# Cloud Security Policy Template

Use this template to outline your organization’s policies and approach to enforcing cloud security. To learn more about crafting your policy, read our guide, “How To Create A Cloud Security Policy”.

| **<Organization>** Cloud Security Policy | |
| --- | --- |
| **Version:** Original  **Last updated:** n/a | |
| **Approved by:** | **Approval date:** |
| **Senior management approval:** | |
| This policy applies to the <specify location of <company name>>    <enter address> | |
| **Purpose**    This cloud security policy sets rules and guidelines for employees, contractors, and other partners of <company name> that might be working on shared cloud platforms like Google Drive and Slack. The policy establishes roles and responsibilities related to cloud security, covering:   * Who is in charge of provisioning user credentials? * What is the approval process for adding new features to your cloud platforms? * Who is in charge of updating software for your cloud security tools? * What compliance regulations do we need to meet? | |
| **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 <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.  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. | |
| **Threat analysis**  <company name> will regularly audit its systems to understand:   * What cloud programs are employees using regularly? * What security systems are already in place governing those programs? * What cloud program are employees NOT using regularly? * How does data move through the organization?   The most recent audit was completed on <date>. The following cloud programs were found to be in use. User roles were reviewed and updated. The latest security patches and version updates were also installed.  **Reviewed by:** <name>  <list cloud programs in use by employees>  The following cloud programs were retired, with user permissions updated and de-installed.  <list cloud programs that were sunsetted>  **The following threats were identified.**  <insert risk assessment>  **RISK IMPACT *select one***   |  | **IMPACT LEVEL** | **DESCRIPTION** | | --- | --- | --- | |  | **NOT SIGNIFICANT** | **Negligible risk of data exfiltration or leakage** | |  | **MINOR** | **Minor risk of data exfiltration or leakage** | |  | **MODERATE** | **Business interruption possible** | |  | **MAJOR** | **Immediate action needed to mitigate threat** | |  | **SEVERE** | **Initiate business continuity plan** |     **RISK PROBABILITY *select one***   |  | **PROBABILITY LEVEL** | **DESCRIPTION** | | --- | --- | --- | |  | **HIGHLY UNLIKELY** | **Rare chance of an occurrence** | |  | **UNLIKELY** | **Not likely to occur under normal circumstances** | |  | **POSSIBLE** | **May occur at some point under normal circumstances** | |  | **LIKELY** | **Expected to occur at some point in time** | |  | **HIGHLY LIKELY** | **Expected to occur regularly under normal circumstances** |     **RISK SEVERITY MATRIX *based on Impact and Probability Levels***   | **IMPACT x PROBABILITY** | **NOT SIGNIFICANT** | **MINOR** | **MODERATE** | **MAJOR** | **SEVERE** | | --- | --- | --- | --- | --- | --- | | **HIGHLY UNLIKELY** | **LOW** | **LOW** | **LOW / MED** | **MEDIUM** | **MEDIUM** | | **UNLIKELY** | **LOW** | **LOW / MED** | **LOW / MED** | **MEDIUM** | **MED / HIGH** | | **POSSIBLE** | **LOW** | **LOW / MED** | **MEDIUM** | **MED / HIGH** | **MED / HIGH** | | **LIKELY** | **LOW** | **LOW / MED** | **MEDIUM** | **MED / HIGH** | **HIGH** | | **HIGHLY LIKELY** | **LOW / MED** | **MEDIUM** | **MED / HIGH** | **HIGH** | **HIGH** |       **RISK SEVERITY LEVEL *select corresponding Severity Level from matrix above based upon Impact and Probability Levels***   |  | **SEVERITY LEVEL** | | --- | --- | |  | **LOW** | |  | **LOW / MED** | |  | **MEDIUM** | |  | **MED / HIGH** | |  | **HIGH** |     **FURTHER ACTION NEEDED? *select one***   |  | **YES** | | --- | --- | |  | **NO** |     **ACTIONS TO IMPLEMENT *if applicable***   | **ACTION** | **ASSIGNED TO** | **DUE DATE** | **STATUS** | | --- | --- | --- | --- | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | | |
| **Policy**    As part of its duty of care to its customers, 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 method for accessing, securing, monitoring and analyzing violations of cloud security. Changes to cloud security systems and procedures will be requested, tested, approved, and recorded for audit 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 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.  4. The IT department will establish an identity and access management program to access <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 the 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 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. | |
| **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. | |
| **Management review**    <Enter name of department or individual> will review and update this cloud security policy on a quarterly 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>. | |

Disclaimer: While we have made every attempt to ensure that the information contained in this guide is accurate to our best efforts, Shoreline Labs, Inc., is not responsible for any errors or omissions, or for any result obtained from the use of this information. This guide is based on a specific point in time, and is no guarantee of completeness, accuracy, timeliness, or of the results obtained from the use of this information. Nothing in this guide should be used as a substitute for the independent investigations and the sound technical and business judgment of your legal and compliance professionals. We do not accept any liability if this guide is used for an alternative purpose from which it is intended, nor to any third party for any purpose. In no event will Shoreline Labs, Inc., its employees or agents, be liable to you or anyone else for any decision made or action taken in reliance on this guide or for any consequential, special or similar damages, even if advised of the possibility of such damage