

Programming Security Guidelines

1. All stored account passwords must be encrypted
 - Must meet the legal requirements of each country in which the information assets are located, including all countries to which the information assets are exported
2. All **Personal Information** (PIM) data must be encrypted
3. All **PCI** (Credit Card Information) data must be encrypted and approved for storage
4. All authentication, PCI, and PIM communications **must be encrypted**, from entry-point to end-point (using SSL or other encryption method when transmitted)
5. Authentication process should use single sign-on (SSO) LDAP.
6. All user authentication attempts are recorded and **logged**
7. Logging / auditing must be done for all PCI, PIM and financial data (SOX) created, changed or deleted
8. Application log retention policy must be documented
9. Establish and document an access control guideline defining the scope for granting access rights to users and the registration and authorization process for users.
 - Minimum access rights are to be considered when granting access to users who have a business need for access. Application Owner/Data Owner must limit access rights to a minimum and must not grant access rights to users who do not need access for business use.
 - Access to administrator functions such as read, write, change, execute, and delete shall be permitted and controlled depending on the user's responsibility
 - Access to data by users must be controlled and based on the confidentiality of the information and the need to access the information.
 - A periodic review of user access rights.
 - As to the business application and related data shared by multiple legal entities, the same access control guideline shall be applied to each legal entity.
 - The strength of required system authentication must meet the following requirements:
 - i. **"SECRET"** (level 1) - two-factor or more is required
 - ii. (Example of two-factor authentication: ID card + PIN)
 - iii. **"CONFIDENTIAL"** (level 2) - one-factor or more is required
 - iv. **"INTERNAL USE ONLY"** (level 3) - one-factor or more is recommended.

10. The application must not display system information, such as OS level, version, middleware, or other products on the server
(ex: http 404 error pages, often returned when pages have been moved or deleted, by default contain local server system information – these pages must be customized to remove the system version & hosting application information)
11. Detailed application connectivity mechanism must be documented
12. Applications with third-party connectivity must be approved, secured, and controlled (requires security audit, NDA)
13. Operational security and recoverability (Business Continuity Planning) must be documented – Operations
14. Separation between development and production is required
15. Third-party software code must be tested and certified
16. Access to program source code shall be restricted (e.g., CVS, source version control software)
17. Review the content of key fields or data file contents periodically to confirm validity and integrity
18. Use dual input, boundary checks, or fields that limit the input data range
 - Test for out-of range values
 - Test for invalid characters in data fields
 - Test for missing or incomplete data
 - Test for exceeding upper and lower data volume limits
 - Test for unauthorized or inconsistent control data
19. All user identification must have a **unique** identifier (user ID)
20. A formal user registration process must be implemented and designed to ensure users have the appropriate approvals
21. The user ID must be disabled after no more than 10 consecutive unsuccessful login attempts during a 30 minute period
22. All failed login messages shall be non-descriptive (e.g., the message will not indicate what part of the log-in failed)
23. Any user ID that has been inactive for a period of 90 days or more shall be disabled
24. Passwords must be at least 6 characters long, 8 characters for privileged accounts, and combine 2 kinds of characters such as alphabet and number. Previously used passwords must not be re-used

25. Server platform hosting the application **MUST** be scanned for potential OS level vulnerabilities, have updated anti-virus signatures, and have up-to-date patches applied