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

PCI DSS Compliance Chart – GateKeeper Enterprise

PCI DSS Requirements	Testing Procedures	Guidance	GateKeeper Implementation
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters. Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.			
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network	2.1.a Choose a sample of system components, and attempt to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords, to verify that ALL default passwords (including those on operating systems, software that provides security services, application and system accounts, POS terminals, and Simple Network Management Protocol (SNMP) community strings) have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.) 2.1.b For the sample of system components, verify that all unnecessary default accounts (including accounts used by operating systems, security	Malicious individuals (external and internal to an organization) often use vendor default settings, account names, and passwords to compromise operating system software, applications, and the systems on which they are installed. Because these default settings are often published and are well known in hacker communities, changing these settings will leave systems less vulnerable to attack. Even if a default account is not intended to be used, changing the default password to a strong unique password and then disabling the account will prevent a malicious individual from re-enabling the account and gaining access with the default password.	Use of GateKeeper Enterprise enables an organization to manage strong credentials across all Windows, Web, and local applications. A user only has to remember a single, strong password. All default passwords can be changed by an organization and stored in the GateKeeper Enterprise password manager.

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

Management Protocol (SNMP) community strings, etc.).	software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled. 2.1.c Interview personnel and examine supporting documentation to verify that: • All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are changed before a system is installed on the network. • Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled before a system is installed on the network.		
Requirement 6: Develop and maintain secure systems and applications. Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.			
6.3.1 Remove development, test and/or custom application accounts, user IDs, and	6.3.1 Examine written software-development procedures and interview responsible personnel to verify that pre-production and/or custom application accounts, user IDs and/or	Development, test and/or custom application accounts, user IDs, and passwords should be removed from production code before the application becomes active or is released to customers, since	Use of GateKeeper Enterprise enables an organization to manage strong credentials across all Windows, web, and local applications. A user only has to remember a single, strong password. All custom application accounts can

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

passwords before applications become active or are released to customers.	passwords are removed before an application goes into production or is released to customers.	these items may give away information about the functioning of the application. Possession of such information could facilitate compromise of the application and related cardholder data.	be stored in the GateKeeper Enterprise Password Vault.
Implement Strong Access Control Measures Requirement 7: Restrict access to cardholder data by business need to know. To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. “Need to know” is when access rights are granted to only the least amount of data/privileges needed to perform a job.			
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	7.1 Examine written policy for access control, and verify that the policy incorporates 7.1.1 through 7.1.4 as follows: • Defining access needs and privilege assignments for each role • Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities • Assignment of access based on individual personnel’s job classification and function • Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved.	The more people who have access to cardholder data, the more risk there is that a user’s account will be used maliciously. Limiting access to those with a legitimate business reason for the access helps an organization prevent mishandling of cardholder data through inexperience or malice.	GateKeeper Enterprise allows an organization to simplify and improve an organization's access control. GateKeeper enforces access authorizations on a per individual and workstation level and enables granularly defined access controls on a per workstation basis. Within the enterprise console, an administrator has the ability to granularly enforce access controls by creating groups/roles based on an individual's job classification and function. Individuals are then assigned to groups/roles and authorized access to workstations based on their group/role membership. Access authorizations can be enforced at an individual and per workstation level as well. This enforces the concept of least privilege by granting accesses to workstations only to those with a required business need.
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	7.1.2.a Interview personnel responsible for assigning access to verify that access to privileged user IDs is: • Assigned only to roles that specifically require such privileged access • Restricted to least privileges necessary to perform job responsibilities.	When assigning privileged IDs, it is important to assign individuals only the privileges they need to perform their job (the “least privileges”). For example, the database administrator or backup administrator should not be assigned the same privileges as the overall systems administrator.	GateKeeper Enterprise allows an organization to simplify and improve an organization's access control and enable granularly defined access controls on a per workstation basis. Within the enterprise console, an administrator can create groups/roles based on an individual's job classification and function. Individuals are then assigned to groups/roles and authorized access

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

	7.1.2.b Select a sample of user IDs with privileged access and interview responsible management personnel to verify that privileges assigned are: • Necessary for that individual's job function • Restricted to least privileges necessary to perform job responsibilities.		to workstations based on their group/role membership. Access authorizations can be enforced at an individual and per workstation level as well. This enforces the concept of least privilege by granting accesses to workstations only to those with a required business need.
7.1.3 Assign access based on individual personnel's job classification and function.	7.1.3 Select a sample of user IDs and interview responsible management personnel to verify that privileges assigned are based on that individual's job classification and function.	Once needs are defined for user roles (per PCI DSS requirement 7.1.1), it is easy to grant individuals access according to their job classification and function by using the already-created roles.	GateKeeper Enterprise allows an organization to simplify and improve an organization's access control and enable granularly defined access controls on a per workstation basis. Within the enterprise console, an administrator has the ability to create groups/roles based on an individual's job classification and function. Individuals are then assigned to groups/roles and authorized access to workstations based on their group/role membership. Access authorizations can be enforced at an individual and per workstation level as well. This enforces the concept of least privilege by granting accesses to workstations only to those with a required business need.
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	7.2 Examine system settings and vendor documentation to verify that an access control system(s) is implemented as follows:	Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. Access control systems automate the process of restricting access and assigning privileges. Additionally, a default "deny-all" setting ensures no one is granted access until and unless a rule is established specifically granting such	GateKeeper Enterprise allows an organization to enable access control systems to prevent unauthorized users from gaining access to data and systems they are not privy to see. GateKeeper Enterprise uses centralized access systems to ensure that system administrators can ensure that only authorized users within certain roles can access systems which contain cardholder data.

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

This access control system(s) must include the following:		access. Entities may have one or more access controls systems to manage user access.	
7.2.1 Coverage of all system components	7.2.1 Confirm that access control systems are in place on all system components.	Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. Access control systems automate the process of restricting access and assigning privileges. Additionally, a default "deny-all" setting ensures no one is granted access until and unless a rule is established specifically granting such access. Entities may have one or more access controls systems to manage user access.	GateKeeper Enterprise allows an organization to enable access control systems to prevent unauthorized users from gaining access to data and systems they are not privy to see. GateKeeper Enterprise uses centralized access systems to ensure that system administrators can ensure that only authorized users within certain roles can access systems which contain cardholder data.
7.2.2 Assignment of privileges to individuals based on job classification and function.	7.2.2 Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.	Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. Access control systems automate the process of restricting access and assigning privileges. Additionally, a default "deny-all" setting ensures no one is granted access until and unless a rule is established specifically granting such access. Entities may have one or more access controls systems to manage user access.	GateKeeper Enterprise allows an organization to enable access control systems to prevent unauthorized users from gaining access to data and systems they are not privy to see. GateKeeper Enterprise uses centralized access systems to ensure that System Administrators can ensure that only authorized users within certain roles can access systems which contain cardholder data.
7.2.3 Default "deny-all" setting.	7.2.3 Confirm that the access control systems have a default "deny-all" setting.	Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data.	GateKeeper Enterprise allows an organization to enable secure access control management systems to prevent unauthorized users from gaining access to data and systems

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

		Access control systems automate the process of restricting access and assigning privileges. Additionally, a default "deny-all" setting ensures no one is granted access until and unless a rule is established specifically granting such access. Entities may have one or more access controls systems to manage user access.	they are not privy to see. GateKeeper Enterprise uses centralized access control systems to ensure that system administrators can ensure that only authorized users within certain roles can access systems which contain cardholder data.
Requirement 8: Identify and authenticate access to system components Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes. The effectiveness of a password is largely determined by the design and implementation of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage.			
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	8.1.a Review procedures and confirm they define processes for each of the items below at 8.1.1 through 8.1.8 8.1.b Verify that procedures are implemented for user identification management, by performing the following:	By ensuring each user is uniquely identified—instead of using one ID for several employees—an organization can maintain individual responsibility for actions and an effective audit trail per employee. This will help speed issue resolution and containment when misuse or malicious intent occurs	GateKeeper Enterprise allows for the creation of unique user accounts which are tied to unique domain names created by the organization (such as user accounts created in Active Directory). Within the GateKeeper Enterprise Hub console, administrators can review the actions of individual users within the organization to identify unusual lock/unlock activity or other indicators of suspect user activity. Additionally, GateKeeper Enterprise allows for detailed logging for access logs.
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	8.1.1 Interview administrative personnel to confirm that all users are assigned a unique ID for access to system components or cardholder data.	By ensuring each user is uniquely identified—instead of using one ID for several employees—an organization can maintain individual responsibility for actions and an effective audit trail per employee. This will help speed issue resolution and containment when misuse or malicious intent occurs	GateKeeper Enterprise allows for the creation of unique user accounts which are tied to unique domain names created by the organization (such as user accounts created in Active Directory). Within the GateKeeper Enterprise console, administrators can review the actions of individual users within the organization to identify unusual lock/unlock activity or other

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

			indicators of suspect user activity. Additionally, GateKeeper Enterprise allows for detailed logging for access logs.
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	8.1.2 For a sample of privileged user IDs and general user IDs, examine associated authorizations and observe system settings to verify each user ID and privileged user ID has been implemented with only the privileges specified on the documented approval.	To ensure that user accounts granted access to systems are all valid and recognized users, strong processes must manage all changes to user IDs and other authentication credentials, including adding new ones and modifying or deleting existing ones.	GateKeeper Enterprise allows an organization to centrally manage the creation, modification, and deletion of user accounts within the GateKeeper's 'Credentials and Token Management' console. Only authorized system administrators can access this console.
8.1.3 Immediately revoke access for any terminated users.			Centralized management, in conjunction with Active Directory, allows for rapid identification and removal of user accounts with the GateKeeper management console. In addition, users' authentication tokens (keys) can be disabled to prevent unauthorized access to systems.