

*Client Logo*

---

<Client Name>  
Security Requirements

---

Version 0.1

<Date>



## Table of Contents

Revision History .....	3
Objective .....	4
Authentication Process.....	4
Account Information .....	4
Passwords.....	5
Applications.....	6
Environments .....	7
Architecture.....	8
Network .....	8
System Administration .....	9
Backups, Logs and Audit .....	10
Logging Requirements .....	10
Legal Requirements for Logging .....	11
Log Retention .....	11
Log Monitoring (Intrusion Detection) .....	12
Availability & Reliability .....	12
Third Party Requirements .....	12
Outsourced Development .....	13

## Revision History

Version	Date	Description	Author

## Objective

The objective of this document is to list some common security requirements that should be considered for data protection

## Authentication Process

### Account Information

Req. #	Requirements	Required
Acct-1	Access to the network and to each system must be controlled through use of individually owned user accounts and associated confidential authentication key or password.	
Acct-2	A formal record must be maintained of all access rights, including complete user or account names and group descriptions.	
Acct-3	Accounts that become inactive or unused must be suspended after sixty (60) days, and, if they remain inactive, deleted after ninety (90) days.	
Acct-4	Temporary user accounts may have to be set up, e.g., for test purposes. Such accounts must have an expiration date.	
Acct-5	Users shall be provided, initially and on a reset, with a temporary password that they are required to change immediately. In order to ensure calls for password reset are valid, user's identities must be verified using information about the user that only the user would know. Temporary passwords must be conveyed to users in a secure manner.	
Acct-6	Unneeded or unsecured special accounts must be restricted or removed. Examples include Guest, Anonymous, Null, and non-user accounts.	
Acct-7	The logon procedure must not request or display information during the logon procedure that would aid an unauthorized user.	
Acct-8	Logon information shall be validated only on completion of all input data. If an error condition arises during login, the system shall not indicate which part of the data is correct or incorrect.	
Acct-9	The number of grace logins must be set to a maximum of six (6) notices. (A grace login allows the user to delay changing their password, and to log in for a fixed number of times, after which they are required to change their password, and cannot proceed to log in until they do.)	

Req. #	Requirements	Required
Acct-10	The number of unsuccessful logon attempts must be limited to five (5) logins. After 5 consecutive unsuccessful logon attempts: 1) record the unsuccessful attempt; and 2) inactivate the account for an automated timeout/reset period of 30 minutes or greater, or in a manner that requires a manual reset by the system administrator.	
Acct-11	User IDs must not give any indication of the user's privilege level (e.g., manager) nor the application system to which they have access.	

### Passwords

Req. #	Requirements	Required
Pass-1	Passwords must have a minimum length of eight (8) characters.	
Pass-2	Passwords must have a mix of alpha and numeric characters.	
Pass-3	Passwords must not contain more than two consecutive identical characters.	
Pass-4	Passwords must not contain any control characters (e.g., Ctrl-C) or blank spaces, which can allow for code/ fault injection.	
Pass-5	Passwords must not be reused for at least six (6) generations (consecutive changes).	
Pass-6	Passwords must be changed when the system prompts, or at least every sixty (60) days if the system does not prompt for a change. Applications that utilize two-factor authorization are not required to expire on a pre-defined schedule.	
Pass-7	Passwords must not be easily guessed by others or through use of automated tools.	
Pass-8	Passwords must be stored encrypted, hashed, or with access controls.	
Pass-9	Password files must be stored separately from the main application system data.	
Pass-10	Default passwords must be changed following installation of software and patches.	
Pass-11	An effective password management system or equivalent password management methodology must be used to authenticate users.	
Pass-12	All passwords generated on behalf of an individual user must conform to password management standards.	

## Applications

Req. #	Requirements	Required
App-1	Users of a system shall not have unauthorized access to other user's data.	
App-2	Passwords must not be stored unencrypted on disk, in computer memory, or in any system-based data repository, e.g., the NT Registry or .netrc files.	
App-3	Passwords must not be embedded in macros, scripts, job control language, programs, or files, unless they have been stored encrypted, hashed, or with access controls.	
App-4	Passwords must not be displayed in clear text on the screen when being entered.	
App-5	Application and system output that contains CONFIDENTIAL/PROPRIETARY data must be routed only to authorized terminals and locations.	
App-6	In scripts and aliases, commands must be executed using fully-qualified command names, for example, full path names. Using the full path name for a command can prevent the execution of malicious code residing in a local directory.	
App-7	Screen savers must be set to activate after a period of fifteen (15) minutes of user inactivity, and must be password protected. Active application sessions must be terminated, unless they can be secured by a screen lock or other protection.	
App-8	Logon credentials must not be cached on the system.	
App-9	Any screen/web page requiring a password entry shall be configured to prevent the caching of the entered password.	
App-10	Information must not be transmitted to cell phones in clear text.	
App-11	Though pager messages are hard to intercept, use appropriate caution when transmitting company data.	
App-12	Applications shall have controls to validate the integrity of data prior to be used as input to the application	
App-13	Applications shall have controls to validate the correct processing of data to detect data integrity errors caused by processing errors or malicious acts.	
App-14	Applications shall have controls to validate the integrity of electronically transmitted data to detect corruption or unauthorized changes.	

Req. #	Requirements	Required
App-15	Applications shall have controls to validate the integrity of processed or stored data.	
App-16	Passwords shall not be sent to the user via email unless the password is encrypted using an approved encryption tool such as Entrust.	
App-17	Passwords shall be encrypted during transmission.	
App-18	Browser based applications shall use 128-bit encryption if it exchanges confidential data with the browser. See Appendix B for more details.	
App-19	Browser based applications that require SSL shall restrict access to browsers capable of supporting 128-bit (or higher) encryption.	

## Environments

Req. #	Requirements	Required
Env-1	Developers who need to access production systems and applications for program maintenance or repair shall be given temporary access, which shall be revoked immediately after use.	
Env-2	Development and testing shall be conducted on non-production machines.	
Env-3	There shall be separation of development, QA and operational system environments.	
Env-4	Production data shall not be used for testing or training purposes. If production data is used as a starting point for creating test data, then appropriate controls must be in place to protect this data, and the data must be effectively depersonalized or altered to manage risk.	

## Architecture

Req. #	Requirements	Required
Arch-1	Confidential data should be appropriately protected during transmission using such tools as encryption.	
Arch-2	All confidential customer data traversing the Internet shall be encrypted.	
Arch-3	All confidential customer information shall be encrypted when stored on the Web server for any length of time.	

## Network

Req. #	Requirements	Required
Net-1	Computing and networking equipment shall not be connected to networks and computing environment unless it has appropriate authorization and adequate security controls incorporated and in use.	
Net-2	Connections by remote computer systems and applications must be authenticated. This is especially important if the connection is via an open network that is outside the control of the client. Authentication for computer-to-computer connections can be carried out at the application, computer or network level. Dedicated private lines can also be used to provide assurance of the source of connections.	

## System Administration

Req. #	Requirements	Required
Sys-1	Use of direct modem access to servers and of server-based functionality with dial-out lines must be approved by the Security Manager.	
Sys-2	Password protection must be used for system utilities.	
Sys-3	System utilities and programs must be restricted and tightly controlled.	
Sys-4	All clocks in systems and communications devices must be set to the correct time and date and the appropriate time zone. Clocks must be automatically synchronized with a national standard Coordinated Universal Time (UTC) server, such as a National Institute of Standards and Technology (NIST)-run atomic clock, within 6 leap seconds. (A leap second is added to the atomic time to decrease the difference between it.)	
Sys-5	There shall be a separation of duties. For example, system administrator accounts should not be used for system user tasks.	
Sys-6	Default passwords must be changed following installation of software and patches.	
Sys-7	Applications that run under a privileged ID or in a privileged mode must be configured and monitored so as to prevent misuse and manage security risk.	
Sys-8	All default system and application passwords must be changed during the installation process.	
Sys-9	The Information Protection Technical Security Standards must be applied to ensure adequate security in system and application installation and configuration.	
Sys-10	Authorization levels for system utilities must be defined and documented.	
Sys-11	Software, software development tools and programs, and system utilities that are unnecessary must be removed. Unnecessary operation systems or kernels must be removed.	
Sys-12	Production systems shall not be implemented with source code, programming libraries, development tools, or utilities not explicitly required to perform production-related functions.	
Sys-13	Program source libraries shall be configured and maintained with appropriate access control.	

Req. #	Requirements	Required
Sys-14	Formal procedures shall be in place to ensure that the appropriate level of controls over changes to production environments.	
Sys-15	Administration of computing devices on the DMZ must be transmitted over channels that are secured end-to-end.	

## Backups, Logs and Audit

### Logging Requirements

Req. #	Requirements	Required
Log-1	Privileged account usage must be logged and monitored.	
Log-2	All use of system utilities must be logged.	
Log-3	To ensure a complete record of events, logs must be produced that include: user IDs; dates and times for log-on and log-off; source IP addresses; terminal identity or location; records of successful and rejected attempts to access system, data and other computing resources.	
Log-4	Audit trails shall be linked to the user identity responsible for the security relevant event.	
Log-5	Log files must be made available by system and application administrators in a readable format for periodic review by an "independent observer" who is trained and authorized in identifying security violations, malicious behaviors, and misuse of privileges.	
Log-6	There shall be audit trails of security-related events.	
Log-7	Logging and data collection shall be in place for systems that have access to or process nonpublic personally identifiable customer information. Logging shall be performed in a secure manner and provide analytical capabilities to identify authorized successful access, identify unauthorized access attempts and security violations, provide audit trails for user action as appropriate, and aid in reconstructing compromised systems.	

## Legal Requirements for Logging

Req. #	Requirements	Required
Leg-1	Browsing of disclosure statements and any other legal notices related to opening or changing the status of an account shall be logged. These activities must be archived so that it can be proved what the customer viewed and/or agreed to.	
Leg-2	Customer actions on websites that impacts or changes their account needs to be archived until 7 years past the closing of the customer's account. Examples of this type of change are the opening of an account, changing the account's mailing address, paying a bill or transferring funds, and changing a password.	
Leg-3	When an account becomes internet-only (no longer receive a paper bill, etc.) additional archiving will be required to demonstrate that the customer saw statement information that would otherwise be available in the paper bill or other paper delivery of information. This allows the client to prove whether a customer saw a statement, fee, or policies.	

## Log Retention

Req. #	Requirements	Required
Ret-1	Log file entries that are less than 60 days old are considered "short-term" logs and must be maintained in a manner that makes them accessible to an investigator within 2 hours of request.	
Ret-2	Log file entries that are older than 60 days are considered "long-term" or "archived" logs and must be maintained in a manner that makes them accessible to an investigator within 24 hours of request.	
Ret-3	All event logs must be retained and appropriately protected for 13 months. After this period, log files may be destroyed. Destruction of logs from online systems and backup media should ensure that the data is not recoverable by unauthorized persons.	

### Log Monitoring (Intrusion Detection)

Req. #	Requirements	Required
Mon-1	Employees have the responsibility to report security-related incidents or suspicious activities immediately.	
Mon-2	There shall be timely review of critical audit trails such as application system utilities and privileged user activities including failed log-in to root and all failed log-in attempts.	
Mon-3	Logging and data collection shall be in place for systems that have access to or process nonpublic personally identifiable customer information to provide audit trails for user action as appropriate.	

### Availability & Reliability

Req. #	Requirements	Required
Avail-1	Critical services shall be protected against denial of service conditions.	
Avail-2	There shall be controls to ensure the ability to recover from failures.	
Avail-3	Business continuity plans shall be established and validated.	

### Third Party Requirements

Req. #	Requirements	Required
Third-1	All Confidential/Proprietary information or materials shall be safely disposed of when no longer needed, such as by shredding paper and CDs or by fully deleting electronic files.	
Third-2	A non-disclosure agreement (NDA) shall be signed by the third parties prior to any exchange of data or confidential information.	
Third-3	Media containing data (tapes, CDs, etc.) shall be secured while at a third party facility.	

## Outsourced Development

Req. #	Requirements	Required
OutS-1	Outsourced projects must have acceptance criteria and test plans to validate the source code.	
OutS-2	Prior to implementation, a review and test of source code for security vulnerabilities, including covert channels or backdoors that might obscure unauthorized access into the system or application must be conducted and documented. This cannot be performed by the third party that has been contracted to do the systems development.	
OutS-3	Security controls for outsourced development include restricting third party access to production source code and systems, and monitoring their access to development systems.	
OutS-4	Outsourced application development must be tested to validate that information protection requirements are met before implementing the system or application in production.	