Cybersecurity Policy Templates

Cloud Service Provider Management Policy

(Last Updated April 2025)

Purpose

Our Cloud Service Provider Policy is designed to establish a comprehensive and systematic framework for the selection, engagement, and continuous oversight of cloud services within our organization. This policy delineates clear criteria and protocols for evaluating potential cloud service providers, ensuring that they meet our stringent security, privacy, and operational performance standards. By laying out structured due diligence and risk assessment procedures, this policy is instrumental in mitigating the potential risks associated with cloud computing, such as data breaches, service disruptions, and compliance lapses.

Scope

The Cloud Service Provider Policy applies to all personnel within our organization, including full-time employees, part-time staff, consultants, and external business partners who interact with cloud computing resources. This policy comprehensively encompasses cloud service providers' selection, implementation, and management. It delineates the scope of cloud services across our infrastructure, including but not limited to SaaS, PaaS, and IaaS models. It prescribes the standards for evaluating potential providers' security posture, managing cloud access controls and data protection mechanisms, and integrating cloud services with our existing IT environment. The policy mandates consistent and rigorous assessments to ensure that cloud engagements align with our organizational security requirements, data governance policies, and regulatory compliance mandates. Adherence to this policy is compulsory for all applicable entities within the company, and it necessitates that any exemptions or deviations be formally reviewed and sanctioned by the appointed governance body overseeing cloud strategy and cybersecurity directives.

Safeguards

To achieve the organization's overall mission, and the purpose of this cybersecurity policy, the organization shall:

CSP-01	Maintain an inventory of each of the organization's authorized Cloud Service Providers (CSPs).
CSP-02	Maintain an inventory of each service authorized for use in each authorized Cloud Service Provider (CSP).
CSP-03	Maintain an inventory of the organization's authorized Software-as-a-Service (SaaS) providers.
CSP-04	Maintain an inventory of the accounts authorized for use in each of the authorized Cloud Service Providers (CSPs) or Software-as-a-Service (SaaS) providers.
CSP-05	Maintain a cybersecurity configuration benchmark for each of the organization's authorized Cloud Service Providers (CSPs).
CSP-06	Maintain a cybersecurity configuration benchmark for each of the services authorized for use in each of the organization's authorized Cloud Service Providers (CSPs).
CSP-07	Maintain a cybersecurity configuration benchmark for each of the organization's authorized Software-as-a-Service (SaaS) providers.
CSP-08	Maintain a cloud configuration vulnerability management system to regularly scan each of the organization's authorized Cloud Service Providers (CSPs) or Software-as-a-Service (SaaS) providers for potential cybersecurity vulnerabilities.
CSP-09	Maintain a Data Loss Prevention (DLP) system to log and alert on potential data loss events in the organization's Cloud Service Providers (CSPs) or Software-as-a-Service (SaaS) providers regularly.

CSP-10 Ensure that appropriate logs from the organization's authorized Cloud Service Providers (CSPs) or Software-as-a-Service (SaaS) providers are enabled on the cloud platform.

CSP-11 Ensure that appropriate logs from the organization's authorized Cloud Service Providers (CSPs) or Software-as-a-Service (SaaS) providers are aggregated into the organization's log management system.

Policy Sanctions

Non-compliance with this policy may result in disciplinary action in line with our corporation's human resources procedures. Consequences may range from mandatory refresher training and written warnings to temporary suspension of remote access privileges and, in severe cases, termination of employment or contractual obligations. Individuals could be subject to legal consequences under applicable laws if violations involve illegal activities. These sanctions emphasize the critical importance of cybersecurity, the individual's role in protecting our digital assets, and the potential risks associated with policy violations. Enforcement will be consistent and impartial, with the severity of the action corresponding directly to the seriousness of the breach.