices.

The intention behind publication of an Email Policy is not to impose restrictions that go against Integrity's established culture of openness, trust, and integrity. Instead, this policy is committed to safeguarding Integrity's employees, partners, and the company from any illegal or damaging actions, whether intentional or unintentional, by individuals.

The corporate email address of employees is owned by Integrity. It is designated for exclusive use in business-related activities that serve the best interests of the company, clients, and customers as a part of regular operations.

Scope:

According to Integrity's **P2000 - Acceptable Use Policy, and P2002 - Asset Management Policy** it is the responsibility of all Integrity employees and contractors to ensure the security and protection of electronic information resources under their control.

The **Email policy** applies to all employees, contractors, vendors, and partners (hereafter referred to as employees) who are assigned or granted access to Integrity's corporate email. This email can be assigned to an individual or a department.

Statement:

Overview

Corporate email is an essential communication tool within our organization, enabling efficient and effective exchange of information both internally and externally. This policy ensures that all users understand the appropriate use of Integrity's email systems, maintain the security and confidentiality of communications, and comply with legal and regulatory requirements.

It is important that employees use corporate emails responsibly and protect the organization from potential risks associated with email misuse, including data breaches, legal liabilities, and reputational damage.

Users should be aware that clear text email is not a confidential means of communication. The organization cannot guarantee that electronic communications will be private. Individuals should be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Users should also be aware that once an email is transmitted it may be altered. Deleting an email from an individual workstation will not eliminate it

from the various systems across which it has been transmitted.

To understand what emails and communications are prohibited according to the policy, please refer ***“P2000 - Acceptable Use Policy”***

Accessing corporate email on devices

Security measures:

- Email access: Corporate emails should be primarily accessed on Integrity issued workstations. If accessed on personal mobile devices, such as tablets or smartphones, those should be registered with Integrity.
- Access on personal workstations are not permitted.
- Authorized application: Integrity has chosen the Outlook application family as the primary method for accessing corporate emails on corporate workstations, as well as corporate and personal mobile devices (Outlook for Desktop, Outlook for Mobile, Outlook Web Access)
- Mobile Device Management: All devices used to access corporate emails must adhere to existing asset management policy. Please refer ***“P2002 - Asset Management Policy”***.
- Email Monitoring: Integrity will have full authority over the corporate email account in use by the employee or department and all monitoring controls in place for emails originating from mobile devices. Employees should have no expectation of privacy when using corporate email on any device.
- Encryption: All emails having Protected Health Information (PHI), and Personally Identifiable Information (PII) should be encrypted.
- Integrity has adopted a DLP (Data Loss Prevention) program to ensure email containing PHI/PII/Confidential information is securely transmitted. All email will be scanned by the system to ensure compliance.
 - If an email is determined to contain a **Low** threshold of content detections, a warning will be generated, violation logged, and appropriate parties at Integrity notified – and the message will be allowed to be sent.
 - If an email is determined to contain a **High** threshold of content detections, a warning will be generated, violation logged, and appropriate parties at Integrity notified – and the message will be blocked until resent in a secure manner.
- Remote Wipe: Employees must agree to Integrity’s ability to remotely wipe corporate email account and associated data from the device in the event of loss, theft, or termination of employment. This applies to both corporate and personal owned devices. In each case it is the responsibility of the employee and their immediate supervisor/manager to inform and engage cybersecurity services.
- Encryption: All mobile devices must employ encryption methods, and any encryption method used must comply with industry best practices and applicable legal requirements.
- Accessing an Integrity email account belonging to another individual requires authorization. Please refer ***“P2000 - Acceptable Use Policy”***
- Personal emails: Employees are allowed to use their personal emails on corporate devices but for the security of the organization, restrictions with regards to sharing corporate data is in place

- **Storage:** Integrity's email systems should not be used as a medium for storage solution of records for use or reference in future. Employees should use designated storage systems for any work-related files or information.
- **Employment separation:** When an employee leaves the company, whether voluntarily or involuntarily, their access to all email services, including any linked applications or third-party services, must be revoked on their last working day. The manager of the departing employee will have access to the employee's emails for up to 30 days.
 - The manager of the departing employee will have access to the employee's emails for a maximum period of 30 days.
 - **Email forwarding or Shared email account:** The manager can request email forwarding or setup a shared account to another designated email address for up to 60 days. This request must be formally submitted to the IT department with a business justification and must be approved by Legal & Compliance, Cybersecurity, and People and Culture.
 - **Auto responder:** The manager can request an autoresponder on the former employee's email account to notify external contacts of the employee's departure and provide alternative contact information. This request also requires a business justification and approvals from Legal compliance, Cybersecurity, and Human Resource.
- **Exceptions:**

Please refer exceptions process stated in ***"P2000 - Acceptable Use Policy"***.
- **Non-Compliance**

Violations of this Email Policy or Acceptable Use Policy may result in appropriate disciplinary measures in accordance with local, state, and federal laws.

All personnel covered by this Policy are obligated to report apparent violations of this program or its associated policies and standards.

Policy Sections:

Policy References:

P2021 - Email Policy		
Document Author	Name: Title: Email:	Sumit Dhawan Manager, Cybersecurity Compliance sumit.dhawan@integrity.com
Document Owner	Name: Title: Email: Approved Date:	Matthew R Williams Senior Director, Cybersecurity & Cloud Engineering, CISO matthew.williams@integrity.com 3/18/2025
Legal Management Approval	Name: Title: Email: Approved Date:	Duncan William McQueen Assistant General Counsel duncan.mcqueen@integrity.com 3/27/2025
Executive Management Approval	Name: Title: Email: Approved Date:	Harsh Singla Chief Technology Officer Harsh.Singla@integrity.com 4/8/2025

Last Published Date: 4/8/2025

Document Version Number 1.0