PORTALGUARD

CJIS Compliance Guidelines: How PortalGuard Can Help

v.3.2-001

PistolStar, Inc. dba PortalGuard
PO Box 1226
Amherst, NH 03031 USA

Phone: 603.547.1200
E-mail: sales@portalguard.com
Website: www.portalguard.com

PortalGuard and Criminal Justice Information System (CJIS) Security Policy Compliance

Those in law enforcement know that the CJIS Policy Guidelines offer a complete and comprehensive guideline on how all Criminal Justice systems need to be structured, audited, and compliant.

Chief among these regulations are requirements that deal specifically with user ID's, remote system access, password compliance, two-factor authorization, auditing and reporting. The matrix below is designed to help you understand which Policy Areas PortalGuard can help you satisfy quickly and efficiently.

If you have further questions on CJIS compliance we invite you to give us a call at 603.547.1200 or visit PortalGuard.com.

Policy Area	Name	PortalGuard Feature
4	Auditing & Accountability	✓
5	Access Control	✓
6	Identification & Authentication	✓

Policy Area 4 - Auditing & Accountability

Control No.	Control Description	PortalGuard Feature
5.4.1 Auditable Events	The following events shall be logged: Successful and unsuccessful system log-on attempts and password changes.	PortalGuard offers a full complement of reporting tools that show when, where, the time, and number of logons by user or user group. The system also maintains a record of failed login attempts as well as password changes.
5.4.4 Time Stamps	The agency's information system shall provide time stamps for use in audit record retention.	PortalGuard offers both real time reporting via a web dashboard interface as well as a daily report that can be archived for record keeping purposes.

Policy Area 5 - Access Control

Control No.	Control Description	PortalGuard Feature
5.5.1 Account Management	The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.	PortalGuard is completely customizable either by unique user ID or User group. The platform allows complete control of system access based on predetermined user needs and profiles setup by the System Administrator.
5.5.2 Access Enforcement	The information system shall enforce assigned authorizations for controlling access to the system and contained information.	PortalGuard provides complete control of user access based on "least privilege" restrictions. System Administrators have complete control over system logins from public vs. secured Wi-Fi, geographic location, network address and time of day.
5.5.3 Unsuccessful Login Attempts	When technically erasable, the system shall enforce a limit of no more than 5 consecutive attempts by a user.	System Administrators have the ability to set the "strike" limit on logins and password reset criteria as well as monitoring the time of day and location.
5.5.5 Session Lock	The information system shall prevent further access to the system by initiating a session lock after 30 minutes of inactivity.	PortalGuard is configurable to a specific time limit by user, user group, or location.

Continued >>>

Policy Area 5 - Access Control

Control No.	Control Description	PortalGuard Feature
5.5.6 Remote Access	The agency shall authorize, monitor, and control all methods of remote access to the information system. The agency shall control all remote accesses through managed access control points.	As noted in the other section of Policy Area 5, PortalGuard offers System Administrators the tools they need to tightly control who logs in, from where, and the time of day.
5.5.7 Wireless Restriction	The agency shall: (i) establish usage restrictions and implementation guidance for wireless technologies; and (ii) authorize, monitor, and control wireless access to the information system.	PortalGuard can be configured to restrict access based on the location, IP address, or method of wireless access (secure v. non-secured).

Policy Area 6 - Identification & Authentication

Control No.	Control Description	PortalGuard Feature
5.6.2.1 Standard Authentication (Password)	The password must be a minimum length of eight (8) characters, not a dictionary word, not the same as the UserID, expire in 90 days, not identical to the last ten (10) passwords, and not displayed when entered.	PortalGuard offers all of these controls along with the ability to provide a password strength meter. System Administrators can set length, strength, and expiration dates quickly and efficiently.
5.6.2.2.2 Advanced Authentication Decision Tree	See Page 149 for complete details on this control.	For sake of brevity in this matrix, PortalGuard can provide the necessary tools to meet this control. Call with any specific questions you may have.

###