

Network Security Policy

Policy Owner

Approved by

Effective Date

Version

Next Review Date

1. Purpose

("**Company**") adopts this Network Security Policy to protect its networks, systems, data, users, and business operations from unauthorized access, misuse, disruption, loss, or alteration. This Policy establishes minimum requirements for designing, operating, monitoring, and maintaining Company networks.

This Policy is an internal governance document. It does not create an employment contract, guarantee continued employment, or limit the Company's right to change its security practices, subject to applicable law.

2. Scope

This Policy applies to all Company-owned, leased, managed, or administered networks, network-connected systems, cloud networking environments, wireless networks, remote access services, security appliances, and related infrastructure.

It also applies to all employees, officers, directors, temporary workers, contractors, consultants, service providers, and other persons who access or administer Company network resources.

3. Policy Authority and Administration

The is responsible for administering this Policy and establishing technical standards consistent with its requirements. Business units, system owners, and users must cooperate with security reviews, investigations, remediation activities, and access-control procedures. The Company may monitor, inspect, restrict, suspend, or terminate access to its networks and systems when reasonably necessary to protect Company operations, information, users, or legal interests.

4. Network Security Principles

The Company shall maintain network security controls that are proportionate to the sensitivity of the data processed, the services provided, and the risks faced by the Company.

Network access must be limited to authorized users, devices, applications, and services with a legitimate business need. Security controls must be designed to reduce unnecessary exposure between network segments, external networks, and sensitive systems.

5. Network Architecture and Segmentation

Company networks must be designed and maintained using documented network architecture appropriate to the Company's operational needs. Network diagrams, system inventories, and records of key network connections must be kept current to a reasonable extent.

The Company shall separate network environments where appropriate, including production, development, testing, administrative, guest, and user-access environments. Systems containing sensitive, confidential, regulated, or business-critical information must receive additional protection through segmentation, restricted routing, access controls, or other suitable safeguards.

Direct access from the public internet to internal systems is prohibited unless the connection has been approved by the , is necessary for a legitimate business purpose, and is protected by appropriate security controls.

6. Firewalls and Perimeter Controls

The Company shall use firewalls, security gateways, cloud security controls, or comparable technologies to manage traffic entering, leaving, and moving within Company networks.

Firewall and security gateway rules must be documented, approved by an authorized administrator, and configured to allow only traffic required for approved business purposes. Rules that permit broad access, unrestricted inbound access, or unnecessary services must not be used without documented risk acceptance from .

Firewall configurations must be reviewed periodically and after material changes to the relevant network environment. Unused, outdated, temporary, or unauthorized rules must be removed or disabled promptly.

7. Access Control

Access to network devices, administrative consoles, virtual private networks, cloud networking services, and other security-sensitive systems must be granted according to the principle of least privilege.

Administrative access must be limited to authorized personnel who require it to perform assigned duties. Shared administrative accounts must be avoided where practical. Individual administrator accounts must be used whenever possible so that actions can be traced to a specific user.

Multi-factor authentication must be used for remote access, privileged access, and other high-risk access methods where technically supported. Access credentials must not be shared, disclosed, stored in unsecured locations, or used by unauthorized persons.

Access rights must be reviewed periodically and promptly changed or revoked when a person changes roles, no longer requires access, or leaves the Company.

8. Remote Access

Remote access to Company networks must be approved, authenticated, encrypted, and limited to authorized users and devices. The Company may require the use of Company-managed devices, virtual private network services, multi-factor authentication, endpoint protection, or other security controls before remote access is permitted.

Users accessing Company resources remotely must protect their devices and connection from unauthorized use. Remote access from public or unsecured networks must use Company-approved encrypted connection methods.

Remote access privileges may be suspended or revoked when there is a suspected security risk, policy violation, change in business need, or termination of the user's relationship with the Company.

9. Wireless Networks

Company wireless networks must use current, Company-approved encryption and authentication methods. Default passwords, default management settings, and unnecessary wireless services must be changed, disabled, or removed before deployment.

Guest wireless access must be separated from internal Company networks. Guest users must not receive access to Company systems, internal data, or administrative network resources unless specifically authorized and protected by appropriate controls.

Unauthorized wireless access points, network extenders, routers, or similar devices may not be connected to Company networks without prior approval from the .

10. Network Device Security

Network devices, including routers, switches, firewalls, wireless access points, load balancers, and comparable infrastructure, must be configured using secure baseline settings approved by the .

Default accounts, credentials, services, ports, protocols, and features that are not required for business operations must be disabled, removed, or restricted where feasible. Management interfaces must be protected against unauthorized access and, where practical, accessible only through designated administrative networks or secure connection methods.

Configuration changes to critical network infrastructure must be documented and approved under the Company's change-management process.

11. Vulnerability and Patch Management

The Company shall assess network infrastructure and network-connected systems for vulnerabilities at intervals appropriate to the risk of the environment. Identified vulnerabilities must be prioritized and addressed based on severity, likelihood of exploitation, business impact, and the sensitivity of affected assets.

Security patches, firmware updates, and configuration updates must be applied within a reasonable timeframe after review and testing. When a patch cannot be applied promptly, the responsible owner must document the reason and implement compensating safeguards when appropriate.

Unsupported or end-of-life network devices and systems must be replaced, isolated, or subject to documented risk acceptance by .

12. Malware and Intrusion Protection

The Company shall use reasonable technical controls to detect, prevent, and respond to malicious network activity. Controls may include intrusion detection or prevention systems, endpoint protection, secure email filtering, domain filtering, network traffic analysis, and threat intelligence services.

Security tools must be configured and maintained in accordance with Company standards. Alerts indicating potential unauthorized access, malware, unusual network behavior, or other security events must be reviewed by authorized personnel.

13. Logging and Monitoring

The Company shall collect and retain security logs from network devices, remote access services, security tools, and other relevant systems to support incident detection, investigation, and operational oversight.

Logs must be protected against unauthorized alteration, deletion, or disclosure. Access to logs must be limited to authorized personnel with a legitimate business need.

The Company may monitor network traffic, user activity, and system events on Company resources to protect its systems, investigate suspected misconduct, meet legal obligations, and maintain business continuity, subject to applicable law.

14. Encryption and Data Transmission

Sensitive Company information must be protected during transmission across public networks or other untrusted connections using Company-approved encryption methods.

Unencrypted protocols must not be used for administrative access, remote access, or the transmission of sensitive information unless an authorized exception has been approved and documented.

15. Third-Party and Cloud Connections

Third-party vendors, service providers, customers, and partners may connect to Company networks only when the connection has a documented business purpose and has been approved by the and, where appropriate, the .

Third-party connections must be limited to the minimum access required and protected by appropriate authentication, encryption, monitoring, and contractual safeguards. The Company may review, restrict, or terminate third-party network access at any time based on security, business, or legal considerations.

Cloud-hosted network environments and services must be configured according to Company security standards and the applicable service provider's security capabilities.

16. Security Incidents

All users must promptly report suspected network security incidents, including unauthorized access, unusual network activity, lost devices, credential compromise, malware alerts, or suspected policy violations, to .

The Company will investigate reported incidents and may take reasonable steps to contain, assess, remediate, recover from, and document the incident. Users and relevant service providers must cooperate with incident-response activities.

The Company may notify affected parties, regulators, insurers, law enforcement, or other entities when required or appropriate under applicable law, contractual obligations, or Company procedures.

17. Acceptable Use and Prohibited Activities

Company network resources may be used only for authorized business purposes and other uses expressly permitted by the Company.

Users must not attempt to bypass security controls, interfere with network operations, connect unauthorized equipment, scan or test systems without authorization, capture network traffic without authorization, share credentials, introduce malicious code, or access systems or data beyond their assigned permissions.

18. Training and Awareness

The Company shall provide security awareness information and training appropriate to the roles and responsibilities of covered personnel. Personnel with privileged access or network-administration duties may be required to complete additional technical or role-specific training.

19. Exceptions

Any exception to this Policy must be requested in writing and approved by after consultation with the . An approved exception must identify the affected systems, business justification, duration, risks, and compensating controls.

Exceptions are temporary unless expressly approved otherwise and may be revoked at any time if the associated risk changes or the business need no longer exists.

20. Compliance and Enforcement

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

The Company may conduct audits, reviews, assessments, or investigations to evaluate compliance with this Policy.

21. Policy Review and Amendment

This Policy will be reviewed at least annually and may be updated when business operations, technology, legal requirements, threats, or Company practices change.

Only may approve amendments to this Policy. The current approved version will supersede prior versions as of its effective date.

22. Acknowledgment

By signing below, the undersigned acknowledges receipt of this Network Security Policy, understands that compliance is required as a condition of access to Company network resources, and agrees to report suspected security concerns promptly.

Signatures

Company

Name

Date

Signature

Acknowledged by

Name

Date

Signature



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

 **Edit PDF**

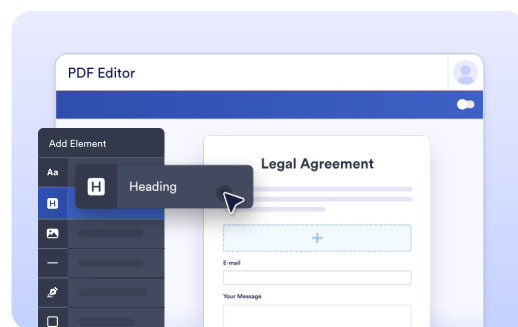
Learn More About Jotform PDF Products

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.

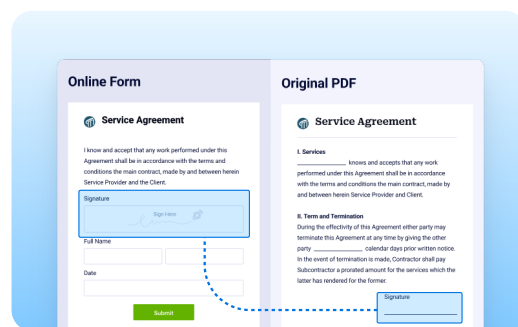
jotform.com/products/pdf-editor/



Smart PDF Forms

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

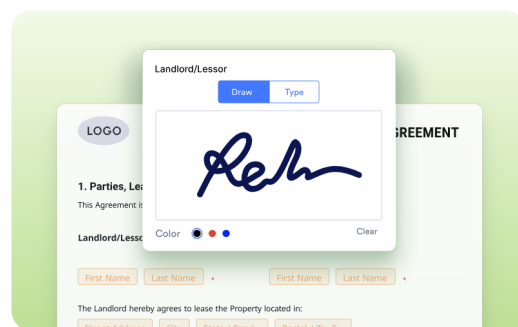
jotform.com/products/smart-pdf-forms/



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.