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

GateKeeper Enterprise IS0 27001 Compliance Chart

A.10.10	**Monitoring**	**Objective: To detect unauthorized information processing activities.**	**GateKeeper**
A.10.10.1	Audit Logging	Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.	GateKeeper Enterprise provides robust Auditing Capabilities that identifies when an individual user (both non-administrators and administrators) was in proximity to a workstation and successfully locked/unlocked it. These audit logs are retained indefinitely. 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. Using the web credential manager, GateKeeper can also log the use of web credentials.
A.10.10.3	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	GateKeeper Enterprise stores all audit records in an encrypted database that is only accessible by an authorized GateKeeper administrator.
A.10.10.4	Administrator and operator logs	System administrator and system operator activities shall be logged.	GateKeeper Enterprise provides robust auditing capabilities that identifies when an individual user (both non-administrators and administrators) was in proximity to a workstation and successfully locked/unlocked it. These audit logs are retained indefinitely. 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. Using the Web credential manager, GateKeeper can also log the use of web credentials.

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

A.11.2	**User access management**	**Objective: To ensure authorized user access and to prevent unauthorized access to information systems.**	
A.11.2.1	User Registration	There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	GateKeeper employs a secure registration process which associates a token with a user account. Users and administrators have the ability to deregister their tokens.
A.11.2.2	Privilege management	The allocation and use of privileges shall be restricted and controlled.	GateKeeper Enterprise provides proximity-based authentication and authorization to workstations. Using GK Enterprise an organization can granularly assign access permissions to individuals/groups on a per workstation basis. This helps enforce the concept of least privilege on a system level.
A.11.2.3	User password management	The allocation of passwords shall be controlled through a formal management process.	GateKeeper Enterprise allows users to use very complex passwords that are associated with their system level accounts and then associated with their token for simple authentication. Users can also use the GateKeeper web credential manager to securely store their web credentials. An organization can effectively allocate passwords through the use of GateKeeper Enterprise.
A.11.3	**User responsibilities**		
A.11.3.1	Password use	Users shall be required to follow good security practices in the selection and use of passwords.	GateKeeper Enterprise allows users to use very complex passwords that are associated with their system level accounts and then associated with their token for simple authentication. Users can also use the GateKeeper web credential manager to securely store their web credentials. An organization can effectively allocate passwords through the use of GateKeeper Enterprise.

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

A.11.3.2	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	GateKeeper Enterprise provides proximity-based authentication and authorization to workstations. When a user is no longer in proximity to their workstation it is automatically locked. This goes beyond relying on a user to manually lock their computers or relying on system level lock screen timeouts.
A.11.5	**Operating system access control**	**Objective: To prevent unauthorized access to operating systems.**	
A.11.5.1	Secure log-on procedures	Access to operating systems shall be controlled by a secure log-on procedure.	GateKeeper Enterprise provides proximity-based authentication and authorization to workstations. When a user is in proximity to a workstation GateKeeper securely logs the user onto the system.
A.11.5.2	User identification and authentication	All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.	GateKeeper Enterprise assigns users a unique token that is associated with their system level account. The GateKeeper token is a unique user identifier and substantiates the claimed identity of the user.
A.11.5.3	Password management system	Systems for managing passwords shall be interactive and shall ensure quality passwords.	GateKeeper manages system level accounts by associating a token with the user credentials. By associating a token with the user account, it allows the user to use random complex passwords for system level authentication. The GateKeeper web credential manager allows the same level of authentication and security for web credentials.
A.11.5.5	Session time-out	Inactive sessions shall shut down after a defined period of inactivity.	GateKeeper Enterprise provides proximity-based authentication and authorization to workstations. When a user is no longer in proximity to their workstation it is automatically locked. This goes beyond relying on a user to manually lock their computers or relying on system level lock screen timeouts.

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

A.10.10	**Monitoring**	**Objective: To detect unauthorized information processing activities.**	
A.10.10.1	Audit Logging	Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.	GateKeeper Enterprise provides robust Auditing Capabilities that identifies when an individual user (both non-administrators and administrators) was in proximity to a workstation and successfully locked/unlocked it. These audit logs are retained indefinitely. 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. Using the web credential manager, GateKeeper can also log the use of web credentials.
A.10.10.3	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	GateKeeper Enterprise stores all audit records in an encrypted database that is only accessible by an authorized GateKeeper administrator.
A.10.10.4	Administrator and operator logs	System administrator and system operator activities shall be logged.	GateKeeper Enterprise provides robust auditing capabilities that identifies when an individual user (both non-administrators and administrators) was in proximity to a workstation and successfully locked/unlocked it. These audit logs are retained indefinitely. 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. Using the Web credential manager, GateKeeper can also log the use of web credentials.