Cybersecurity Policy Templates

Safeguard Selection Management Policy

(Last Updated April 2025)

Purpose

Our Cybersecurity Safeguard Selection Policy aims to establish a systematic and consistent approach to developing, maintaining, and enforcing security policies that align with industry standards, regulatory requirements, and our organization's risk appetite. This policy aims to provide clear guidelines and procedures for creating, reviewing, approving, disseminating, and enforcing security policies across our organization. By implementing effective policy management practices, this policy seeks to ensure that our security policies remain current, relevant, and enforceable, supporting protecting our systems, data, and networks from potential vulnerabilities and threats. Through a centralized and coordinated process, we aim to promote a culture of security awareness, accountability, and compliance, while enabling the efficient governance of our cybersecurity program.

Scope

The Cybersecurity Safeguard Selection Policy applies to all employees, contractors, vendors, and third-party entities connected to our organization's network infrastructure and information systems. This policy encompasses identifying, assessing, monitoring, and mitigating cybersecurity threats and vulnerabilities. It outlines the procedures and practices for proactive threat intelligence, security monitoring, incident response, and recovery measures. The policy applies to all devices, systems, applications, and data assets owned or used by the organization. Compliance with this policy is mandatory for all individuals, and it is essential to promptly report any potential or actual cybersecurity threats. Any exceptions or deviations from this policy require approval from the designated authority responsible for cybersecurity threat management.

Safeguards

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

SAF-01 Maintain a detailed and documented taxonomy of all cybersecurity threats that could harm the organization's information systems.

SAF-02 Regularly evaluate cybersecurity threats to the organization and define, document, and approve cybersecurity safeguards to address these threats.

SAF-03 Maintain subscriptions to relevant cybersecurity threat intelligence feeds to ensure the organization's threat taxonomy is updated with the latest cybersecurity threats.

SAF-04 Maintain a detailed and documented list of characteristics that will be used to model each threat in the organization's cybersecurity threat taxonomy.

SAF-05 Ensure that the organization's threat model prioritizes each of the threats in the organization's cybersecurity threat taxonomy.

SAF-06 Maintain a documented board of directors-level cybersecurity policy that defines the high-level categories of cybersecurity safeguards that will be implemented to achieve the goals defined in the organization's cybersecurity program charter.

SAF-07 Maintain a detailed and documented list of all appropriate cybersecurity safeguards the organization must implement to achieve the goals defined in its cybersecurity program charter.

SAF-08 Ensure that the organization has aspirationally defined a complete list of the appropriate cybersecurity safeguards it must implement to achieve the goals defined in its cybersecurity program charter.

SAF-09 Ensure that the organization's cybersecurity safeguard documentation clearly defines the scope of applicability for each documented cybersecurity safeguard.

SAF-10	Ensure that the organization's cybersecurity safeguard documentation clearly defines the sanctions imposed if the documented cybersecurity safeguards are violated.
SAF-11	Ensure that the organization's cybersecurity safeguard documentation clearly defines mappings to regulatory or standards-based requirements for each documented cybersecurity safeguard.
SAF-12	Ensure that the organization's cybersecurity safeguard documentation clearly defines a business stakeholder responsible for each documented cybersecurity safeguard.
SAF-13	Ensure that the organization's cybersecurity safeguard documentation clearly defines the job roles that must be aware of each of the documented cybersecurity safeguards.
SAF-14	Ensure that the organization's cybersecurity safeguard documentation clearly defines a quantifiable measure of compliance for each of the documented cybersecurity safeguards.
SAF-15	Maintain detailed and documented acceptable use statements that define how an organization's workforce members shall appropriately utilize information systems.
SAF-16	Ensure that each prioritized threat in the organization's cybersecurity threat model is mapped against each of the corresponding cybersecurity safeguards in the organization's list of documented safeguards.
SAF-17	Regularly review all of the documentation used to define the organization's cybersecurity safeguards to ensure they are appropriate and up-to-date.

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.