Information Security Policy

Organization

Effective Date

Version

Approved by

Policy Owner

Next Review Date

1. Purpose

This Information Security Policy establishes the principles, responsibilities, and minimum requirements for protecting (“***Company***”) information, information systems, and technology resources. Its purpose is to preserve the confidentiality, integrity, and availability of Company information and to reduce the risk of unauthorized access, loss, alteration, disclosure, disruption, or misuse.

2. Scope

This Policy applies to all Company personnel, including employees, officers, directors, temporary workers, contractors, consultants, interns, and other individuals who access, process, store, transmit, or manage Company information or technology resources.

This Policy applies to information in any form, including electronic records, paper records, verbal communications, databases, devices, cloud services, applications, networks, and removable media. It also applies to third parties that handle Company information or access Company systems on the Company’s behalf.

3. Policy Statement

The Company will maintain an information security program that is appropriate to its operations, the nature of the information it handles, and the risks it faces. All personnel must protect Company information and use Company technology resources responsibly, lawfully, and only for authorized business purposes.

Jotform
Automatically create polished, fillable and signable documents
Clone the document for free!

Security controls must be proportionate to the sensitivity of the information and the potential impact of a security incident.

4. Information Classification and Handling

The Company will classify information according to its sensitivity and business value. At a minimum, information may be categorized as Public, Internal, Confidential, or Restricted.

Public information may be shared externally when authorized. Internal information is intended for Company use and must not be disclosed outside the Company without approval. Confidential and Restricted information requires heightened protection and may include personal information, financial information, credentials, customer data, proprietary business information, legal records, security information, and trade secrets.

Personnel must handle information according to its classification. Confidential and Restricted information may only be accessed, used, shared, retained, or destroyed when there is a legitimate business need and appropriate authorization.

5. Access Control

Access to Company information systems and data will be granted according to the principle of least privilege. Personnel will receive only the access necessary to perform their assigned duties.

Each user must have a unique account or other approved means of identification. Shared accounts are prohibited unless specifically approved by _____ and protected through documented compensating controls.

Access rights must be reviewed periodically and updated promptly when an individual's role changes, access is no longer required, or their employment or engagement ends. Access to sensitive systems and information must be removed or disabled as soon as reasonably practicable following separation from the Company.

Jotform
Automatically create polished, fillable and signable documents
Clone the document for free!

6. Authentication and Password Security

Personnel must use strong, confidential authentication credentials and must not share passwords, authentication codes, access tokens, or other account credentials with unauthorized persons.

Multi-factor authentication must be used for remote access, privileged accounts, and other systems designated by the Company based on risk. Passwords must meet Company standards for length, complexity, reuse, and change requirements.

Personnel must promptly report any suspected compromise, loss, or unauthorized use of their credentials.

7. Acceptable Use of Technology Resources

Company technology resources, including devices, systems, networks, email accounts, software, and cloud services, must be used responsibly and primarily for authorized business purposes.

Personnel must not:

- Circumvent security controls or access restrictions.
- Install unauthorized software or connect unauthorized devices to Company systems.
- Use Company systems to engage in unlawful, harmful, fraudulent, or abusive activity.
- Store Company information in unapproved applications, personal accounts, or personal cloud-storage services.
- Download, copy, transmit, or disclose Company information without a legitimate business purpose and required authorization.

The Company may monitor, review, and protect its technology resources to the extent permitted by applicable law and its internal practices.

8. Device and Endpoint Security

Company-managed devices must use approved security controls, including supported operating systems, security updates, malware protection, device encryption where appropriate, screen-lock settings, and access controls.

Jotform
Automatically create polished, fillable and signable documents
Clone the document for free!

Personnel must protect devices from theft, loss, damage, and unauthorized access. Devices containing Company information must not be left unattended in unsecured locations.

Personal devices may access Company systems only when authorized by the Company and subject to applicable security requirements. The Company may restrict, remove, or revoke access from personal devices when necessary to protect Company information.

9. Network and Remote Access Security

Access to Company networks and systems from outside Company-controlled locations must use approved remote-access methods and security controls.

Personnel working remotely must take reasonable steps to protect Company information, including using secure networks, preventing unauthorized viewing of sensitive information, and keeping devices physically secure. Public or unsecured wireless networks should not be used to access sensitive Company systems unless an approved secure connection is in place.

10. Data Protection and Encryption

The Company will use reasonable safeguards to protect Company information during storage, transmission, and processing. Encryption or other appropriate protective measures must be used for Confidential and Restricted information when required by the Company's security standards or risk assessment.

Personnel must use Company-approved methods when transferring sensitive information. Sensitive information must not be sent through unsecured channels unless authorized safeguards are in place.

11. Email, Messaging, and Phishing Protection

Personnel must remain alert to phishing, impersonation, malware, fraudulent payment requests, suspicious links, and other social-engineering attempts.

Before responding to unusual requests involving payments, credentials, sensitive information, or changes to account details, personnel must verify the request through an independent and trusted communication method.

Jotform
Automatically create polished, fillable and signable documents
Clone the document for free!

Suspicious messages, links, attachments, or system activity must be reported promptly to [ ]. Personnel should not open, forward, or interact with suspected malicious content unless instructed by authorized security personnel.

12. Software, Systems, and Change Management

The Company will maintain reasonable procedures for approving, configuring, updating, and securing software and systems.

Security updates, patches, and vulnerability remediation must be applied within timeframes appropriate to the severity of the risk. Material changes to systems that process Confidential or Restricted information must be reviewed and approved through the Company's change-management process.

Only authorized personnel may administer Company systems or make changes to security settings, production environments, or access controls.

13. Third-Party and Cloud Service Providers

Before a third party is granted access to Company information or systems, the Company will assess the security risks associated with the engagement. Contracts with applicable third parties should include confidentiality, data protection, security, incident-notification, and access-control obligations appropriate to the services provided.

Third-party access must be limited to the minimum scope and duration necessary for the approved business purpose. The Company will periodically review material third-party relationships based on risk.

14. Security Incident Reporting and Response

All personnel must promptly report actual or suspected security incidents, including lost or stolen devices, unauthorized access, malware infections, accidental disclosures, phishing attempts, suspicious system activity, and data loss.

Reports must be made to [ ]. Personnel must not attempt to conceal, delete, or alter evidence related to a suspected incident.

Jotform Automatically create polished, fillable and signable documents Clone the document for free!

The Company will investigate reported incidents, take reasonable containment and recovery measures, and notify affected parties or authorities when required by applicable law, contractual obligations, or the circumstances of the incident.

15. Backup, Retention, and Secure Disposal

The Company will maintain backup and recovery practices appropriate to its operational needs and the sensitivity of its information.

Company information must be retained only for as long as required for legitimate business, legal, contractual, or operational purposes. When information or devices are no longer needed, they must be securely deleted, destroyed, or disposed of using methods appropriate to the type and sensitivity of the information.

16. Security Awareness and Training

Personnel will receive information security training appropriate to their role and level of access. Training may address topics such as password security, phishing awareness, data handling, remote work, incident reporting, and acceptable use.

Personnel with elevated access or specialized security responsibilities may be required to complete additional training.

17. Compliance, Monitoring, and Audits

The Company may review compliance with this Policy through monitoring, access reviews, security assessments, audits, testing, or other reasonable measures.

Personnel must cooperate with authorized security reviews, investigations, and remediation activities. Failure to comply with this Policy may result in corrective action, removal of access, disciplinary action, termination of employment or engagement, or other appropriate action.

Jotform
Automatically create polished, fillable and signable documents
Clone the document for free!

18. Exceptions

Any exception to this Policy must be requested in writing and approved by _____ before the exception takes effect, unless immediate action is necessary to address an urgent business or security need.

Approved exceptions must identify the scope, duration, business justification, risks, and any alternative safeguards required by the Company. Exceptions may be withdrawn if the related risk is no longer acceptable.

19. Policy Administration and Review

_____ is responsible for administering this Policy and maintaining related standards, procedures, and guidance.

This Policy will be reviewed at least annually and may be revised when there are material changes to the Company's operations, technology environment, risk profile, legal obligations, or security practices. The Company may amend or withdraw this Policy at its discretion, subject to applicable law.

20. Acknowledgement

By signing below, the undersigned acknowledges that they have received, read, and understood this Information Security Policy. The undersigned agrees to comply with the Policy and to report suspected security incidents or violations promptly.

Signatures

Approved by

Name _____

Date _____

Signature _____

Recipient

Name _____

Date _____

Signature _____

Jotform Automatically create polished, fillable and signable documents Clone the document for free!

Jotform

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

Edit PDF

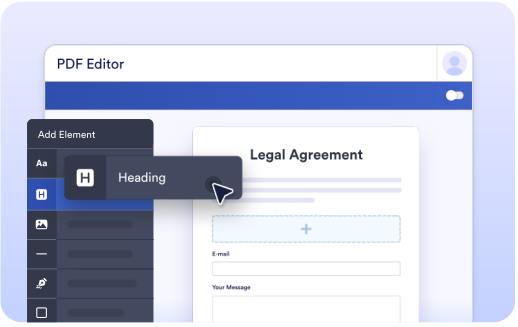
Learn More About Jotform PDF Products

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.

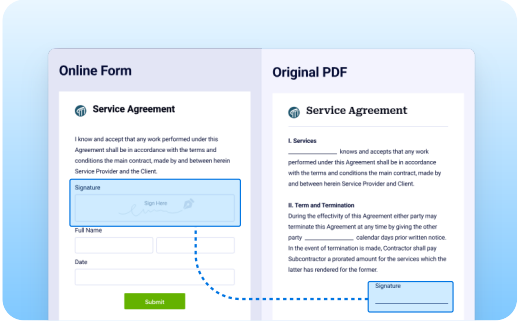
jotform.com/products/pdf-editor/



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.