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

NIST 800-171 and 800-53 Compliance Chart - GateKeeper

Control Family	Control Details	800-171 Control Number	800-53 Control Number	Implementation
Access Control	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	3.1.1	AC-3	GateKeeper Enterprise provides proximity-based authentication and authorization to workstations. Using GateKeeper Enterprise, an organization can assign granular access permissions to individuals/groups on a per workstation basis. GateKeeper automatically locks a user's computer when they are no longer in proximity to their workstation immediately protecting unauthorized users from accessing a system.
Access Control	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	3.1.2	AC-3	GateKeeper Enterprise provides proximity-based authentication and authorization to workstations. Using GateKeeper Enterprise, an organization can assign granular access permissions to individuals/groups on a per workstation basis. GateKeeper automatically locks a user's computer when they are no longer in proximity to their workstation immediately protecting unauthorized users from accessing a system.

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

Access Control	Employ the principle of least privilege, including for specific security functions and privileged accounts.	3.1.5	AC-6	GateKeeper Enterprise provides proximity-based authentication and authorization to workstations. Using GateKeeper Enterprise, an organization can assign granular access permissions to individuals/groups on a per workstation basis. This helps enforce the concept of least privilege on a system level.
Access Control	Limit unsuccessful logon attempts.	3.1.8	AC-7	GateKeeper has the ability to lock a user's account after an administrator-defined number of unsuccessful login attempts.
Access Control	Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	3.1.10	AC-11	GateKeeper automatically locks a user's workstation when they are no longer in proximity to their workstation - preventing access/viewing of data.
Audit and Accountability	Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	3.3.1	AU-3	GateKeeper Enterprise provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it. These audit logs are retained indefinitely.
Audit and Accountability	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	3.3.2	AU-3	GateKeeper Enterprise provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it.

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

Audit and Accountability	Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	3.3.5	AU-3	GateKeeper Enterprise provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it. GateKeeper can connect to a syslog server and integrate with an enterprise security architecture. Authorized admins have the ability to export audit logs to further enable audit review, analysis, and reporting processes.
Audit and Accountability	Provide audit reduction and report generation to support on-demand analysis and reporting.	3.3.6	AU-7	GateKeeper Enterprise provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it. GateKeeper can connect to a syslog server and integrate with an enterprise security architecture. Authorized admins have the ability to export audit logs to further enable audit review, analysis, and reporting processes.
Audit and Accountability	Protect audit information and audit tools from unauthorized access, modification, and deletion.	3.3.8	AU-9	GateKeeper Enterprise provides proximity-based authentication and authorization to workstations and thus can protect audit information and audit tools from unauthorized access.
Audit and Accountability	Limit management of audit functionality to a subset of privileged users.	3.3.9	AU-9	GateKeeper Enterprise provides proximity-based authentication and authorization to workstations and thus can protect audit functionality to a subset of users.
Identification and Authentication	Identify information system users, processes acting on behalf of users, or devices.	3.5.1	IA-4	GateKeeper Enterprise provides proximity-based identification, authentication and authorization to workstations. Using GateKeeper an organization can identify a user at a workstation.

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

Identification and Authentication	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	3.5.2	IA-4	GateKeeper Enterprise provides proximity-based identification, authentication and authorization to workstations. Using GateKeeper Enterprise an organization can assign granular access permissions to individuals/groups on a per workstation basis.
Identification and Authentication	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	3.5.3	IA-5	GateKeeper Enterprise has the capability to enforce multifactor authentication for all access to a workstation.
Identification and Authentication	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	3.5.4	IA-2	GateKeeper is a proximity-based identification and authentication solution. A user must be present to unlock their workstation making it inherently replay-resistant.
Identification and Authentication	Prevent reuse of identifiers for a defined period.	3.5.5	IA-4	GateKeeper can integrate with an organization's Active Directory to enforce this control.
Identification and Authentication	Disable identifiers after a defined period of inactivity.	3.5.6	IA-4	GateKeeper can integrate with an organization's Active Directory to enforce this control.
Identification and Authentication	Enforce a minimum password complexity and change of characters when new passwords are created.	3.5.7	IA-5	GateKeeper can integrate with an organization's Active Directory to enforce this control.
Identification and Authentication	Prohibit password reuse for a specified number of generations.	3.5.8	IA-5	GateKeeper can integrate with an organization's Active Directory to enforce this control.

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

Identification and Authentication	Allow temporary password use for system logons with an immediate change to a permanent password.	3.5.9	IA-5	GateKeeper can integrate with an organization's Active Directory to enforce this control.
Identification and Authentication	Store and transmit only encrypted representation of passwords.	3.5.10	IA-5	GateKeeper uses AES-256 encryption to store and transmit passwords.
Identification and Authentication	Obscure feedback of authentication information.	3.5.11	IA-6	GateKeeper PIN login is obscured and all authentication information is obscured.
Physical Protection	Maintain audit logs of physical access.	3.10.4	PE-3	GateKeeper is a proximity-based identification and authentication solution using a physical dongle. A user must be physically present to access a workstation. Audit logs of physical access using GateKeeper are stored indefinitely on the GateKeeper Enterprise server.
Physical Protection	Control and manage physical access devices.	3.10.5	PE-3	GateKeeper is a proximity-based identification and authentication solution using a physical dongle. A user must be physically present to access a workstation. Audit logs of physical access using GateKeeper are stored indefinitely on the GateKeeper Enterprise server.