Cybersecurity Policy Templates

Software Development Management Policy

(Last Updated April 2025)

Purpose

Our Software Development Policy aims to define and implement robust, secure, and standardized practices throughout the software lifecycle, including design, development, testing, deployment, and maintenance. This policy aims to mitigate the risks associated with insecure coding practices, inadequate testing, and unauthorized modifications, thereby ensuring the reliability, stability, and security of the software we create and deploy. By establishing clear procedures, this policy upholds our commitment to deliver high-quality, secure software that supports our business objectives, meets regulatory compliance standards, and provides value to our stakeholders while protecting our digital assets' integrity, confidentiality, and availability.

Scope

The Software Development Policy applies to all software development activities conducted by employees, contractors, and third-party vendors on behalf of our organization. It encompasses the entire software development lifecycle, including planning, design, coding, testing, deployment, maintenance, and retirement of software applications and systems. This policy applies to all software development projects, regardless of the platform, programming language, or development methodology employed. It establishes guidelines, standards, and best practices to ensure the security, reliability, and integrity of the software developed within our organization. Compliance with this policy is mandatory for all individuals involved in software development, and adherence to industry-specific regulations, software licensing requirements, and intellectual property rights is essential. Deviations or exceptions to this policy must be approved by the designated authority responsible for software development governance and security.

Safeguards

To achieve the organization's overall mission, and the purpose of this cybersecurity policy, the organization shall:

SDM-01	Ensure the organization's software development program adheres to the organization's cybersecurity governance safeguards.
SDM-02	Ensure that each of the organization's software application development teams is governed by the organization's approved cybersecurity governance program.
SDM-03	Maintain a documented Software Development Lifecycle (SDLC) to govern the organization's development and maintenance of software applications.
SDM-04	Ensure that each of the organization's software application development teams follows the organization's approved Software Development Lifecycle (SDLC).
SDM-05	Maintain an approved inventory of each software development coding language used by the organization's software application development teams (by team).
SDM-06	Maintain a documented set of coding standards for each software development coding language used by the organization's software application development teams.
SDM-07	Ensure that each organization's software development coding standards define how software application developers perform input validation in their software applications.
SDM-08	Ensure that each organization's software development coding standards define how software application developers will only utilize organization and industry-approved encryption algorithms in their software applications.
SDM-09	Ensure that each organization's software development coding standard defines how software application developers will only utilize organization,

and industry-approved data exchange protocols in their software applications.

SDM-10 Ensure that each of the organization's software development coding standards specifically defines how software application developers will perform error handling in their software applications.

SDM-11 Ensure that each of the organization's software development coding standards defines how software application developers will include data privacy values in their software applications.

SDM-12 Maintain technical safeguards to create separation between the organization's development and production application systems.

SDM-13 Ensure that the organization's non-production application systems do not contain any sensitive or personally identifiable information.

SDM-14 Ensure that the organization's software application development teams do not have privileged access to the organization's production application systems.

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.