Cybersecurity Policy Templates

Safeguard Implementation Management Policy

(Last Updated April 2025)

Purpose

Our Cybersecurity Safeguard Implementation Policy aims to establish a structured and standardized approach to managing cybersecurity projects throughout their lifecycle, ensuring the successful implementation of security initiatives and the protection of our organization's information assets. This policy aims to provide clear guidelines and procedures for the planning, execution, monitoring, and controlling of cybersecurity projects, integrating security requirements into all phases of project management. By implementing effective project management practices, this policy seeks to minimize project risks, optimize resource allocation, and ensure the timely delivery of cybersecurity solutions that align with industry best practices and regulatory obligations. Through consistent methodologies and collaboration between stakeholders, we strive to enhance our organization's security posture, strengthen our resilience against cyber threats, and safeguard the confidentiality, integrity, and availability of our systems, data, and networks.

Scope

The Cybersecurity Safeguard Implementation Policy applies to all employees, contractors, and stakeholders involved in the planning, execution, and oversight of cybersecurity projects within our organization. This policy encompasses the management of projects aimed at enhancing the organization's cybersecurity posture, implementing security controls, and addressing vulnerabilities and risks. It covers project initiation, planning, execution, monitoring, and closure phases, ensuring that cybersecurity requirements are integrated throughout the project lifecycle. The policy establishes guidelines for project governance, risk management, stakeholder communication, and resource allocation to ensure the successful delivery of cybersecurity projects. Compliance with this policy is mandatory for all individuals involved in cybersecurity project 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:

IMP-01	Define a process the organization will use to document and track each of its cybersecurity projects (such as a formal Project Management Office (PMO)).
IMP-02	Maintain a cybersecurity project tracking system (such as a Project Management Office (PMO) tool) to track each organization's cybersecurity projects.
IMP-03	Ensure the organization's cybersecurity project tracking system is used to document each of the organization's active cybersecurity projects.
IMP-04	Ensure the organization's cybersecurity project tracking system prioritizes each of its active cybersecurity projects.
IMP-05	Ensure the organization's cybersecurity project tracking system is used to track the capital implementation costs for each organization's active cybersecurity project.
IMP-06	Ensure the organization's cybersecurity project tracking system is used to track the personnel implementation costs for each organization's active cybersecurity project.
IMP-07	Ensure the organization's cybersecurity project tracking system is used to track the status of each organization's active cybersecurity project.
IMP-08	Define a process the organization shall use to document and track each of the organization's approved cybersecurity exceptions when these cause information systems or software applications to be out of compliance with the organization's approved cybersecurity safeguards.
IMP-09	Define a process the organization shall use to document which business stakeholder(s) are authorized to approve cybersecurity exceptions in the organization's cybersecurity exception process.

IMP-10	Maintain a system to track all approved and documented cybersecurity exceptions to the organization's approved cybersecurity safeguards (such as a Governance, Risk, and Compliance (GRC) system or risk register).
IMP-11	Define a process the organization shall use to document and track each of the organization's issues (or defects) when these cause information systems or software applications to be out of compliance with the organization's approved cybersecurity safeguards.
IMP-12	Ensure that the organization assigns appropriate resources to address each of its cybersecurity projects and issues in a timely manner.
IMP-13	Regularly review each of the cybersecurity projects, cybersecurity exceptions, and cybersecurity issues to the organization's approved cybersecurity safeguards and report the status of each to the organization's 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.