Kiteworks

BEST PRACTICES

CMMC Media Protection Best Practices Checklist

Protecting physical and electronic media that stores CUI and FCI involves a strategic approach that combines technology, policy, and awareness. Consider the following best practices when developing a media protection program that adheres to the CMMC 2.0 media protection requirement.

- **1. Conduct Regular Employee Training for Proper Media Protection:** Regular training sessions addressing media protection—and the sensitive information stored on that media—keep employees updated on the latest threats and prevention techniques, fostering a culture of security awareness and vigilance. By understanding these evolving threats, employees are better equipped to identify and respond to suspicious activities.

- **2. Implement Strict Access Controls to Limit Media Access:** Implement stringent access controls to ensure that only authorized personnel have the ability to handle and interact with confidential data, whether it is stored in physical formats or in electronic mediums. For physical media, use secure storage solutions liked locked cabinets and restricted areas where only those with the appropriate clearance can enter. For electronic media protection, focus on digital security like passwords, biometrics, and multi-factor authentication (MFA).

- **3. Use Encryption Tools to Protect Physical and Electronic Media:** Encryption for data in transit and at rest ensures sensitive data remains confidential and secure from unauthorized access. Convert data into a secure, unreadable format without that requires the appropriate decryption key.

- **4. Establish a Comprehensive Media Protection Policy:** A media protection policy should contain clear guidelines on the proper handling of sensitive media. Naturally, the policy should be communicated to employees. The policy should contain secure storage, transport, usage, and disposal protocols that help maintain data integrity and confidentiality.

- **5. Regularly Audit and Monitor Media Use and Storage Practices:** Systematically review and assess the protocols and technologies your organization employs to manage your digital and physical media so you can pinpoint any weaknesses or vulnerabilities in your existing systems that might be exploited by malicious actors. Audits often include evaluating the effectiveness of encryption methods, access controls, and data handling procedures. Monitoring practices keep track of how data is moving within the organization and who has access to it. This continuous oversight allows organizations to detect unauthorized access or data leakage promptly.

CMMC Media Protection Best Practices Checklist

- [ ] **1. Conduct Regular Employee Training for Proper Media Protection:** Regular training sessions addressing media protection—and the sensitive information stored on that media—keep employees updated on the latest threats and prevention techniques, fostering a culture of security awareness and vigilance. By understanding these evolving threats, employees are better equipped to identify and respond to suspicious activities.

- [ ] **2. Implement Strict Access Controls to Limit Media Access:** Implement stringent access controls to ensure that only authorized personnel have the ability to handle and interact with confidential data, whether it is stored in physical formats or in electronic mediums. For physical media, use secure storage solutions liked locked cabinets and restricted areas where only those with the appropriate clearance can enter. For electronic media protection, focus on digital security like passwords, biometrics, and multi-factor authentication (MFA).

- [ ] **3. Use Encryption Tools to Protect Physical and Electronic Media:** Encryption for data in transit and at rest ensures sensitive data remains confidential and secure from unauthorized access. Convert data into a secure, unreadable format without that requires the appropriate decryption key.

- [ ] **4. Establish a Comprehensive Media Protection Policy:** A media protection policy should contain clear guidelines on the proper handling of sensitive media. Naturally, the policy should be communicated to employees. The policy should contain secure storage, transport, usage, and disposal protocols that help maintain data integrity and confidentiality.

- [ ] **5. Regularly Audit and Monitor Media Use and Storage Practices:** Systematically review and assess the protocols and technologies your organization employs to manage your digital and physical media so you can pinpoint any weaknesses or vulnerabilities in your existing systems that might be exploited by malicious actors. Audits often include evaluating the effectiveness of encryption methods, access controls, and data handling procedures. Monitoring practices keep track of how data is moving within the organization and who has access to it. This continuous oversight allows organizations to detect unauthorized access or data leakage promptly.