Cybersecurity Policy Templates

Safeguard Validation Management Policy

(Last Updated April 2025)

Purpose

Our Cybersecurity Safeguard Validation Policy aims to establish a systematic and comprehensive framework for planning, conducting, and managing cybersecurity audits within our organization. This policy aims to provide clear guidelines and procedures for assessing the effectiveness of our cybersecurity controls, identifying vulnerabilities and weaknesses, and ensuring compliance with industry standards, legal regulations, and internal policies. By implementing effective audit management practices, this policy seeks to enhance our cybersecurity governance, identify areas for improvement, and mitigate potential risks and threats. Through regular audits and independent assessments, we strive to maintain the integrity, confidentiality, and availability of our systems, data, and networks while continuously improving our security posture and demonstrating our commitment to security to stakeholders.

Scope

The Cybersecurity Safeguard Validation Policy applies to all employees, contractors, and stakeholders involved in conducting and managing cybersecurity audits within our organization. This policy encompasses the planning, execution, and oversight of audits to evaluate cybersecurity controls and processes' effectiveness, compliance, and maturity. It covers internal and external audits, including regulatory compliance audits, vulnerability assessments, penetration tests, and security risk assessments. The policy establishes guidelines for audit planning, scoping, resource allocation, documentation, and reporting. It ensures that audit findings are addressed, remediation plans are developed, and continuous improvement is fostered. Compliance with this policy is mandatory for all individuals involved in Cybersecurity Safeguard Validation, 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:

VAL-01 Maintain a cybersecurity safeguard validation (audit) plan that documents the assessments the organization shall perform to validate the quality of the organization's cybersecurity safeguards.

VAL-02 Ensure that the organization's cybersecurity safeguard validation (audit) plan is a multi-year plan that regularly addresses all of the scopes the organization should assess.

VAL-03 Ensure that the organization's cybersecurity safeguard validation (audit) plan establishes criticality rankings for each of the assessment scopes in its assessment plan.

VAL-04 Ensure that the organization's cybersecurity safeguard validation (audit) plan defines who should perform each assessment scope in its assessment plan.

VAL-05 Ensure that the organization's cybersecurity safeguard validation (audit) plan includes each of the cybersecurity penetration testing scopes it should assess regularly.

VAL-06 Ensure that the organization's cybersecurity safeguard validation (audit) plan includes software application penetration tests in its assessment plan.

VAL-07 Ensure that the organization's cybersecurity safeguard validation (audit) plan includes red team cybersecurity assessments in its assessment plan.

VAL-08 Ensure that the organization's cybersecurity safeguard validation (audit) plan defines where cybersecurity penetration testing should be performed only against test systems due to the sensitivity of such systems.

VAL-09 Ensure that the organization's cybersecurity safeguard validation (audit) plan defines how cybersecurity penetration testing should utilize vulnerability scanners as a part of the assessments.

VAL-10	Ensure that the organization's cybersecurity safeguard validation (audit) plan defines when cybersecurity penetration testing should be documented in machine-readable formats (such as SCAP).
VAL-11	Ensure that the organization's cybersecurity safeguard validation (audit) plan defines how the organization will monitor user accounts during cybersecurity penetration tests.
VAL-12	Ensure that the organization's leadership stakeholders regularly approve the organization's cybersecurity safeguard validation (audit) plan.
VAL-13	Ensure that the organization's leadership stakeholders regularly allocate and assign resources to the organization's safeguard validation (audit) plan and complete each assessment according to the schedule defined.
VAL-14	Ensure that the organization documents the results of each cybersecurity assessment in a central software platform (such as a Governance, Risk, and Compliance (GRC) tool).
VAL-15	Ensure that the organization tracks the progress of each cybersecurity assessment in a central software platform (such as a Governance, Risk, and Compliance (GRC) tool).
VAL-16	Ensure that the organization regularly reports the results of each cybersecurity assessment to its leadership stakeholders.

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.