Kiteworks

Best Practices for Meeting the CMMC Access Control Requirement

Access controls are critical for protecting sensitive content. For the CMMC 2.0 Access Control requirement, defense contractors should strongly consider these best practices:

☑ **1. Implement Role-Based Access Control (RBAC):** Organize roles within your company according to specific job responsibilities and allocate access permissions based on these roles. Known as Role-Based Access Control (RBAC), this approach significantly reduces the risk of unauthorized data access. By implementing RBAC, you ensure that employees are granted only the permissions essential for their job functions, thereby enhancing security and maintaining tight control over sensitive information.

☑ **2. Enforce Multi-Factor Authentication:** Protect systems and applications – especially those containing sensitive information like intellectual property (IP) and personally identifiable and protected health information (PII/PHI) – with multi-factor authentication (MFA). MFA requires employees to enter more than one method of identity verification before allowing access to systems or data. Typically, MFA combines something the employee knows, like a password or PIN, with something the user has, such as a smartphone with an authentication app, or something the user is, like a fingerprint or facial recognition. This layered approach creates additional, significant hurdles for potential attackers.

☑ **3. Conduct Regular Access Reviews:** Continuously monitor and revise access permissions to protect sensitive data. This process involves routinely checking who has access to specific information and ensuring that only those who are currently authorized can view or modify it. It's essential, for example, to revoke a consultant or other third-party's access to sensitive content when they are no longer engaged in a client project. It applies to employees, too. Permissions should be revoked when employees no longer require access to content, e.g., when they have transitioned to different roles within the organization or have left the company.

☑ **4. Implement Audit Logs and Monitoring:** Maintain detailed audit logs of all access activities, recording every instance where users or systems access resources within an environment. These logs should include information like user ID, timestamp, type of access (e.g., login, file access, changes made), source IP address, and any other relevant parameters that can help in identifying who did what and when. These comprehensive logs serve as historical records that can be reviewed and analyzed to understand access patterns and behaviors, as well as identifying anomalies, such as repeated failed login attempts, access from unfamiliar IP addresses, or unusual times of access that deviate from normal patterns.

Best Practices for Meeting the CMMC Access Control Requirement

☑ **5. Train Employees on Access Control Policies:** Implement a comprehensive security awareness training program that continually educates employees about the importance of access controls. Regular training sessions should focus on different types of access controls, such as physical, administrative, and technical controls, and understand how to apply them in their daily work. Employees should also be informed about the latest threats and how to recognize and respond to potential security breaches.