Building and Managing Staff

Cybersecurity is more than technology and processes. People are at the heart of any cybersecurity program. This means hiring people you can trust with the sensitive tasks they have to complete and giving them the tools they need to be successful.

Background checks, including criminal and financial checks, are essential for a healthy hiring process. In addition, carefully manage staff access, both physical and electronic, and provide them the training they need so they can make good cybersecurity decisions.

Goals

1. Conduct background checks for new hires (Level 1 maturity)
2. Use available cybersecurity training to improve your cybersecurity posture (Level 1 maturity)

Actions

For Building and Managing Staff, the necessary actions are the same for all maturity levels.

1. Conduct at least a national agency check for any hires. Your state or county may have other background check options for you.
2. Provide security awareness training for all staff.
3. Track training either through a human resources portal or manually through a worksheet. You can use the Level 1 maturity Cyber Education worksheet as a template.
4. Implement actions for proper logical access in User Management
5. Implement actions for proper system configuration in Managing Infrastructure

Learn More

- MS-ISAC® Cybersecurity Awareness Toolkit features educational materials designed to raise cybersecurity awareness. Digital materials are aggregated for your use.
- Federal Virtual Training Environment (FedVTE): Online Courses Free online cybersecurity training to State, Local, Tribal, and Territorial (SLTT) governments.
- Learn how to protect yourself, your family and your devices with tips and resources from the National Cybersecurity Alliance's Stay Safe Online initiative. See also its YouTube channel.

Mapping to CIS Controls and Safeguards

- 14.1: Establish and Maintain a Security Awareness Program (Level 1 maturity)
- 14.2: Train Workforce Members to Recognize Social Engineering Attacks (Level 1 maturity)
- 14.3: Train Workforce Members on Authentication Best Practices (Level 1 maturity)
- 14.4: Train Workforce on Data Handling Best Practices (Level 1 maturity)
- 14.5: Train Workforce Members on Causes of Unintentional Data Exposure (Level 1 maturity)
- 14.6: Train Workforce Members on Recognizing and Reporting Security Incidents (Level 1 maturity)
- 14.7: Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates (Level 1 maturity)
- 14.8: Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks (Level 1 maturity)
- 14.9: Conduct Role-Specific Security Awareness and Skills Training (Level 2 maturity)

Mapping to CIS Handbook Best Practices

- 13, 16, 54, 57, 58, 59, 82, 87