Cybersecurity Policy Templates

Third-Party Management Policy

(Last Updated April 2025)

Purpose

Our Third-Party Risk Management Policy aims to establish a robust and risk-based approach for evaluating, selecting, contracting, and monitoring third-party vendors and partners to ensure the security of our organization's information assets. This policy aims to provide clear guidelines and procedures for assessing the cybersecurity posture of third parties, managing vendor relationships, and enforcing contractual obligations related to security controls and data protection. By implementing effective third-party management practices, this policy seeks to mitigate the potential risks posed by third-party relationships, safeguard our systems, data, and networks from unauthorized access and breaches, and protect our sensitive information's confidentiality, integrity, and availability. Through a comprehensive due diligence process, regular monitoring, and ongoing communication, we strive to establish and maintain a trusted ecosystem of third-party providers that align with our security standards, regulatory requirements, and overall risk appetite.

Scope

The Third-Party Risk Management Policy applies to all employees, contractors, and stakeholders engaging and collaborating with third-party entities with access to the organization's systems, data, or networks. This policy encompasses the assessment, selection, contracting, and ongoing management of third-party vendors, suppliers, partners, and service providers to protect the organization's sensitive information and maintain the integrity of its cybersecurity posture. It sets forth guidelines and procedures for evaluating third parties' cybersecurity capabilities and practices, including due diligence assessments, contractual obligations, and periodic audits. The policy mandates the inclusion of robust cybersecurity controls and requirements within vendor contracts and establishes mechanisms for monitoring, reporting, and remediation of any identified risks or incidents. Compliance with this policy is mandatory for all individuals involved in third-party management, and any deviations or exceptions require approval from the designated authority responsible for cybersecurity governance.

Safeguards

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

TPR-01	Maintain a process for approving each of the organization's third parties that store or process any of the organization's technology systems or data.
TPR-02	Maintain a Governance, Risk, and Compliance (GRC) or similar platform to document and inventory each of the organization's third parties that store or process any of the organization's technology systems or data.
TPR-03	Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar platform to document and inventory each of the organization's third parties that store or process any of the organization's technology systems or data maintains a complete inventory of all such third parties.
TPR-04	Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar platform to document and inventory each of the organization's third parties that store or process any of the organization's technology systems or data documents the demographics of all such third parties (such as business owner, criticality, whether data is shared).
TPR-05	Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar platform to document and inventory each of the organization's third parties that store or process any of the organization's technology systems or data maintains a complete data inventory of all data stored or processed by such third-parties.
TPR-06	Maintain consistent, appropriate, and approved contract language for each organization's third parties that store or process any of the organization's technology systems or data.
TPR-07	Ensure that the organization's third-party contract language includes provisions requiring any third party that experiences a significant cybersecurity event (such as a data breach) to promptly report it to the organization.

TPR-08	Ensure that the organization's third-party contract language includes provisions that all third parties must implement cybersecurity safeguards.
TPR-09	Ensure that the organization's third-party contract language includes provisions requiring all third parties to implement a defined set of cybersecurity safeguards, also defining which of those safeguards are optional versus mandatory.
TPR-10	Ensure that each of the organization's third parties that store or process any of the organization's technology systems or data signs the agreed-upon contract terms.
TPR-11	Ensure that each of the organization's third parties that store or process any of the organization's technology systems or data is regularly assessed for the appropriate cybersecurity safeguards.
TPR-12	Ensure that each of the organization's third parties that store or process any of the organization's technology systems or data is monitored for significant cybersecurity events.
TPR-13	Ensure that each of the organization's third parties that store or process any of its technology systems or data are given an aggregate cybersecurity rating based on their criticality, implementation of appropriate cybersecurity safeguards, and occurrence of significant cybersecurity events.
TPR-14	Ensure that each of the organization's third parties that store or process any of the organization's technology systems or data are appropriately decommissioned when there is no longer a need for the third party to perform such services.

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.