APPLICATION SECURITY PROCEDURE

Purpose: This procedure identifies what is required to ensure the development of a secure application.

Procedure: The five basic areas covered by this document include:

Standards for Privacy and Security
User Account Management
Data Protection
Application Configuration and Operations
Application Development Based on Secure Coding Guidelines

Each area identifies specific concerns about how the application manages an activity or accesses the data set. All applications must identify how the application handles a particular function. Instances in which the application does not handle a specific function should be noted as a finding. A finding neither passes nor fails the application. It is, however, an indication that additional attention must be given to that particular issue.

Standards for Privacy and Security

Determine if the data collected and maintained in the system is required to be secured in accordance with state or federal laws, regulations or policies. Specific development standards may impact on the design, implementation, and maintenance of an application.

1. **Does the application contain information designated as containing protected or regulated data sets?**

   Finding: Yes____ No____ N/A____

   Data managed and maintained by state applications may include sensitive information regulated by numerous state and/or federal statutes. If the data is so regulated, this is a finding. Document the requirement under which the data must be protected. These may include one or more of the following:

   a. Exemption of NH Right to Know statute (RSA 91-A:5)____
   b. Health Insurance Portability and Accountability Act (PL 104-191)
   c. Standards for Privacy of Individually Identifiable Health Information (45 CFR 160 and 164)____
   d. Family Educational Rights and Privacy Act (20 USC 1232g and 34 CFR 99)____
   e. Unique Pupil Identification (RSA 193-E:5)____
   f. Privacy Act of 1974 (5 USC 552a)____
   g. Federal Tax Information (FTI)____
   h. Payment Card Industry (PCI) Data Security Standard (PCI DSS Req. 6.x)____
      Note: see Payment Card Industry Data Security Standards Application Development and Maintenance Procedures for additional requirements
   i. Other: ____

   If any protected or regulated data sets are included as indicated above, please provide specific information about application security standards required to be in place. Include any documents required by an audit team to determine if the statutory or regulatory requirements have been met.

   A finding in this instance indicates that higher security and data protection methods may be required.

APPLICATION SECURITY PROCEDURE

User Account Management

Best practices relative to how users and processes authenticate to the system as well as issues relative to account management.

1. **Does the application have a process to authenticate all users and clients?**
Finding: Yes____ No____ N/A____
Regardless of authentication approach, the application must authenticate every session. Validate that the application prompts for credentials when opening a second session when one is already active. In the case of a browser, determine if credentials can be cached within the browser and can be reissued without requiring user input. To check, close all browser sessions and immediately initiate another session. If the new session doesn't require authentication, this is a finding.

For each process, determine the nature of the authentication. Authentication may involve one or more of the following:

- A password (something you know)
- An X.509 certificate or hardware token (something you have)
- A biometric (something you are)

In addition, the authentication may involve a user account database specific to the application or it may involve leveraging the authentication service of an operating system or directory service.

If the authentication is based on passwords, the passwords must conform to the OIT User Account and Password Policy

If authentication is based on any technology other than a user ID and password, it must be at least as strong as a password-based authentication approach that complies with the standards listed above. The primary measure of strength is that a brute force attack on the alternative authentication technology would be expected to take at least as long as a brute force attack on an appropriately configured password system. Most commercial token and biometric authentication methods meet these criteria, but study the technology carefully if it is non-standard.

Describe how this is done: ____

2. **Are user IDs unique?**
Finding: Yes____ No____ N/A____
Identify duplicate user IDs. If any duplicates are discovered, this is a finding.

Describe how this is done: ____

3. **Have all unnecessary built-in user IDs been disabled?**
Finding: Yes____ No____ N/A____
Built-in accounts are those that are added as part of the installation of the application software. Verify that these accounts have been removed or disabled. If enabled built-in accounts are present, document the reason for their existence. If these accounts are not necessary to run the application, this is a finding.

Describe how this is done: ____

4. **Is there a mechanism to disable inactive user IDs?**
Finding: Yes____ No____ N/A____
Identify all users that have not authenticated in accordance with User Account Maintenance Policy. If any of these are active, this is a finding.

Describe how this is done: ____

5. **Does the application enforce complex passwords?**
   Finding: Yes____ No____ N/A____
   Review the code or process to ensure that enforces password complexity in accordance with the User Account Maintenance Policy. If the code is found to have weak passwords, this is a finding.

   Describe how this is done: ____

Data Protection

The following checks relate to the use of permissions and cryptography to protect data both while it is at rest and while it is in transit. Information concerning identification of sensitive data can be obtained from the data owner.

1. **Does the application enable a client to authenticate the application server with which it communicates?**
   Finding: Yes____ No____ N/A____
   The application must enable clients to authenticate the server or the application it is communicating with. The most common example of this type of authentication is when a client validates a server's certificate when initiating an SSL or IPSEC connection.

   If the server authentication process is not initiated by a user action (e.g., authentication of backend devices), then review the configuration of these devices to determine how the authentication occurs. If the client's authentication of the server does not involve cryptographic methods, this is a finding.

   Describe how this is done: ____

2. **Is Sensitive application data protected at rest?**
   Finding: Yes____ No____ N/A____
   Sensitive data must be protected by appropriate file permissions. With respect to authentication and authorization information, only administrators and the application or OS process that access the information should have any permissions to these files. In many cases, local backups of the accounts database exist so these must be included in the scope of the review. If any other user has the ability to write to an I&A database or read authentication credentials, this is a finding. If non-privileged users can read information other than authentication credentials (e.g., list users but not passwords), this is a finding.

   Authentication credentials such as passwords are required to be encrypted. If the data encryption functionality is not configurable and the data are stored in ASCII or another readable format, then this is a finding.

   With respect to non-public user data, identify data owners and any documented instructions they have regarding who should have what level of access to particular data. Review permissions on selected application data files (or database tables).

   If the permissions granted to users are beyond the minimum necessary to meet business and application requirements, then this is a finding.

   Describe how this is done: ____

3. **Is sensitive application data protected in transit?**
Finding: Yes____ No____ N/A____
Identify what authentication protocols are utilized and which, if any, send passwords in clear text (e.g., Telnet, FTP and basic HTTP authentication). If such techniques are used, determine if a lower-level protocol provides encryption service. Examples include IPSEC, L2TP, PPTP and STU/STE devices. If neither an authentication protocol nor a network service encrypts passwords before they traverse a network, this is a finding.

Note: If application and database are colocated on the same machine data transmission between them does not need to be encrypted.

Describe how this is done: ____

4. **Does sensitive information from production database exports remain unmodified after import to a development database?**
Finding: Yes____ No____ N/A____
If there are such exports and the database includes sensitive data identified by the data owner as sensitive, is there a process to modify it prior to or after importing into the development environment. If there is not, then this is a Finding.

Describe how this is done: ____

5. **Does the application log security-relevant events?**
Finding: Yes____ No____ N/A____
Minimum security events to be audited should include:

- Startup and shutdown
- Authentication
- Authorization/permission granting
- Actions by trusted users
- Process invocation
- Controlled access to data by individually authenticated user
- Unsuccessful data access attempt
- Data deletion
- Data transfer
- Application configuration change
- Application of confidentiality or integrity labels to data
- Override or modification of data labels or markings
- Output to removable media
- Output to a printer

For sensitive or confidential data, events to be audited should include:

- UserID of user or process ID of process causing the event
- Success or failure of attempt to access security file
- Date/time of event
- Type of event
- Success or failure of event
- Seriousness of event violation
- Success or failure of login attempt
- Denial of access resulting from excessive number of login attempts

APPLICATION SECURITY PROCEDURE

- Blocking or blacklisting of UserID, terminal, or access port, and reason for the action
- Activities that might modify, bypass, or negate security safeguards controlled by the application,
- For authentication/authorization events: origin of request (e.g., originating host's IP address)
- For write or delete events: name of data object written or deleted
  If all the required events and associated details are not included in the log or there is not logging mechanism, this is a finding. The mechanism that performs auditing may be a combination of the operating system, web server, database, application, etc.

Describe how this is done: _______________________________________

Application Configuration and Operation

The following checks deal with the operation of the application. The checks involve looking at the operational aspects of the application.

1. **Does the application authorize actions before they are executed?**
   Finding: Yes____ No____ N/A____
   Determine how the application authorizes transactions. The authorization function may leverage file permissions enforced by the operating system or views enforced by the database software. Alternatively, authorization mechanisms may be built into the application code.

   If neither the application code nor the access controls of supporting software provide appropriate controls preventing unauthorized users from performing transactions that require authorization, then this is a finding.

   Describe how this is done: ____

2. **Does the application allow authentication credentials to be stored on client computers after a session terminates?**
   Finding: Yes____ No____ N/A____
   Persistent cookies are the primary means by which an application stores authentication information over more than one browser session. If identification information (e.g., user name, ID or key properties, credentials) exists, this is a finding.

   The application may use means other than cookies to store user information. If the reviewer detects an alternative mechanism for storing authentication and authorization information locally, this is also a finding.

   Describe how this is done: ____

3. **Are authentication credentials or sensitive data stored in the application's code?**
   Finding: Yes____ No____ N/A____
   Review source code (including global.asa, if present), scripts, and HTML forms to locate any instances in which a password, certificate, or sensitive data is included in code. If any of these are found, then this is a finding.

   Describe how this is done: ____

4. **Does the application validate user inputs before processing them?**
   Finding: Yes____ No____ N/A____
   Invalid input includes presence of scripting tags within text fields, query string manipulation, SQL command, and invalid data types and sizes.

   For script tag embedding, select a text field of the application that accepts at least 15 characters. Try to input a script tag (<script>) into the field. If the data is accepted without an error, access the data entered via the application (this process will vary depending upon the application). If the script tag in its entirety is displayed within the application this is a finding.

   For SQL injection, select web pages for testing that use input fields that are matched against a field in the data. For example, the reviewer may choose a page that has an input field looking for a name that will be used to match all names within the database. Instead of entering a name such as *smith*, enter the following in the field: *smith' or 1=1* --. If the results display more names than smith, this is a finding.

For testing invalid sizes and types, test various fields on multiple HTML forms and other input mechanisms. For example, if the field is for a SSN, enter a text string. If the field is for a date, enter a word, etc. If invalid data is accepted, this is finding.

Overall, select a sampling of source code, look for conditional statements, regular expressions, or calls to input validation routines near input routines in source code. Regular expression syntax varies depending upon programming language but will validate that the input data is of the expected format, length and type by validating it against elements in an expression. If data input validation is not being performed, this is a finding.

Describe how this is done: ____

5. **Is the application vulnerable to buffer overflows?**
Finding: Yes____ No____ N/A____
Check to determine if users can enter data larger than the application is expecting

This testing should include the following:

- Very large number including large precision decimal numbers in numeric data fields
- Both negative and positive numbers should be included in numeric data fields
- Large amounts of data (at least 1024K) into the text fields
- If the application is a web-based application that utilizes query strings, testing should include passing at least 500 characters of data into the query string parameter.

If the application gives an error that indicates that the error condition is not being checked, this is a finding.

Additionally, source code checking should be done. Select samples of source code to examine. The following items should be checked:

- For C code, applications should use only signed values (not unsigned values)
- Buffer sizes should not be defined as a fixed size
- Buffer size should not be smaller than a source buffer

If any of these items are found in code, this is a finding.

Describe how this is done: ____

6. **Can application users circumvent the intended user interface to access resources in its supporting infrastructure?**
Finding: Yes____ No____ N/A____
Review the application architecture and identify the application's "threat surface" – i.e., access points into each of the application's networked components. For example, a backend server may accept SQL queries and SSH connections and also have an NFS share. Next, examine firewall rules and router ACLs that prevent clients from reaching these access points, effectively reducing the area of the threat surface. For example, if the backend database

accepts queries but is in a networked area so that there are no user workstations and firewall rules allow only web traffic, this is not a finding.

For each the remaining access points, attempt to access these resources in a similar manner as the application would without utilizing the user interface (e.g., send SQL query using a tool outside of the application or attempt to access a share using command line utilities). If a user can authenticate to any of these remaining access points outside of the intended user interface, then this is a finding. The finding details should note the application component accessed and the method or tool used to access it.

If the application is a web application, logon and perform several routine functions, saving URLs at each step. After log out, use the saved URLs to determine if a resource can be obtained without authentication. Enter the IP addresses and host names of supporting servers to determine if these other servers can be directly accessed without first accessing the portal. If access is granted without any authentication, this is a finding.

Describe how this is done: ____

7. **Are non-privileged users allowed to perform privileged functions?**
Finding: Yes____ No____ N/A____
Log on as an unprivileged user. Examine the user interfaces (graphical, web and command line) to determine if any administrative functions are available. Privileged functions include the following:

- Create, modify and delete user accounts and groups
- Grant, modify and remove file or database permissions
- Configure password and account lockout policy
- Configure policy regarding the number and length of sessions
- Change passwords or certificates of users other than oneself
- Determine how the application will respond to error conditions
- Determine auditable events and related parameters
- Establish log sizes, fill thresholds and fill behavior (i.e., what happens when the log is full)
  If non-privileged users have the ability to perform any of the functions listed above, this is a finding.

Describe how this is done: ____

8. **Does the application allow users to explicitly terminate a session (logout)?**
Finding: Yes____ No____ N/A____
Log on to the application and then attempt to log out. If the ability to log out is absent this is a finding.

Check whether the application properly destroys or “smashes” a session when the function to logout out is exercised. To check, authenticate to the application, then choose the function or feature to logout and terminate the session. After logout if any features of the application can be accessed without having to re-login or re-authenticate, then this is a finding.

Describe how this is done: ____

APPLICATION SECURITY PROCEDURE

9. **Does the application use accounts with privileges not necessary for proper operation?**
   Finding: Yes____ No____ N/A____
   Identify the application user account(s) that the application uses to run. Determine the user groups in which each account is a member. List the user rights assigned to these users and groups and evaluate whether any of them are unnecessary. If the rights are unnecessary, this is a finding. If the account is a member of the Administrators group (Windows) or has a User Identification (UID) of 0 (i.e., is equivalent to root) (Unix) this is a finding. If this account is a member of the SYSAdmin fixed server role in SQL Server, this is a finding. If the account has DDL (Data Definition Language) privileges, (create, drop, alter) or other system privileges this is a finding.

   Describe how this is done: ____

10. **Does the application include an explicit error and exception handling capability?**
    Finding: Yes____ No____ N/A____
    Application error and exception messages displayed to users reveal information that could be utilized in a subsequent attack. The application code should not rely on internal system generated error handling. If the errors are not be handled by the application and are being processed by the underlying internal system, this is a finding.

    Customized application error should not include variable names, variable types, SQL strings, or source code. Errors that contain field names from the screen and a description of what should be in the field should not be considered a finding.

    Describe how this is done: ____

11. **Can an application failure result in an insecure state?**
    Finding: Yes____ No____ N/A____
    Simulate a failure. This can be accomplished by stopping the web server service and or the database service. Check to ensure that application data is still protected. Some examples of tests follow. Try to submit SQL queries to the database. Ensure that the database requires authentication before returning data. Try to read the application source files, access should not be granted to these files because the application is not operating. Try to open database files. Data should not be available because the application is not operational. If any of these tests fail, this is a finding.

    Describe how this is done: ____

12. **Does the application environment (server infrastructure) use unnecessary services or software within the environment?**
    Finding: Yes____ No____ N/A____
    Examine the configuration of the servers. Determine what software is installed on the servers. If there are services or software present that are not needed for the application, this is a finding. Some examples of this may be Office installed on a Domain Controller or FTP installed on a web server.

    Describe how this is done: ____

APPLICATION SECURITY PROCEDURE

Application Development Based on Secure Coding Guidelines

The following checks deal ensuring that security is built into the application at every stage of the software development lifecycle. The checks involve looking at the developing and coding aspects of the application.

1. **Was a code review conducted prior to release to customers for testing?**
   Finding: Yes____ No____ N/A____
   Prior to releasing the application to customers for UAT testing, a code review should be done to identify potential coding vulnerabilities. Vulnerabilities in custom code can be exploited to gain access to the application, the data or network.

   If a code review has not been performed prior to release of the application to a customer, then this is a finding.

   Describe how this is done: ____

2. **Were change control processes followed in the development of the application and promotion through various environments?**
   Finding: Yes____ No____ N/A____
   As the application was promoted through a development, test and production environment, were appropriate ICRs and segregation of responsibilities followed to ensure that the production environment is not compromised? Development and testing environments typically have less stringent security settings that do not exist in a production environment.

   If DOIT standard change control processes have not been performed prior to release of the application to a customer, then this is a finding.

   Describe how this is done: ____

3. **Was the application developed following secure coding guidelines?**
   Finding: Yes____ No____ N/A____
   The application layer is high-risk and can be targeted by both internal and external threats. At a minimum, the application development team must code to prevent exploitation identified by the OWASP Top Ten which includes, but is not limited to,

   SQL Injection, OS Command Injection, LDAP injection
   Buffer Overflows
   Insecure Cryptographic Storage
   Insecure Communications
   Improper Error Handling
   Cross-Site Scripting (XSS)
   Improper Access Control
   Cross-Site Request Forgery

   If application developers have not followed secure coding guidelines, then this is a finding.

   Describe how this is done: ____

Accountability: This procedure applies to all applications created and maintained by the DoIT.

APPLICATION SECURITY PROCEDURE

It is the responsibility of each DoIT Division Director and Bureau Chief or their designee to enforce this policy. Employees who do not comply with this policy shall be subject to disciplinary action as outlined in the Administrative Rules of the Division of Personnel.

Description: This procedure provides a common approach to application security.

Reference:

System Development Methodology (SDM)
Application Security Policy
Application Security Scan Request Form
SDM Security Guidelines
Administrator Account and Password Policy
User Account and Password Policy
User Account Maintenance Policy
IT Standards Exception Policy
Payment Card Industry Data Security Standards Application Development and Maintenance Procedures
Payment Card Industry Data Security Standards Application Development and Maintenance Form