Cybersecurity Policy Templates

Education Management Policy

(Last Updated April 2025)

Purpose

Our Cybersecurity Education Policy aims to establish a comprehensive framework for promoting a culture of cybersecurity awareness, knowledge, and responsible behavior throughout our organization. This policy aims to provide guidelines and procedures for developing, implementing, and continuously improving cybersecurity education and awareness programs that empower our employees to recognize, prevent, and respond to potential cyber threats. By prioritizing education and awareness, this policy seeks to enhance the overall security posture of our organization, reduce the likelihood of human error leading to security incidents, and foster a sense of shared responsibility for protecting our systems, data, and networks. Through regular training, communication, and engagement initiatives, we strive to cultivate a vigilant and resilient workforce equipped to safeguard our sensitive information and assets in the face of evolving cybersecurity risks.

Scope

The Cybersecurity Education Policy applies to all our organization's employees, contractors, vendors, and stakeholders. This policy encompasses planning, developing, implementing, and evaluating cybersecurity education and awareness programs to foster a culture of security awareness and responsible behavior. It covers training sessions, workshops, communication campaigns, and resources to enhance understanding of cybersecurity risks, best practices, policies, and procedures. The policy applies to all individuals who access the organization's network, systems, and sensitive information. Compliance with this policy is mandatory for all personnel, and active participation in cybersecurity education and awareness initiatives is required. Any exceptions or deviations from this policy 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:

EDU-01	Ensure that all workforce members have access to the documentation defining the cybersecurity safeguards related to their roles and responsibilities.
EDU-02	Maintain a technology platform for delivering cybersecurity-related education to workforce members (such as a Learning Management System (LMS)).
EDU-03	Maintain a technology platform (such as a Learning Management System (LMS)) for tracking cybersecurity-related education delivered to workforce members.
EDU-04	Ensure that all workforce members (including engineers, developers, and privileged users) regularly receive appropriate education on cybersecurity safeguards related to their roles and responsibilities.
EDU-05	Ensure that all workforce members regularly receive appropriate cybersecurity awareness training that is appropriate to their roles and responsibilities.
EDU-06	Ensure that the organization's cybersecurity education program appropriately educates workforce members on securely authenticating to information systems.
EDU-07	Ensure the organization's cybersecurity education program appropriately educates workforce members on securely communicating over untrusted networks.
EDU-08	Ensure that the organization's cybersecurity education program appropriately educates workforce members on securely handling data, including the most likely reasons data may be exposed.

EDU-09	Ensure the organization's cybersecurity education program appropriately educates workforce members on securely responding to social engineering techniques, including identifying and handling such activities.
EDU-10	Ensure the organization's cybersecurity education program appropriately educates workforce members on securely reporting cybersecurity safeguard failures.
EDU-11	Ensure that the organization's cybersecurity education program appropriately educates workforce members on securely reporting potential cybersecurity incidents to the organization.
EDU-12	Regularly perform educational activities that reinforce the organization's cybersecurity education program and validate the effectiveness of the program.
EDU-13	Regularly validate the effectiveness of the organization's cybersecurity education program using quantifiable measures that can be reported to business stakeholders.
EDU-14	Regularly report the results of the validation of the effectiveness of the organization's cybersecurity education program to business 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.