Cybersecurity Policy Templates

Program Management Policy

(Last Updated April 2025)

Purpose

Our Cybersecurity Program Management Policy aims to establish a comprehensive framework that ensures the confidentiality, integrity, and availability of our organization's information assets. This policy seeks to protect our systems, data, and networks from unauthorized access, misuse, and potential threats while promoting responsible and secure practices throughout the organization. By implementing robust governance measures, this policy seeks to mitigate risks, enhance the resilience of our infrastructure, foster a culture of security awareness, and align our cybersecurity efforts with industry best practices and regulatory requirements. Through effective governance, we strive to maintain the trust of our stakeholders, safeguard our reputation, and safeguard the sensitive information entrusted to us.

Scope

The Cybersecurity Program Management Policy applies to all our organization's employees, contractors, vendors, and stakeholders, irrespective of their roles or responsibilities. This policy encompasses all aspects of cybersecurity governance, including strategic planning, risk management, compliance, incident response, and continual improvement. It establishes a framework to guide the organization in effectively managing and mitigating cybersecurity risks, protecting critical information assets, and ensuring sensitive data's confidentiality, integrity, and availability. The policy outlines the responsibilities and accountabilities of individuals within the organization for maintaining a robust cybersecurity posture, complying with relevant laws and regulations, and adhering to industry best practices. Compliance with this policy is mandatory for all personnel, and any exceptions or deviations must be approved by 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:

PRG-01 Maintain a cybersecurity program charter that authorizes the existence of a program and gives authority to the program team to use organizational resources to achieve the program objectives.

PRG-02 Ensure that the organization's cybersecurity program charter defines its scope and applicability to each of the organization's business units or related entities.

PRG-03 Ensure that the organization's cybersecurity program charter defines the ultimate goal of the cybersecurity program as the confidentiality, integrity, and availability of the organization's information systems.

PRG-04 Ensure that the organization's cybersecurity program charter defines all the cybersecurity regulations and standards it shall use to define its goals for specific cybersecurity safeguards.

PRG-05 Ensure that the organization's cybersecurity program charter or supporting documentation formally defines the organization's approach to cybersecurity governance and risk management.

PRG-06 Ensure that the organization's cybersecurity program charter defines the executive leadership sponsor for the organization's cybersecurity program.

PRG-07 Ensure that the organization's cybersecurity program charter establishes the authority of the stakeholder committee responsible for the program.

PRG-08 Ensure that the organization's cybersecurity program charter or supporting documentation lists the specific stakeholder committee members responsible for the organization's cybersecurity program.

PRG-09 Ensure that the organization's cybersecurity program charter or supporting documentation lists the specific members of the stakeholder committee responsible for its cybersecurity program and that they are from a diverse set of business units, not simply the technology teams.

PRG-10 Ensure that the organization's cybersecurity program charter or supporting documentation defines the roles and responsibilities of the stakeholder committee members responsible for the organization's cybersecurity program.

PRG-11 Ensure that the organization's cybersecurity program charter or supporting documentation defines the logistics details (such as meeting cadence and rules of order) for the stakeholder committee responsible for the organization's cybersecurity program.

PRG-12 Ensure that the organization's cybersecurity program charter has been formally reviewed and updated by the organization's board of directors or executive leadership team.

PRG-13 Ensure that the organization's board has formally approved the organization's cybersecurity program charter of directors or executive leadership team.

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.