Retention Science
2601 Ocean Park Blvd. Ste 104
Santa Monica, CA 90405
310.598.6658
support@retentionscience.com

Access Control Policy

Category:	Access Control
Date Last Edited:	May 12, 2015
Version:	2.1.2

Access Control Policy

Purpose

The purpose of this policy is to establish security requirements, in order to ensure controlled access to the information resources of Retention Science.

Scope

This policy applies to all users of information assets including Retention Science employees, employees of temporary employment agencies, vendors, business partners, and contractor personnel and functional units regardless of geographic locations.

This Policy covers all Information Systems environments operated by Retention Science or contracted with a third party by Retention Science. The term “IS environment” defines the total environment and includes, but is not limited to, all documentation, physical and logical controls, personnel, hardware (e.g. mainframe, distributed, desktop, network devices, wireless devices), software, and information.

Although this Policy explicitly covers the responsibilities of users, it does not cover the matter exclusively. Other Retention Science Information Security policies, standards, and procedures define additional responsibilities. All users are required to read, understand and comply with the other Information Security policies, standards, and procedures. If any user does not fully understand anything in these documents, he should consult with his systems administrator, business or functional manager, or human resources department, as applicable, who will contact the Information Security Department.

The Information Security Department shall resolve any conflicts arising from this policy.

Responsibilities

- The sponsor of this policy is the Information Security Manager.

- The Security department is responsible for maintenance and accuracy of the policy.
- Any questions regarding this policy should be directed to the Security Department.

Definitions

Definition of some of the common terms:
Authentication: The identification requirements associated with an individual using a computer system. Identification information must be securely maintained by the computer system and can be associated with an individual's authorization and system activities.
Availability: Ensuring that authorized users have access to information and associated assets when required.
Confidentiality: Ensuring that information is accessible only to those authorized to have access.
Critical: Degree to which an organization depends on the continued availability of the system or services to conduct its normal operations.
Integrity: Safeguarding the accuracy and completeness of information and processing methods.
Sensitive: Concerned with highly classified information or involving discretionary authority over important official matters.

Policy Statement

Access controls are necessary for Retention Science systems that contain sensitive or limited access data. This policy describes the mechanisms used to implement access controls and responsibilities to ensure a high level of information security.

Business requirement for access control

Access control policy

Access to information must be specifically authorized in accordance with Retention Science's Access Control policy. Access to information will be controlled on the basis of business and security requirements, and access control rules defined for each information system.

All Retention Science users must be allowed to access only those critical business information assets and processes, which are required for performing their job duties.

Access to critical business information assets and activation of user accounts for contractors, consultants, temporary workers, or vendor personnel must only be in effect when the individual is actively performing service for Retention Science departments, franchises, operating companies, or operating units.

Access for contractors, consultants, or vendor personnel to Retention Science critical business information assets will be provided only on the basis of a contractual agreement. Any non-employees and/or visitors at Retention Science must wear a clearly displayed visitor's badge at all times while on the premises. For PCI covered data, visitors are asked to surrender the physical token before leaving the facility or at the date of expiration. After business hours, guards on patrol actively perform surveillance of the Retention Science premises.

Individuals being involuntarily terminated are subject to Retention Science Employee Exit Policy.

User access management

User registration

The registration and termination of users must be in accordance with the User Registration and Termination Procedure.

All users of information resources must have a unique User ID and authorization from the system owner or management, to access Retention Science's information assets.

All users must be provided with a written statement of their access rights and terms and conditions for usage of these rights.

No users are provided access to any information system before the full completion of authorization procedure.

A formal record of all registered users must be maintained. This record must be checked periodically for unused, redundant, or expired user accesses or accounts, or incorrect privileges.

Redundant User-ID's must not be re-issued to new users.

Accounts that are inactive for a maximum period of 90 days must be disabled, after verification for a valid cause.

User account of personnel transferred to different Retention Science departments must be reviewed for adequate privileges.

New accounts that have not been logged within for a maximum period of 14 days must be disabled.

User accounts of personnel quitting Retention Science must be removed immediately after their termination of job.

All third party personnel requiring access to Retention Science's information systems must follow Third Party Access Authorization procedure for registration to access Retention Science's information assets. For PCI covered data, a visitor log is retained for a minimum of three months, unless otherwise restricted by law.

Privilege Management

All privileges to the users must be assigned through a formal authorization procedure and Retention Science must ensure that no privileges are assigned before the completion of the authorization procedure.

All privileges must be allocated as and when required on a need to know basis. Detailed records must be maintained for all privileges allocated.

User Password Management

All users must follow Retention Science's Password policy regarding their passwords usage and management.

Initial temporary passwords must be conveyed in a secure manner. Wherever Retention Science standard encryption algorithm option is available, initial temporary passwords shall be conveyed via e-mail.

All users must change their temporary password on first login.

In case of forgotten passwords, temporary passwords should be issued only after positive identification of the user.

All passwords relevant to the System Administrator who has resigned or terminated, must be changed.

Users should not store password on a computer or at a place, which has public access. All users should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

- Contain at least three of the five following character classes:

  - Lower case characters

  - Upper case characters

  - Numbers

  - Punctuation

  - "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)

- Contain at least fifteen alphanumeric characters.

Specifically for PCI covered data:

- Shared, group or generic passwords and accounts are explicitly prohibited.
- User passwords must be changed at least every 90 days.
- Passwords must be at least seven characters and contain a mixture of letters and numbers.
- Users may not reuse any of their last four passwords.

Review of User Access Rights

All user access rights must be reviewed every 6 months.

Review of all special privileged access rights must be carried out at an interval of 3 months.

User responsibilities

Password use

All users must abide by the Password Policy.

Unattended user equipment

All users must enable password-protected screen savers on user desktops, portable computers/laptops, and servers. The user should set the timer to enable the screen saver after not more than 15 minutes of inactivity.

Each user must terminate active sessions when activities are finished.

For mainframe computers, users must log off after completion of their tasks.

Clear Desk and Clear Screen Policy

The clear desk and clear screen policy is used to reduce the risks of unauthorized access, or loss of, or damage to, information. The following are the policy standards:

- Users must log off their computers when their workspace is unattended.
- Users must shut down their computers at the end of the workday. Laptop computers, computer terminals and printers should be switched off when not in use and should be protected by locks, passwords and the like.
- All confidential information must be removed from the desk and locked in a drawer or file cabinet when the workstation is unattended and at the end of the workday.
- File cabinets containing confidential information must be locked when not in use or when not attended.
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.
- Passwords must not be posted on or under a computer or in any other accessible location.

Network access control

Policy on use of network services

Access to networks and network services must be specifically authorized in accordance with Retention Science's User Access Control procedures.

Access to networks and network services will be controlled on the basis of business and security requirements, and access control rules defined for each network. Physical and logical access to diagnostic and configuration ports will be controlled.

Segregation in networks

Retention Science's information systems network must be divided into logical segments based on the access requirements.

Internal network must be segregated from the external network with different perimeter security controls on each of the networks.

The connectivity between internal and external networks must be controlled.

For systems subject to PCI requirements, a firewall must be in place at each Internet connection and between any DMZ and the Intranet. No card data may reside on any Internet facing systems. Further, outbound traffic from payment card applications to IP addresses within the DMZ is restricted.

Network connection control

A Service Policy Table must be formulated for each service that is allowed through each firewall.

All external connections by business partners and customers must be documented and authorized in accordance with the defined “Security Change Request” procedure.

Network routing control

Appropriate routing control mechanisms must be deployed to restrict information flows to designated network paths within the control of Retention Science.

Network routing controls must be based on positive source and destination address checking mechanisms.

Security of network services

Retention Science must obtain detailed descriptions of the security attributes of any external services (if any) from external Network services providers

Security attributes description must establish the confidentiality, integrity, and availability of business applications and the level of controls (if any) required to be applied by Retention Science.

Description of the security controls must be included in the agreement of the service.

Operating system access control

Automatic terminal identification

Automatic terminal identification must be used when it is important that transactions are only initiated from a specific terminal or location.

Terminal log-on procedures

The terminal logon procedure must disclose a minimum amount of information about the system.

System administrators must set the password management system to suspend the User-Id after three consecutive unsuccessful attempts. A system administrator must receive approval from the user's supervisor to reset the User-Id.

The logon procedure must not identify the system or application until the logon process has been successfully completed.

The system must validate the logon information only on completion of all input data. After a rejected logon attempt, the logon procedures must terminate. The procedure must not explain which piece of information (the User-Id or password) was the reason for the logon termination. If an error condition occurs, the system must not indicate which part of the data is correct or incorrect. The logon procedures must set a maximum time allowed for the logon process. If the time is exceeded, the system must terminate the logon process.

On successful completion of logon, the logon procedures must display the date/time of the previous successful logon, and the number and date/time of unsuccessful logon attempts since the last
successful logon.

User identification and authentication

Retention Science departments must identify and authenticate all users uniquely before granting the appropriate system access.

The User-Id naming convention must be consistent and documented.

User-Ids must not be shared between users.

Specifically for PCI covered data:

- 2-factor authentication must be used for remote access to the network by employees, administrators and third-parties
- Accounts used by vendors for remote maintenance are disabled

Use of system programs

Access to and use of system programs must be restricted and controlled.

Use of system programs must be limited to authorized individuals.

All actions done by an individual on system programs must be logged.

All unnecessary system utilities and software, including compiler programs, must be removed.

Terminal time-out

All systems must be locked after 15 minutes of inactivity.

Limitation of connection time

Wherever possible, all critical systems must have a defined time slots for access and connectivity.

PCI covered data

Retention Science will ensure that the usage policies for critical employee facing technologies require the following:

- Explicit management approval to use the technologies.
- All technology use be authenticated with user ID and password or other authentication item.
- A list of all devices and the personnel who have access.
- Labeling devices with owner, contact information, and its purpose
- When accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media technologies.

Remote access sessions must be automatically disconnected after 15 minutes of inactivity.

Application access control

Information access restriction

Access to Retention Science information resources and application must be restricted to users who require them and in accordance with information Access Control Policy and Asset Classification Policy.

All users must have controlled access (Read, Write, Modify, Execute and Full control) to all information resources and business applications of Retention Science, in accordance to their requirements.

The owner of the information resources and business application must review the access rights based on criticality of information or at every 6 months.

Sensitive system isolation

All sensitive systems like Switch Element Configuration Management System, Business Support System, Operation Support System and Integrated Customer Management System must have an isolated and highly secured computing architecture. Programs that could override system and application controls must be restricted and controlled.

Monitoring

Monitoring system access and use

All event details on information system must be logged and stored for 6 months for ordinary systems and one year for critical systems.

All information systems and business application must be monitored and results of monitoring must be reviewed periodically.

All system clocks must be synchronized and reviewed for inaccuracy and drift.

All unsuccessful login attempts to critical servers must be recorded, investigated, and escalated to management.

Access Controls – Other

Mobile computing and remote access

All mobile computing facilities (e.g. laptop computers, palm top computers, notebooks, mobile phones) must be used in a secured environment, using cryptographic controls for communication purposes.

All mobile computing facilities (laptop computers, palm top computers, notebooks, mobile phones) must not be left unattended and must be physically locked.

All mobile computing facilities (e.g. laptop computers, palm top computers, notebooks, mobile phones) must have boot passwords.

All personnel using remote access must be provided with a secure connection (E.g.: – Secure Socket Layer, IPSec, Virtual Private Network, encryption) to Retention Science's information system network.

All wireless connection technology used must be designed in accordance with defined access control procedures.

The maintenance and support, audit, monitoring, training on security controls and practices, management of access rights, and physical security for remote access, must be in accordance with the defined procedures.

Head of the departments must restrict remote access to specific time and duration for all personnel availing these facilities.

Shared Folders

Access to shared folders must be authorized for specific persons only.

Shared Folders must be used for work purpose only. Sharing any non-work related is not permitted.

Compliance Measurement

Compliance with Access Control Policy is mandatory. Managers must ensure continuous compliance monitoring within their organizations. Compliance with Access Control Policy will be a matter for periodic review by Information Security Audit team as per the audit guidelines and procedures mentioned in Security Control Framework and the Security Auditing Guidelines.

Compliance measurement should also include periodic review for Security Quality Assurance. Violations of the policies, standards, and procedures of will result in corrective action by management. Disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets
- Other actions as deemed appropriate by management, Human Resources, and the Legal Department.

Waiver Criteria

This Policy is intended to address information security requirements. Requested waivers must be formally submitted to the Information Security Department, including justification and benefits attributed to the waiver, and must be approved by the Information Security Manager. The waiver should only be used in exceptional situations when communicating non-compliance with the policy for a specific period of time. At the completion of the time period the need for the waiver should be reassessed and re-approved, if necessary. No policy should be provided waiver for more than three consecutive terms. The waiver should be monitored to ensure its concurrence with the specified period of time and exception. All exceptions to this policy must be communicated through the Policy Waiver Request Form.