imprivata

CJIS compliance checklist

CJIS compliance is critical

The CJIS Security Policy contains specific IT requirements. We've provided a checklist of rules from the CJIS compliance guidelines focusing on remote access, audit trails, and password requirements.

CJIS third-party remote access recommendations

- Implement a software access solution featuring a "credential vault" or other form of password management.
- Maintain a detailed audit log. The audit should record the who, what, when, and why of remote access.
- Require multifactor authentication (MFA) for all remote access.
- Discontinue using solutions like VPN, Remote Desktop, or WebEX as a method of remote access.

About Imprivata

Imprivata delivers simple and secure access management solutions for mission-critical industries to ensure every second of crucial work is both frictionless and secure. Imprivata's platform of innovative, interoperable access management and privileged access security solutions enable organizations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership.

AUDITING AND USER ACCOUNTABILITY

- ☐ Allow administrators to easily view who has access to passwords, and track when and how those credentials are accessed or used.
- ☐ Generate detailed audit reports based on user access, permissions, and passwords.

ACCESS CONTROLS

- ☐ Allow password restriction based on a user's role (job duties or administrative levels).
- ☐ Establish a centralized password management system so that a user's access and permissions can be easily changed or restricted should they leave their role.
- ☐ Lock access based on failed login attempts, and automatically notify administrators of such an event.
- ☐ Require authentication after a set period of inactivity.

IDENTIFICATION AND AUTHENTICATION

- ☐ Allow administrators to create a password policy that meets CJIS complexity requirements (at least eight characters long, expire within 90 days, etc.).
- ☐ Formalize an audit plan for compliance/HR regarding response to high risk events found
- ☐ Assign team members to specific tasks to meet report requirements