Cybersecurity Policy Templates

Risk Communication Management Policy

(Last Updated April 2025)

Purpose

Our Cybersecurity Risk Communication Policy aims to establish a structured and consistent approach for identifying, assessing, documenting, and communicating cybersecurity risks to key stakeholders within our organization. This policy aims to provide clear guidelines and procedures for the timely and accurate reporting of cybersecurity risks, ensuring that decision-makers have the necessary information to make informed risk management decisions. This policy seeks to enhance transparency, accountability, and risk awareness throughout the organization by implementing effective risk reporting practices. Through standardized risk reporting formats, risk metrics, and risk mitigation recommendations, we strive to enable proactive risk management, prioritize resource allocation, and strengthen the overall cybersecurity posture of our organization. We aim to foster a risk-aware culture through regular and comprehensive risk reporting, enable risk-based decision-making, and protect our systems, data, and networks from potential threats.

Scope

The Cybersecurity Risk Communication Policy applies to all employees, contractors, and stakeholders responsible for assessing, managing, and reporting cybersecurity risks within our organization. This policy encompasses identifying, analyzing, and reporting potential and existing cybersecurity risks, vulnerabilities, and threats that could impact the confidentiality, integrity, and availability of critical systems and data. It sets forth guidelines for risk assessment methodologies, risk classification, and risk reporting formats to ensure consistent and accurate reporting across the organization. The policy mandates the timely reporting of cybersecurity risks to the designated authorities, including executive management, risk management committees, and regulatory bodies, as required. Compliance with this policy is mandatory for all individuals involved in cybersecurity risk reporting, 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:

COM-01	Maintain a Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform to document, track, and report on the organization's cybersecurity risks.
COM-02	Ensure the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform maps its cybersecurity tools against approved and prioritized cybersecurity safeguards.
COM-03	Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform automatically integrates with all appropriate cybersecurity technologies to aggregate data regarding potential cybersecurity risks.
COM-04	Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform manually records the status of cybersecurity safeguards that cannot be automatically entered into the system.
COM-05	Ensure the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform defines quality thresholds for each aggregated, quantified data point.
COM-06	Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform utilizes dashboards that report cybersecurity risk on a safeguard basis.
COM-07	Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform utilizes dashboards that report cybersecurity risk per business unit.
COM-08	Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform utilizes

dashboards that report cybersecurity risk in a way that takes approved exceptions into account and in a way that does not take approved exceptions into account.

COM-09 Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform regularly reports cybersecurity risk to executive leadership stakeholders.

COM-10 Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform regularly reports cybersecurity risk to business stakeholders.

COM-11 Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform regularly reports cybersecurity risk to technical 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.