GATEKEEPER

240-547-5446
info@gkaccess.com
gkaccess.com

# CJIS Compliance Chart - GateKeeper Enterprise

| Section | Key Activity | Performance Criteria | GateKeeper Solution |
|---|---|---|---|
| **5.5.5** | **Account Management** | Account Management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group memberships, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges.<br>The agency responsible for account creation shall be notified when:<br>1. A user's information, system usage or need-to-know or need-to-share changes.<br>2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured. | GateKeeper Hub allows you to tie individual accounts to users and group accounts to computers to distinguish between them. Accounts with different privileges can be allowed/restricted access to different computers. The logs maintained in the GateKeeper Hub application record all changes made to a user's account and permission roles. |
| **5.6.1** | **Access Enforcement** | The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. Explicitly Authorized Personnel include, for example, security administrators, system and network administrators, and other privileged usurers with access to system control, monitoring, or administration functions.<br>Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and | Administrator can create access control policies on GateKeeper Hub to only allow authorized personnel to access computers with sensitive information using their GateKeeper token. Adding/updating/deleting these policies can only be done by users with administrative privileges to the GateKeeper Hub application. |

| | | | |
|---|---|---|---|
| | | associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users in the information system. | |
| **5.6.2.1.2** | **Session Lock** | The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. | GateKeeper desktop application triggers lock/unlock events on the computer based on the user's proximity. As soon as the user walks away, the computer locks to prevent inadvertent data exposure. |
| **5.6.2.2.1** | **Identification Policy and Procedures** | Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling add/or deleting former users. | Each GateKeeper token assigned to a user is uniquely identified by a serial number. Each user on the network needs to have a user account associated with their full name and token serial number. Even in a shared credentials environment, users can be uniquely identified along with the session count and time on each computer. |
| **5.5.5** | **Personal Identification Number (PIN)** | When agencies utilize a PIN in conjunction with a token for the purpose of advanced | GateKeeper Hub allows administrators to set PIN complexity settings adhering to CJIS |

| | | | |
|---|---|---|---|
| | | authentication, agencies shall follow the PIN attributes described below.<br>1. Be a minimum of six (6) digits.<br>2. Have no repeating digits (i.e. 112233).<br>3. Have no sequential patterns (i.e. 123456).<br>4. Not be the same as Userid.<br>5. Expire within a maximum of 365 calendar days.<br>6. Not be identical to the previous three (3) PINs.<br>7. Not be transmitted in the clear outside the secure location.<br>8. Not be displayed when entered. | requirements for all workstations on the network. |
| **5.6.1** | **Advanced Authentication Requirement** | Organizations must use multi-factor authentication if employees are accessing CJI. This is alike to using a debit or credit card that requires PIN input. | GateKeeper allows administrators to enforce two-factor login (2FA) policies on each computer on the network - restricting the use of Windows credentials for logging in. |