

Email Security Policy

Effective Date

Version

Policy Owner

Approved by

Review Date

1. Purpose

("**Company**") adopts this Email Security Policy to protect Company information, systems, personnel, customers, and business partners from email-based threats. This Policy establishes rules for using Company email accounts, handling email messages and attachments, reporting suspected threats, and protecting sensitive information transmitted by email.

2. Scope

This Policy applies to all employees, officers, directors, contractors, temporary workers, consultants, and other individuals authorized to access or use Company email accounts, email systems, or Company information through email.

This Policy applies whether email is accessed from a Company-issued device, a personal device authorized for business use, or a remote location.

3. Policy Statement

Company email systems are provided primarily for authorized business purposes. All users must use email responsibly, protect Company information, and follow the security requirements in this Policy.

Limited personal use may be permitted where it does not interfere with work responsibilities, create security risks, violate Company policies, or result in material cost or disruption to the Company.

4. Account Access and Authentication

Users must access Company email only through approved accounts, devices, applications, and authentication methods. Users must not share passwords, authentication codes, recovery codes, or access credentials with any other person.

Users must create and maintain strong, unique passwords for Company email accounts. Where multi-factor authentication is available, it must be enabled and used.

Users must promptly notify if they believe their email account, password, device, or authentication method may have been compromised.

5. Acceptable Use

Users must use Company email professionally and in a manner consistent with Company policies, applicable law, and contractual obligations. Users must not use Company email to:

- Send unlawful, discriminatory, harassing, threatening, or offensive communications.
- Transmit malicious software, unauthorized software, or content that may damage Company systems.
- Conduct unauthorized commercial activity, political campaigning, or personal business activity.
- Impersonate another individual or misrepresent the sender's identity, authority, or relationship with the Company.
- Send confidential Company information to unauthorized recipients.
- Forward Company email to personal email accounts or unauthorized third-party services.
- Circumvent Company security controls, monitoring systems, or retention requirements.

6. Phishing and Suspicious Messages

Users must remain alert to phishing, impersonation, business email compromise, fraudulent invoice requests, malicious links, and suspicious attachments.

A user must not click a link, open an attachment, provide credentials, approve a payment, change banking information, or disclose sensitive information when a message appears unexpected, suspicious, or inconsistent with normal business practices.

Before acting on a request involving payments, financial account changes, payroll changes, confidential information, credentials, or urgent instructions, users must independently verify the request through a trusted communication channel, such as a known telephone number or a separate verified contact method.

Suspected phishing or malicious email must be reported immediately to using .

7. Attachments, Links, and Downloads

Users must exercise caution before opening email attachments, clicking links, or downloading files. Users may open only content that is expected, relevant to their work, and from a trusted source.

Files or links that appear unusual, are password-protected without explanation, request credentials, use unexpected file types, or create urgency must be reported for review before being opened or used.

Users must not disable security warnings, bypass email filtering tools, or install software received through email without authorization from .

8. Protection of Sensitive Information

Users must protect confidential, personal, financial, health, proprietary, and other sensitive information sent or received by email.

Before sending sensitive information, users must confirm the recipient's identity, email address, authorization, and need to receive the information. Users must use Company-approved encryption, secure file-sharing, or protected delivery methods when required by Company procedures or the sensitivity of the information.

Sensitive information must not be included in an email subject line. Users should minimize the information included in an email and send only what is necessary for the stated business purpose.

9. External Email Communications

Users must take particular care when communicating with external recipients. Before sending an external email, users must review the recipient list, attached files, embedded links, and message content for accuracy and appropriateness.

Users must not send confidential information to a personal email address, unverified third party, or recipient outside the Company unless the disclosure is authorized and protected by an approved method.

Where required, external communications must include Company-approved confidentiality notices, disclaimers, or other required business language.

10. Email Forwarding and Auto-Forwarding

Automatic forwarding of Company email to personal email accounts or unauthorized external accounts is prohibited.

Users may configure forwarding rules only where approved by and where the forwarding arrangement does not expose Company information or interfere with retention, monitoring, or security requirements.

11. Email Retention and Deletion

Users must retain and delete email records in accordance with the Company's records retention requirements, legal holds, and applicable business procedures.

Users must not delete, alter, conceal, or destroy email messages that are subject to a legal hold, investigation, audit, dispute, regulatory inquiry, or other preservation requirement.

12. Monitoring and Privacy

Company may monitor, access, review, retain, filter, or disclose Company email and related system activity to the extent permitted by applicable law and Company procedures. Monitoring may be used to protect Company systems, investigate security incidents, support business operations, comply with legal obligations, and enforce this Policy.

Users should not expect personal privacy when using Company email systems, except where applicable law provides otherwise.

13. Security Incidents

Users must immediately report any suspected or confirmed email security incident to . Incidents include suspected account compromise, misdirected emails, unauthorized disclosures, phishing attempts, malware, fraudulent payment requests, or unusual account activity.

Users must preserve relevant messages, attachments, and related information unless instructed otherwise by . Users must not attempt to investigate, remediate, or communicate externally about an incident unless authorized to do so.

14. Training and Compliance

The Company may require users to complete email security training, phishing awareness training, or other related education. Users must complete required training within the stated timeframe and follow related procedures issued by the Company.

Failure to comply with this Policy may result in restricted access, corrective action, disciplinary action up to and including termination of employment or engagement, and other action permitted by applicable law or contract.

15. Exceptions

Any exception to this Policy must be approved in writing by and . Approved exceptions must specify the scope, duration, business justification, and any required compensating security measures.

16. Policy Administration and Amendments

is responsible for administering this Policy and may issue supporting procedures, standards, and guidance.

The Company may amend, replace, suspend, or withdraw this Policy at any time, subject to applicable law. This Policy does not create an employment contract, guarantee continued employment, or limit the Company's right to manage its business and workforce.

17. Acknowledgment

By signing below, the undersigned acknowledges receipt of this Email Security Policy, confirms that they have read and understood it, and agrees to comply with its requirements.

Signatures

Company

Name

Date

Signature

Employee or User

Name

Date

Signature



This document is a PDF copy of **Email Security Policy** template. You can edit it with **Jotform Sign** and convert to an eSign document with **Jotform Sign**.

 **Edit PDF**

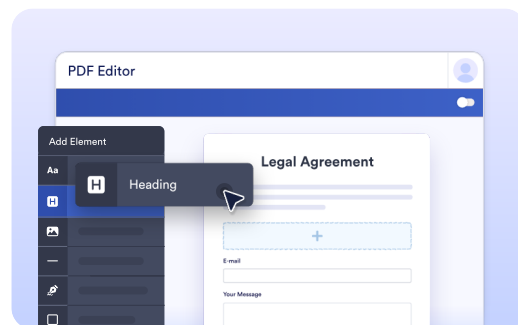
Learn More About Jotform PDF Products

Jotform offers powerful PDF solutions. Check them out below.

Jotform PDF Editor

Turn form submissions into PDFs automatically ready to download or save for your records.

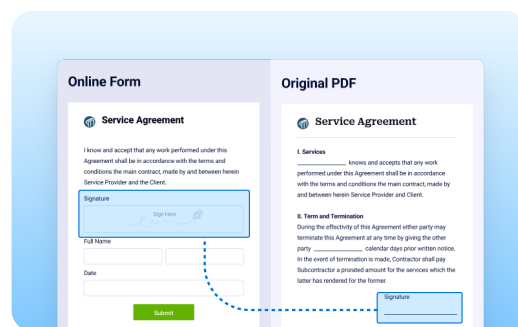
jotform.com/products/pdf-editor/



Smart PDF Forms

Convert your PDF files into online forms that are easy to fill out on any device.

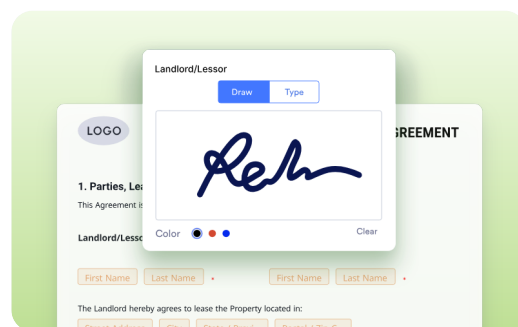
jotform.com/products/smart-pdf-forms/



Jotform Sign

Collect e-signatures with Jotform Sign to automate your signing process.

jotform.com/products/sign/



These templates are suggested forms only. If you're using a form as a contract, or to gather personal (or personal health) info, or for some other purpose with legal implications, we recommend that you do your homework to ensure you are complying with applicable laws and that you consult an attorney before relying on any particular form.