****

**Cloud security policy template**

|  |
| --- |
| **Title:** Cloud securitypolicy |
| **Department:**  | **Version:** Original |
| **Approved by:**  | **Approval date:**  |
| **Senior management approval:**  |
| **Effective date:**  | **Last updated:**  |
| **Author:**  |
| **Scope**This policy applies to the <specify location of <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 provision of security for cloud-supported activities that protect <company name>'s cloud-based 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 cloud security policy is all information technology systems, software, databases, applications and network resources that are implemented in cloud-based and/or managed service infrastructures needed by the Company to conduct its 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. 4 *Security and Privacy Controls for Federal Information Systems and Organizations*; NIST SP 800-144 *Guidelines on Security and Privacy in Public Cloud Computing* and theFFIEC Information Technology Examination Handbook for Information Security (2016).Cloud security policy compliance is managed by the IT data security team, with support from other IT departments. To achieve compliance, cloud security processes must include appropriate procedures and identify staffing and technology resources to meet compliance requirements. Cloud service vendors are required to demonstrate compliance with this policy. Compliance verification is performed monthly by the IT department, internal audit or other appropriate entity. |
| **Policy**As part of its duty of care to its customers and as a matter of good business practice, the confidentiality, integrity and availability of all IT applications, data, systems and network resources implemented in a cloud environment at <company name> are to be managed by a formal information security management program. This program will provide a controlled and orderly method by which access to cloud-based <company name> information systems is requested and granted, security of cloud-based systems and data is monitored and analyzed, violations of cloud security are addressed and mitigated, and changes to cloud security systems and procedures are requested, tested, approved and communicated for audit and recordkeeping 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 implemented in cloud services as identified by IT department management.
2. The IT department will define cloud security processes and procedures; secure and utilize specialized software and systems to reduce the threat of cloud security breaches; regularly test the security of the company’s perimeters and the cloud service vendor’s perimeters using penetration tests and other forensic methods; and document all information cloud procedures and controls.
3. The <company name> IT department will prepare and document IT information security and cybersecurity plans with a focus on cloud services; it will facilitate the maintenance and review of those plans.
4. The IT department will periodically conduct a risk assessment of the internal and external threats and vulnerabilities of the IT environment, as applicable to all cloud environments.
5. The IT department will establish a policy for data media implemented in cloud services, its creation, storage and destruction.
6. The IT department will establish a policy for accessing <company name> systems, networks, applications and files implemented in cloud services, both locally and remotely, including passwords and other cloud security access controls; this policy will also include authentication of <company name> and non- <company name> users.
7. The IT department will ensure that malware (e.g., viruses, spam, phishing attacks, denial-of-service attacks and other unauthorized access attempts) is prevented through the use of antivirus software and other appropriate prevention and detection resources. It will ensure that cloud service vendors have similar antimalware capabilities and that the use of those services shall be approved by <company name>.
8. The IT department will establish a network perimeter security policy to ensure that unauthorized attempts to penetrate the <company name> internal cloud security perimeter are prevented. It will also have a similar policy for cloud service vendors.
9. The IT department will establish and document a formal process for identifying a possible breach in cloud-based network perimeters (e.g., denial-of-service attack, phishing), assessing the breach, 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 cloud environments, whether internal, hybrid and/or public clouds.
10. The IT department will establish and document a formal process for identifying a possible internal cloud security breach (e.g., theft of information, social engineering, unauthorized access to systems), assessing the breach, 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.
11. The IT department will provide cloud security education, training and awareness programs.
12. The IT department will include business continuity and disaster recovery in its cloud security controls.
13. The IT department will define consequences of violations of cloud security policy.
14. The IT department will define how cloud security incidents are reported and managed.
15. The IT department, in collaboration with the company legal department, shall prepare and have executed the appropriate service level agreements (SLAs) with cloud service providers to ensure acceptable third-party cloud vendor performance.
16. Data in use at <company name>, whether at rest or in motion, within any approved cloud environment, must be encrypted.
17. <company name> employees must sign an employee contract agreeing to accept and comply with cloud security policies at the time they are hired and on a regular basis (e.g., annually) through the employee handbook and/or in contract renewals to account for policy changes over time.
18. All proposed changes to cloud security operations are to be documented in detail.
19. Cloud security breaches that may impact <company name>'s IT operations are identified in the company’s information security management system and associated plans.
20. The IT department will develop a schedule of all relevant cloud security activities for the company, and will ensure that these activities are completed on time.
21. The IT department will ensure all cloud security policies and associated procedures will comply with appropriate legislative, regulatory and contractual requirements, as well as accepted standards and good practice.
22. All proposed changes to this IT cloud security policy are to be processed and documented by the company’s IT change management system.
 |
| **Policy leadership** **<Title of executive>** is designated as the corporate owner responsible for cloud security activities for the Company. Resolution of issues in the support of cloud security activities should first be coordinated 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 -- The <enter name of department or individual> is responsible for planning, organizing and implementing all activities that fulfill this policy.
* Policy maintenance and updating -- The <enter name of department or individual> is responsible for all activities associated with maintaining and updating this policy.
* Policy monitoring and review -- The <enter name of department or individual> is responsible for monitoring and reviewing this policy.
* Policy improvement -- The <enter name of department or individual> is responsible for defining and implementing activities that will improve this policy.
* Policy auditing -- The <company name> internal audit department, or an approved external audit organization, organizes and coordinates the completion of cloud security policy audits, in collaboration with the IT department.
 |
| **Management review**<Enter name of department or individual> will review and update this cloud security policy on an annual basis. As changes to this cloud security policy are indicated in the course of business, <enter name of department or individual> may initiate a change management process to update this policy. |
| **Policy enforcement**The **<title of executive>** will enforce this policy. |
| **Penalties for noncompliance** In situations where cloud security 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 cloud security policy and any SLAs established with external cloud service firms within the allotted time for resolution may result in verbal reprimands, notes in personnel files and termination (for internal incidents) and fines, legal actions and such other remedies as deemed appropriate (for external incidents). |
| **Policy location**The policy will be signed, scanned into an electronic file and posted in the following location on the network: <enter location of policy>. |