Division of Enterprise Technology

Security Guidelines for Local Government Access of State Systems

Effective Date: 01-03-2019

Background

Securing state information systems is critical. Wisconsin residents rely on the state, counties, and municipalities to deliver services reliably and safely. Cyber attacks are a continuous threat to the delivery of those services. The state needs your help to protect state systems and residents' information.

Cyber threats focus on the weakest link within systems, primarily the people using those systems. This document provides basic guidelines to reduce risks and ensure fundamental cybersecurity standards.

Basic Guidelines for Appropriate Access to and Use of State Systems

Authentication and Access Control

1. Prohibit employees from sharing passwords.
2. Passwords used to access state systems must meet or exceed the following minimum requirements:
    a. Must have at least eight (8) characters;
    b. Must not have user's name, organization, or user id in the password;
    c. Must contain three of these four data types: upper case alphabetic, lower case alphabetic, numeric, special character;
    d. Must not be constructed of a single word found in the dictionary – passphrases constructed of multiple words are acceptable as long as they meet the other criteria outlined in this section; and
    e. Users shall not be permitted to construct passwords that are identical or substantially similar to passwords that they had previously used.
    f. Require password changes at least every 60 days.
3. Enforce a limit of no more than four consecutive invalid access attempts by a user before they are locked out.
4. Consider 2 factor or 2 step login (something you know and something you have) for access to systems and data for those users with elevated privileges.
5. Maintain a formal, documented process for granting and revoking access to all state systems that process or store sensitive information.
6. Require segregation of duties and the principle of least privilege for employees (they can access only the information and resources necessary for their specific job responsibilities).
7. Immediately revoke access rights upon employee separation or if a change in job role eliminates the requirement for continued access.
8. Ensure all access rights are reviewed at least annually by appropriate supervisor(s). Consider conducting this review during annual employee performance evaluations.

Media Protection and Information Transfer

9. Provide direction to employees for securely handling, transporting, storing, and disposing of electronic media such as USB flash drives, CDs, and DVDs, as well as printed media such as paper copies of information printed from state systems.

10. Comply with all applicable laws pertaining to the retention and disposition of public records, including sections 19.21-19.39, Wis. Stats., and chapter Adm 12, Wis. Admin. Code.
11. Only use encrypted communications to transfer controlled or sensitive information – for example, SSL (Secure Sockets Layer).
12. Restrict staff from forwarding sensitive information to personal email or social media.

System Security and Vulnerability Management

13. Replace unsupported hardware and software on a timely basis.
14. Ensure all networked devices have up-to-date:
    a. Patches / Firmware (no later than 30 days of release by vendor)
    b. Antivirus software
    c. Spam and spyware protections
    d. Web filtering software to protect against malicious websites
15. Ensure employees lock desktops when they walk away.
16. Implement password-protected screensavers to activate after no longer than 15 minutes of non-use.
17. Employ appropriate physical safeguards and visitor access controls to prevent unauthorized access to all areas and systems used to process or store state data.
18. Consider cyber liability insurance; some insurance includes some compliance services with the insurance.
19. Retention of backups offsite is strongly recommended.
20. Retention of login records is strongly recommended.
21. Immediately notify all appropriate parties in the event of inappropriate/unauthorized disclosure/use of information is suspected or confirmed. Contact the State Chief Information Security Officer: Bill Nash, (608) 224-3779, Bill.Nash@wisconsin.gov for events involving state systems/data.

Awareness and Training

22. Conduct annual cybersecurity awareness training for employees and contract staff.

# # #