Cybersecurity
Policy Templates

CRF SANS

Configuration Management Policy

(Last Updated April 2025)

Purpose

Our Cybersecurity Configuration Management Policy aims to establish a structured and standardized approach for managing and controlling the configuration of our organization's information systems, networks, and devices. This policy aims to provide clear guidelines and procedures for identifying, documenting, tracking, and maintaining system configurations to ensure their integrity, availability, and security. By implementing effective configuration management practices, this policy seeks to minimize the risk of unauthorized access, data breaches, and system disruptions caused by misconfigurations or vulnerabilities. Through configuration baselines, change management processes, and regular audits, we strive to enforce consistent and secure configurations, reduce the attack surface, and protect the confidentiality, integrity, and availability of our systems and data. By prioritizing configuration management, we enhance our overall cybersecurity posture, maintain compliance with industry standards and regulatory requirements, and safeguard the interests of our stakeholders.

Scope

The Configuration Management Policy applies to all our organization's employees, contractors, and stakeholders and encompasses the management and control of configuration settings and changes within our IT infrastructure. This policy covers all hardware, software, network devices, and systems that require consistent and secure configurations to maintain their integrity, availability, and compliance with organizational standards. It establishes guidelines for configuration baselines, change management processes, and version control to ensure that configurations are documented, approved, and monitored. The policy also defines procedures for configuration drift detection, configuration audits, and configuration backups. Compliance with this policy is mandatory for all individuals within the organization, and any deviations or exceptions require approval from the designated authority responsible for configuration management and cybersecurity governance.

Safeguards

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

CFG-01 Maintain a library of approved operating system configuration benchmarks to ensure that each organization's operating systems are configured securely.

CFG-02 Ensure that the organization's approved operating system configuration benchmark defines the organization as able to disable all unnecessary services in the operating system.

CFG-03 Ensure that the organization's approved operating system configuration benchmark defines that the organization shall define configuration benchmarks for each necessary service, including databases, SMB services, tiny services, VoIP, and similar services.

CFG-04 Ensure that the organization's approved operating system configuration benchmark defines the organization as having unnecessary scripting languages in the operating system.

CFG-05 Ensure that the organization's approved operating system configuration benchmark defines it as enabling advanced logging for operating system shells (such as Microsoft PowerShell or BASH).

CFG-06 Ensure that the organization's approved operating system configuration benchmark defines that the organization shall enforce cybersecurity services such as Data Execution Protection (DEP), Address Space Layout Randomization (ASLR), and User Account Control (UAC).

CFG-07 Ensure that the organization's approved operating system configuration benchmark defines its ability to disable autorun on its operating system.

CFG-08 Ensure that the organization's approved operating system configuration benchmark defines that the organization shall enable machine locks (screensavers) after a defined period of inactivity.

CFG-09 Ensure that the organization's approved operating system configuration benchmark defines the organization as requiring a secure boot process to verify the integrity of the operating system before loading (such as UEFI).

CFG-10 Ensure that the organization's approved operating system configuration benchmark defines that the organization shall disable unnecessary wireless protocols and networks on the organization's endpoints.

CFG-11 Maintain a library of approved software application configuration benchmarks that will be used to ensure that each of the organization's software applications is configured securely.

CFG-12 Maintain a configuration enforcement system to enforce the organization's approved operating system and application configurations on each of the organization's computing systems.

CFG-13 Ensure that the organization's configuration enforcement system enforces the organization's approved operating system and application configurations, regardless of the computing system's location (whether onsite or operating remotely).

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.