

4.

SECURITY AND CONTINUITY OF OPERATIONS - Protect the enterprise through robust security and continuity programs

Manage Vulnerability

The goals of Vulnerability Management are:

- Test the reporting and tracking capabilities of Security Center
- Obtain and deploy a scanner for testing
- Prove the tools and architecture are sustainable and repeatable to implement in other agencies
- Develop and implement a Vulnerability Management Program that utilizes consistent assessment and reporting tools for the enterprise

The State of Wisconsin will continue to focus on maintaining a secure technology environment and culture. We will shape, design, evaluate, and drive opportunities related to enhancing IT security by raising awareness of security threats and vulnerabilities to the state.

4.1 EDUCATION, AWARENESS, AND TRAINING - *cultivate a security awareness culture within Wisconsin state agencies by providing continuous training and educational opportunities.*

OBJECTIVES

- Implement a monthly security training program using the STAR Enterprise Learning Management System.
- Hold cyber response team training and exercises for state and local government members of the Wisconsin cyber response teams, private-sector utilities, and the Wisconsin National Guard Computer Network Defense Team.
- Host an annual statewide Wisconsin Governor's Cyber Summit each October.
- Recognize and market October as cybersecurity awareness month to highlight IT security and privacy awareness, education, and training.

4.2 SECURITY - *promote an evolutionary change through the development of an effective vulnerability management program to mitigate risks and to ensure State of Wisconsin IT systems are configured appropriately and securely.*

OBJECTIVES

- Create a formal Vulnerability Management Program.
- Employ the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities, especially in software and firmware to mitigate the risk of compromise associated with known vulnerabilities.
- Implement specifically designed software tools that collect system configuration data and assist in the assessment of the information collected in order to identify where vulnerabilities exist and to remediate identified vulnerabilities.
- Engage in a Multifactor Strategy with authentication that combines two or more credentials to create a layered defense that makes it more difficult for an unauthorized person to access physical locations, computing devices, networks, or databases.
- Execute a Network Access Control (NAC) initiative to develop an enterprise level implementation strategy for network protection, which will identify and control who and what connects to the state network.

NAC is a method of enhancing security by restricting the availability of network resources to only those endpoint devices that comply with defined security policies. Depending on the security profile of a user's device, NAC can restrict the data and systems available to the user, as well as employ anti-threat applications such as firewalls, antivirus software and spyware-detection programs. NAC will identify and control who and what connects to the state network. There are many devices that connect to the state network every day.

4.3 WISCONSIN CYBER DISRUPTION RESPONSE PLAN - use the *Cyber Disruption Response Plan* as a guide for training, response and recovery of operations, and for addressing probable cyber disruptions in order to protect the state's cyber infrastructure, both public and private.

OBJECTIVES

- Identify the core capabilities necessary to address the threat environment and sustain the security and resilience of our state during a cyber event.
- Reduce the probability of failure through cyber hygiene, system monitoring, and information sharing.
- Diminish the consequences of failure through mitigation activities, access/identity controls, and training and exercises.
- Minimize the reaction and restoration times when failure occurs through cyber teams and resources.
- Form a governance structure to construct and refine this plan from Critical Infrastructure and Key Resources (CIKR) sectors.

The plan provides a description of roles and responsibilities, tasks, integration, and actions required to protect the state's cyber infrastructure, both public and private. The strategies promote our commitment to securing cyberspace and protecting the Wisconsin citizens who rely on Internet technologies in their daily activities. The governance authority, the Wisconsin Cyber Security Plan Working Group, serves as a forum of subject matter experts specifically charged with the responsibility to prepare for, respond to, and recover from cyber disruptions that could impact the state.

4.4 IT DISASTER RECOVERY (ITDR) - deploy a strategy to ensure the continuity and resilience of enterprise IT services.

OBJECTIVES

- Compile current state business impact analyses (BIA) to understand recovery point and time objectives for applications and services.
- Create a plan to address the gaps between BIA expectations and current IT recovering capabilities.
- Identify and engage plan owners and stakeholders in the development of ITDR application and infrastructure continuity plans, including dependency mapping.
- Utilize the state's continuity software program to document ITDR plans for all applications and infrastructure.