Application Security Policy

Purpose

This document establishes the corporate policy and standards for ensuring that applications developed or purchased at Landstar Title Agency, Inc meet a minimum acceptable level of security.

Policy

All applications developed or purchased at Landstar Title Agency, Inc must be configured according to the requirements defined in this document.

Note: Single user utilities authorized by the Chief Information Officer (CIO) may be excluded from these requirements.

Requirements

Refer to these sections in this policy for application security requirements:

Violation of Policy

Failure to adhere to all requirements stipulated in this policy and all related documents may result in disciplinary actions, up to and including

- Immediate removal of any applicable hardware/software/access to the Landstar Title Agency, Inc computer network or business systems
- Formally reporting the incident to Landstar Title Agency, Inc senior management
- Termination of employment
- Any other action deemed necessary by Landstar Title Agency, Inc senior management

Review

Landstar Title Agency, Inc has voluntarily adopted this policy for its sole and exclusive use. This policy and all related documents will be reviewed annually or as needed based on prevailing business conditions.

Approved

Kenneth Warner, Esq., Vice President and Senior Counsel

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

General Requirements for All Landstar Title Agency, Inc Applications

Login Access Control

Applications must adhere to these login access control requirements:

- Applications must require all users to enter an individual username and password to access the application.
  Note: Web applications that do not contain confidential data and only allow view or post capabilities may be exempt from this requirement.
- Direct access to the operating system or database is prohibited—once a user is logged in, the application cannot expose a user interface that allows the user to directly execute operating system or database commands.
- Passwords must not display as they are typed.
- Passwords must be encrypted when
  - Stored (using a 256-bit one-way hash)
  - Transmitted across the network

Password Controls

Applications must require

- Users to change their passwords every calendar year or provide an approved process to register the user's machine with the application
- Complex passwords of 8 or more characters for all applications, with password lockout and password history features enabled

Windows authentication may alternately be used. See Password Policy.

Audit Trails

Applications must provide audit log reporting for

- Logon activity
- Changes to user accounts, access rights, or confidential information within the application
- All other audit requirements stipulated in the application's requirement document

All audit data must be maintained in the active database for a minimum of 90 days. All audit records must contain

- User ID of the person or process attempting the operation
- Date/time the event occurred (to the second)
- Object involved in the operation
- Type of action attempted
- Indication of success or failure

Operating Systems

Applications must be capable of running

- On vendor-supported versions of operating systems and associated service packs
- With standard security features of the operating system and database enabled and utilized

Object and Function Access

Object and function access must be configurable to allow

- System users and/or groups to be restricted to
  - Executing only those system functions for which they have been assigned
  - Accessing only those system objects for which they have been assigned
- Limited directory/share permissions for network access to the application and associated databases
  Note: User accounts must be added to specific user groups in order to access the application.

Each application shall grant the minimum object and function access to its users that is consistent with their assigned duties. All access decisions must be audited quarterly by the application business administrator and revised as needed.

Administration

Applications must be able to generate a report containing all users, including their type of access.

All security settings, access rules, user/group profiles, and audit data must be protected against unauthorized modification.

Business Continuity

Each application must establish documented business continuity requirements. See Business Continuity Policy.

Vendor Support

All vendor-supplied default settings (for example, passwords, SNMP community strings, and unnecessary accounts) must be changed or disabled before the application or system is placed into production. Systems may not possess any non-standard or undocumented mechanism for access. All access to a system or application must be coordinated through Landstar Title Agency, Inc using approved access control mechanisms.

Database Requirements

A current, vendor supported, version of the database must be delivered with the application. Data must also be stored so that users of the application cannot bypass the application's security (or gain more access) when accessing the data at the operating system or database levels).

Fields that contain NPI must be encrypted. For more information, see Non-Public Information Security and Disposal Policy.

E-commerce/Web Applications

Overview

This section lists requirements for all Landstar Title Agency, Inc electronic commerce (e-commerce) applications. An e-commerce application is an application used to conduct business utilizing the Internet.

Web Server

E-commerce Web servers must meet these requirements:

- Servers must be running supported versions of both the operating system and Web server.
- Vendor recommendations or checklist for security must be applied.
- All unnecessary software, files, and utilities must be removed from the server.
- Web sites or applications must not reside on the boot drive (drive C).
- System drives must be hidden from user interaction.
- Default Web accounts may only be run with guest privileges.
- Applications must be run as services that do not have administrator privileges.
- Servers must contain an automated utility to monitor activity and alert administrators to security violations.
- Transaction data and FTP files automatically must be removed from the server when they are no longer required for processing

Network Design

E-commerce network design must meet these requirements:

- The Web server must be located behind a firewall with only required ports allowed from the Internet. **Examples:** Port 80, 443, or 21
- All confidential information such as any personal, financial, or authentication data must be stored on a database server that is separate from the Web server.
- A firewall must separate the Web server and any database server with only required traffic allowed.
- Critical Web applications must not reside on servers that are hosting other applications such as FTP sites or non-critical websites

Database

E-commerce databases must meet these requirements:

- The Web application must not access the database using the default administration account. An account with the minimum access required must be created instead.
- Database passwords must not be imbedded in application code or files.
- The database server must be located on a secure network subnet that is not accessible from the Internet or other public networks.
- Encryption should be accomplished using 256-bit encryption algorithm in conjunction with the Windows Security API.
- All unused stored procedures should be removed—xp_cmdshell, xp_startmail, xp_sendmail, and sp_makewebtask must never be used.

Code Content

E-commerce code content must meet these requirements:

- Never use GET to send sensitive information—use POST instead.
- Include files

  - Must be placed outside of virtual roots with proper ACLs implemented
  - Should be renamed to .asp
- Dangerous C++ functions should be replaced
- HTML editors, debuggers, and all similar utilities must be removed from production Web servers.
- If using Visual C++, code should be compiled with -GS and debug builds compiled with -RTC1.
- Ensure no directories are protected with DACLs of Everyone Full Control.
- Ensure the application code does not reference internal server names or usernames.
- Ensure error messages do not provide sensitive information (filenames, stack traces, connection strings, etc.).
- The application should guard against
  - Cross-site scripting
  - Injection attacks
- Limit the directories and permissions accessible by scripts.
- Do not require a MAPI profile to send mail.
- Do not rely on HTML for parameter checking (for example, maxlength).
- Remove all comments from HTML on production servers.

Authentication

E-commerce authentication must meet these requirements:

- HTTP Basic authentication and Microsoft's Passport must not be used. Forms authentication over HTTPS is acceptable, but Windows authentication is preferred.
- Encryption must be used to protect authentication data, and the no cache option should also be used.
- Persistent cookies may not be used to store authentication data. Encryption must be used to protect temporary stored credentials in cookies, hidden tags, etc.
- Unattended processes must not run under an account with administrative privileges.
- Do not allow users to access the application through a non-designated entry point, such as a bookmark or fully qualified URL.
- Authentication must happen on the server side, not on the client side.
- Users must log in each time to use any application; persistent authorization must not be used.
- Application must limit simultaneous logins.
- Allow multiple users to use the same application on a single terminal server.

Input Validation

E-commerce input validation must meet these requirements:

- Apply the approach of only allowing valid input instead of eliminating invalid input throughout the application.
- Allowable character list must be defined per application.
- Use a list of allowable characters instead of a list of forbidden characters to validate data.
- Ensure input validation ignores null bytes and does not interpret as end of character.
- Never pass unchecked user input to file system commands.
- Utilize programming languages that incorporate bounds checking for buffers, such as Java or C#.

User Session

E-commerce user sessions must meet these requirements:

- Random session IDs must be utilized.
- User sessions should time out after 60 minutes of inactivity.

- Logouts must cause all session artifacts (ID, cookie, etc.) to be cleared.
- Users should be re-authenticated in order to gain access to the application after all session disconnects.
- A privacy statement must be displayed on the home page of all Web sites and applications.

Change Control

E-commerce change control must meet these requirements:

- Software development and testing must occur on systems not located in the production environment.
- All production software modifications must be approved by management prior to production deployment.
- Developers must not have access to production environments.