****

**Network perimeter security policy template**

|  |
| --- |
| **Title:** Network perimeter securitypolicy  |
| **Department:**  | **Version:** Original |
| **Approved by:** | **Approval date:**  |
| **Senior management approval:** |
| **Effective date:** | **Last updated:** |
| **Author:** |
| This policy applies to <company name>, <address>. |
| **Authority** This policy is hereby approved and authorized.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Name Title Date\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Name Title Date |
| **Purpose** The purpose of this policy is to define the activities associated with the provision of network perimeter security for access to <company name> information systems, networks, data, databases and other information assets. Additional policies governing other information security activities will be addressed separately. |
| **Scope**The scope of this network perimeter security policy includes all IT systems, software, databases, applications and network resources that are implemented in company-owned and maintained facilities and cloud-based and/or managed service infrastructures needed by the company to conduct business. |
| **Statement of compliance**This policy is designed to be compliant with ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements; NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations; the NIST Framework for Improving Critical Infrastructure Cybersecurity; and the FFIEC Information Technology Examination Handbook for Information Security (2016).Network perimeter security policy compliance is managed by the IT data security team, with support from other IT departments, such as telecommunications and network services. To achieve compliance, network perimeter security processes must include appropriate procedures and identify staffing and technology resources to meet compliance requirements. Network service carriers and security equipment and application vendors are required to demonstrate compliance with this policy. Compliance verification is performed monthly by the IT department, internal audit or other appropriate entities. |
| **Policy**As part of our duty of care and as a matter of good business practice, the confidentiality, integrity and availability of all IT applications, data, systems and network resources accessed by one or more network perimeters at <company name> are to be managed by a formal information security management program that includes network perimeter security. This program will provide a controlled and orderly method by which remote access to <company name>'s information systems is requested and granted, security of network perimeters is monitored and analyzed, violations of perimeter security are addressed and mitigated, and changes to perimeter security systems and procedures are requested, tested, approved and communicated for audit and record-keeping purposes.1. This policy addresses all <company name> technology, systems, data and networks implemented in private, hybrid and/or public cloud infrastructures, plus all other <company name> IT assets accessed by network perimeters as identified by IT department management.
2. The IT department will define network perimeter security processes and procedures; secure and utilize specialized software and systems to reduce the threat of unauthorized perimeter breaches; regularly test the security of the company's perimeters and any third-party perimeters using penetration tests and other forensic methods; and document all network perimeter security procedures and controls.
3. The <company name> IT department will prepare and document IT information security plans that address network perimeters and will facilitate the maintenance and review of those plans.
4. The IT department will periodically conduct a risk assessment of the internal and external risks, threats and vulnerabilities of the IT network perimeters.
5. The IT department will establish a policy for accessing <company name> systems, networks, applications and files, both locally and remotely, via its network perimeters such as security access and authentication controls for <company name> and external users.
6. The IT department will ensure malware, such as viruses, spam, phishing attacks, denial-of-service attacks and other unauthorized access attempts, are prevented using specialized network security software and other appropriate prevention and detection resources, such as firewalls, intrusion detection systems and intrusion prevention systems.
7. The IT department will ensure all software associated with network perimeter breach prevention systems and applications are regularly reviewed and the rules for analyzing suspicious code are updated regularly to remain current with existing and unplanned threats.
8. The IT department will ensure external network service carriers and related vendors have similar network perimeter security capabilities and the use of those services shall be approved by <company name>.
9. This policy ensures unauthorized attempts to penetrate the <company name> network perimeters are prevented. <Company name> will also have a similar policy for third-party service vendors.
10. The IT department will establish and document a formal process for identifying possible breaches in the network perimeter, capturing and containing the malicious code if possible, assessing the breach, determining the nature and impact of the breach, notifying <company name> management of the breach, minimizing the impact of the breach and documenting the steps taken when dealing with the incident. This process will apply to all network perimeters, whether internal, hybrid and/or public clouds.
11. The IT department will establish and document a process for identifying internal breaches, assessing the breach, capturing and containing data on the breach, determining the nature and impact of the breach, notifying <company name> management of the breach, minimizing the impact of the breach and documenting the steps taken when dealing with the incident.
12. The IT department will provide network perimeter security education, training and awareness programs.
13. The IT department will include business continuity and disaster recovery in its network perimeter security controls.
14. The IT department will define consequences for violating the network perimeter security policy.
15. The IT department will define how network perimeter security incidents are reported and managed.
16. The IT department, in collaboration with the company legal department, will prepare and execute the appropriate service-level agreements with network service providers and equipment vendors to ensure acceptable third-party vendor performance.
17. <Company name> employees must sign an employee contract agreeing to accept and comply with security policies -- including those associated with network perimeters -- when they are hired and on a regular basis through the employee handbook and/or in contract renewals to account for policy changes.
18. All proposed changes to network perimeter security operations will be documented in detail.
19. Network perimeter security breaches that may impact <company name> IT operations are identified in the company's information security management system and associated documents.
20. The IT department will develop a schedule of all relevant network perimeter security activities for the company and will ensure that these activities are completed on time.
21. The IT department will ensure all network perimeter security policies and associated procedures comply with appropriate legislative, regulatory and contractual requirements as well as accepted standards and practices.
22. All proposed changes to this policy must be processed and documented through the company's IT change management system.
 |
| **Policy leadership** **The <title of executive>** is designated as the corporate owner responsible for network perimeter security activities for the company. Resolution of issues in support of network perimeter security activities should be discussed with IT management, the corporate information security team, the networking team and others as needed. |
| **Policy responsibilities*** **Policy approval.** The **<title of executive>** is responsible for approving this policy.
* **Policy implementation.** <Name of department or individual> is responsible for planning, organizing and implementing all activities that fulfill this policy.
* **Policy maintenance and updating.** <Name of department or individual> is responsible for all activities associated with maintaining and updating this policy.
* **Policy monitoring and review.** <Name of department or individual> is responsible for monitoring and reviewing this policy.
* **Policy improvement.** <Name of department or individual> is responsible for defining and implementing activities that will improve this policy.
* **Policy auditing.** The internal audit department, or an approved external audit organization, is responsible for organizing and coordinating the completion of network perimeter security policy audits, in collaboration with the IT department.
 |
| **Management review**<Name of department or individual> will review and update this policy on an annual basis. As changes to this policy are indicated in the course of business, <name of department or individual> may initiate a change management process to update the policy. |
| **Policy enforcement**The **<title of executive>** will enforce this policy. |
| **Penalties for noncompliance** In situations where network perimeter security activities do not comply with this policy, the IT security team will prepare a report stating the reason(s) for noncompliance and present it to IT management for resolution. Failure to comply with this network perimeter security policy and any service-level agreements established with external network service firms and equipment vendors within the allotted time for resolution may result in verbal reprimands, notes in personnel files and termination for internal incidences and fines, legal actions and such other remedies as deemed appropriate for external incidences. |
| **Policy location**The policy will be signed, scanned into an electronic file and posted in the following location on the network: <location of policy>. |