****

**Cybersecurity policy template**

|  |
| --- |
| **Title:** Cybersecuritypolicy  |
| **Department:**  | **Version:** Original |
| **Approved by:** | **Approval date:**  |
| **Senior management approval:** |
| **Effective date:** | **Last updated:** |
| **Author:** |
| This policy applies to <company name>, <enter 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 provisioning of cybersecurity for the identification of and response to unauthorized attacks, such as phishing and ransomware, on the organization's information systems, networks, data, databases and other information assets. Additional policies governing other cybersecurity activities will be addressed separately. |
| **Scope**The scope of this cybersecurity policy includes all IT systems, software, databases, applications and network resources that are used on-premises, 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).Cybersecurity policy compliance is managed by the IT data security team, with support from other IT departments. To achieve compliance, cybersecurity processes must include appropriate procedures and identify staffing and technology resources to meet compliance requirements. Cybersecurity 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 at <company name> are to be managed by a formal cybersecurity management program. This program will provide an orderly method for preventing, identifying, capturing, analyzing and mitigating unauthorized access to <company name>'s information systems and resources. All changes to cybersecurity systems and procedures will be tested, approved and communicated for audit and record-keeping purposes.1. This policy addresses all <company name> technology, systems, data and networks implemented in company-owned and managed IT facilities; private, hybrid and/or public cloud infrastructures, plus all other <company name> IT assets implemented in managed services as identified by IT department management.
2. The IT department will define cybersecurity processes and procedures; secure and utilize specialized software and systems to reduce the threat of cybersecurity breaches; regularly test the security of the company's perimeters and the cybersecurity vendor's services using penetration tests and other forensic methods; and document all cybersecurity procedures and controls
3. The IT department will prepare and document information security and cybersecurity plans, and will facilitate the maintenance and review of those plans.
4. The IT department will periodically conduct a risk assessment of internal and external threats and vulnerabilities of the IT environment, as applicable to all operating IT environments.
5. The IT department will ensure malware, such as viruses, spam, phishing attacks, denial-of-service attacks and other unauthorized access attempts, are prevented using antivirus software and other appropriate cybersecurity prevention and detection resources. It will ensure cybersecurity and other IT vendors have similar antimalware capabilities, and the use of those services shall be approved by <company name>.
6. In coordination with this policy, the IT department will establish a network perimeter security policy to prevent unauthorized attempts to penetrate the <company name> network perimeter.
7. The IT department will establish a process for identifying possible breaches in the network perimeter, determining the nature and possible impact of the breach, notifying <company name> management of the breach, minimizing the impact of the breach as quickly as possible and documenting the steps taken when dealing with the incident. This process will apply to all operating environments, including cloud environments, whether internal, hybrid and/or public clouds.
8. The IT department will establish and document a formal process for identifying a possible internal cybersecurity breach, such as theft of information, social engineering or unauthorized access to systems. The process will involve assessing the breach, determining the nature and possible impact of the breach, notifying <company name> management, minimizing the impact of the breach and documenting the steps taken when dealing with the incident.
9. The IT department will provide cybersecurity education, training and awareness programs.
10. The IT department will include business continuity and disaster recovery among its cybersecurity controls.
11. The IT department will define consequences of violations of cybersecurity policy.
12. The IT department will define how cybersecurity incidents are reported and managed.
13. The IT department, in collaboration with the legal department, will prepare and execute the appropriate service-level agreements with cybersecurity equipment and service providers to ensure acceptable third-party vendor performance.
14. Data at <company name>, whether at rest or in motion, must be encrypted.
15. <Company name> employees must sign a contract agreeing to accept and comply with the cybersecurity policies when they are hired and on a regular basis (e.g., annually) through the employee handbook and/or in contract renewals.
16. All proposed changes to cybersecurity operations must be documented in detail.
17. Cybersecurity breaches that may impact <company name> are identified in the company's information security management system and associated documents.
18. The IT department will develop a schedule of all cybersecurity activities, and will ensure these activities are completed on time.
19. The IT department will ensure all cybersecurity policies and associated procedures comply with appropriate legislative, regulatory and contractual requirements, as well as accepted standards and practices.
20. All proposed changes to this policy are to be processed and documented on the company's IT change management system.
 |
| **Policy leadership****The <title of executive>** is designated as the corporate owner responsible for cybersecurity activities. Resolution of issues in support of cybersecurity activities must be discussed with IT management, the corporate information security 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 cybersecurity policy audits, in collaboration with the IT department.
 |
| **Management review**<Name of department or individual> will review and update this cybersecurity policy on an annual basis. As changes to this cybersecurity 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 cybersecurity response and recovery 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 cybersecurity policy and any service-level agreements established with external cybersecurity firms 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>. |