Cybersecurity
Policy Templates

CRF SANS

# Resilience Management Policy

*(Last Updated April 2025)*

## Purpose

Our Resilience Management Policy aims to establish a comprehensive framework for ensuring the availability, resilience, and timely recovery of our critical systems, data, and networks in the event of a cybersecurity incident or disruption. This policy aims to provide clear guidelines and procedures for developing, implementing, and testing business continuity plans that address cybersecurity risks and potential threats to our operations. By implementing effective business continuity practices, this policy seeks to minimize the impact of cyber incidents, maintain essential business functions, and protect the interests of our stakeholders. Through proactive risk assessment, incident response planning, and regular testing and evaluation, we strive to mitigate vulnerabilities, reduce downtime, and enable the swift restoration of normal operations in the face of cyber disruptions. By prioritizing business continuity, we ensure the continuity of our services, safeguard our reputation, and maintain the trust of our customers, partners, and employees.

## Scope

The Resilience Management Policy applies to all our organization's employees, contractors, and stakeholders. It encompasses the planning, implementing, and managing strategies to ensure the continuous operation and availability of critical systems, processes, and services during disruptive incidents or disasters. This policy covers the identification of potential risks and vulnerabilities, the development of business impact analyses, the formulation of continuity plans, and the establishment of incident response and recovery procedures. It outlines the roles, responsibilities, and communication protocols during business continuity events and sets guidelines for testing, training, and maintaining readiness. 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 business continuity and cybersecurity governance.

## Safeguards

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

RES-01 Maintain a documented Business Continuity and Disaster Recovery (BCP / DR) program that documents the organization's safeguards to address business continuity.

RES-02 Maintain a documented cybersecurity Incident Management (IM) program that documents the organization's safeguards to address cybersecurity incident management.

RES-03 Ensure that the organization's documented Incident Management (IM) plan defines workforce members' roles and responsibilities during a cybersecurity incident.

RES-04 Ensure that the organization's documented Incident Management (IM) plan defines the leadership and decision-making responsibilities workforce members have during a cybersecurity incident.

RES-05 Ensure that the organization's documented Incident Management (IM) plan defines a communications plan the organization should use during a cybersecurity incident.

RES-06 Ensure that the organization's documented Incident Management (IM) plan defines how incidents should be reported to the organization (including how to handle whistleblowing cases).

RES-07 Ensure that the organization's documented Incident Management (IM) plan defines how to report to external groups (such as partners, law enforcement, regulators, and others) during a cybersecurity incident.

RES-08 Ensure that the organization's documented Incident Management (IM) plan defines how to report a cybersecurity incident to those impacted by the incident.

RES-09 Ensure that the organization's documented Incident Management (IM) plan defines the roles and responsibilities of the technical incident response team or security operations center during a cybersecurity incident.

RES-10 Ensure the organization's documented Incident Management (IM) plan defines how and where to document cybersecurity incidents.

RES-11 Ensure that the organization's documented Incident Management (IM) plan defines categories or classifications levels of cybersecurity incidents and how to classify incidents at each level.

RES-12 Ensure that the organization's documented Incident Management (IM) plan defines the requirement that the organization perform root cause analysis of each cybersecurity incident.

RES-13 Define a process the organization shall use to ensure that the organization's documented Incident Management (IM) plan defines how the documentation will be regularly reviewed and updated.

RES-14 Define a process for regularly testing the organization's Incident Management (IM) plans.

RES-15 Regularly perform tabletop exercises with key stakeholders to test the organization's Business Continuity and Disaster Recovery (BCP / DR) and Incident Management (IM) plans.

RES-16 Define a process the organization shall use to report Incident Management (IM) statistics to the organization's business stakeholders.

RES-17 Maintain technical cybersecurity tools to help the organization detect and respond to cybersecurity incidents as described in the organization's Incident Management (IM) plans.

RES-18 Regularly test the organization's cybersecurity Incident Management (IM) tools to ensure they function as expected to help it detect and respond to cybersecurity incidents.

RES-19 Maintain a cybersecurity forensics and threat-hunting program to help the organization detect and respond to cybersecurity incidents.

RES-20 Maintain cybersecurity forensics tools to help the organization create forensics images of computing systems to detect and respond to cybersecurity incidents.

RES-21 Define a process the organization shall use to update its Business Continuity and Disaster Recovery (BCP / DR) and Incident Management (IM) documentation after changes to its information technologies.

RES-22 Maintain an enterprise backup architecture to regularly create backups of the organization's computing systems and data.

RES-23 Maintain a trusted system image for each class of computing endpoint to ensure that it can be quickly restored in the case of a cybersecurity incident.

RES-24 Maintain a trusted system image for each computing server to ensure that it can be quickly restored in the case of a cybersecurity incident.

RES-25 Maintain technical access controls on each of the organization's backups to ensure that only authorized users have access to them (including encrypting physical access controls).

RES-26 Maintain immutable backups for each of the organization's computing systems and data to ensure they cannot be accidentally deleted or by malicious individuals.

RES-27 Define a process the organization shall use to test the organization's backups regularly.

## 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.