Password Policy

Purpose

This document establishes the corporate policy and standards for passwords at Landstar Title Agency, Inc..
This policy

- Identifies minimum password security requirements for all information systems including networks, applications, data stores, and any other electronic resource to which access is granted by the use of a password
- Applies to all users, applications, and systems with an account (or any form of access) that supports or requires a password on any system managed by or on behalf of Landstar Title Agency, Inc.

Policy

All employees are responsible for following the standards defined in this document when configuring, managing, or using any form of access to company information resources.

System Configuration Requirements

Information systems, such as applications, operating systems, and telephony systems (where applicable), must be configured to use Windows Authentication or programmatically meet the equivalent of these Windows operating system settings:

- Prohibit reuse of passwords for a minimum of 12 password change periods.
- Users must change their passwords at least every 90 days (excluding Windows Service Accounts).
- Passwords must have a minimum length of 8 characters and contain characters from at least 3 of these 4 categories (otherwise known as strong passwords):
  - Uppercase letters (A - Z)
  - Lowercase letters (a - z)
  - Numbers (0 - 9)
  - Special characters (for example, !, $, #, or %)
- Allow 5 failed password logon attempts before system lockout.
- Set minimum password age to one day.
- Set account lockout duration to 15 minutes.
- Where applicable, leverage Group Policy Object (GPO) or another mechanism to enforce system configuration requirements, with these additions:
  - Prohibit “store passwords using reversible encryption.”
  - All logon attempts must be registered according to the defined audit log configuration settings.
- Password protect computer screen savers.

Administrative Accounts

Administrative accounts must adhere to these standards:

- All accounts with administrative privileges must be protected with a strong password.
- If an employee has an administrative account, the password for each administrative account must be unique and cannot be the same as the password used for the employee’s regular account.
- Passwords for each account must be different from the password used for any non-Landstar Title Agency, Inc. account.

- When an employee with administrative access to routers, switches, and firewalls terminates employment with Landstar Title Agency, Inc., all console passwords must be changed.

Password Protection

All passwords

- Must be treated as sensitive and confidential information and not shared with anyone
- Must not be used by anyone other than the account owner
- Must never be written down, stored online, left in voice mail, or stored anywhere in an office or on any computer system without an authorized encryption method
- And their associated user names may not be written together in the same communication
- That are electronically communicated must be set to immediately require a password change on first use

Unless written approval from management is obtained, users cannot circumvent password entry with auto logon, application remembering, embedded scripts, biometric devices, or hard-coded passwords in client software.

Servers

All servers owned by or operated on behalf of Landstar Title Agency, Inc. must be configured and managed according to these minimum security standards

- All servers must have unique user names and strong passwords assigned to all users.
- Windows server-specific passwords must adhere to these standards:
  - The “password never expires” option is not allowed on any account, except an approved service account.
  - Password must meet complexity requirements and must be enabled.
  - Require users to change their password every time an administrator enters a new password for their account.
  - Require a unique username and password for each Windows user.
  - Do not send unencrypted passwords when connecting to third party servers.
  - Require passwords for all accounts.
- UNIX server-specific passwords must adhere to these standards:
  - Default passwords for privileged accounts must be changed immediately upon installation.
  - Knowledge of the root level passwords (UID=0) must be restricted to the UNIX system administrators.
- SQL server-specific passwords must adhere to these standards:
  - Always use a strong password for the system administrator (sa) account.
  - Enable the audit events Audit App Role Change Password and Audit Login Change Password.

Routers and Network Devices

All passwords on routers and network devices must

- Be changed from any factory default to a strong password
- Have service password encryption enabled
- Be encrypted using Cisco’s MD5-password encryption algorithm (4 routers NVRAM)
- Use MD5-encrypted passwords (for telnet, console, auxiliary, and enable)
- Be documented and known only to network administrators

Firewalls

All firewall passwords must

- Use the MD5 hash
- Be at least 12 characters long
- Be changed at least every 180 days
- Be known only by approved and designated firewall administrators
- Be different than router and switch passwords
- Use unique access and privilege-level (enable) passwords

Note: SNMP community name strings must also comply with these standards, but must not match firewall passwords.

Handheld Devices – See Mobile Devices Policy

Databases

Database passwords must not be imbedded in application code or files.

Default Passwords Supplied by Vendors

Use of default, vendor-supplied passwords can result in unauthorized access, serious disruption of operations, and loss of revenue. Default passwords are well-known and easily-determined via public information.

All vendor-supplied default passwords supplied with hardware (such as routers, switches, PBX, and gateway components) or software (such as operating systems, databases, and applications) must be changed or disabled before any system is put into production. Systems may not possess any non-standard or undocumented mechanism for access.

Suspected Password Compromise

Users who suspect their account or password has been compromised should

- Report the incident to their manager
- Change all passwords immediately

Windows Service Accounts

Windows service accounts must adhere to these standards:

- All service accounts must be reviewed by senior management once every 6 months. Audit evidence must be kept on file to confirm review has been conducted.
- Approved service accounts are the only accounts that may use the “password never expires” setting.
  - All service account passwords must be manually rotated at least every 180 days
  - Any exceptions must be approved through the Managing Exceptions Process.
  - Users must be prohibited from authenticating as a service account

Telephony Systems

Voice mail system passwords and personal identification numbers (PINs) must meet these configuration and usage standards:

- Administrator passwords must be constructed to contain a combination of alpha-characters and numerics (excluding * and #) with a minimum of 8 total characters.
- Voice mail PINs must be a minimum of 4 digits.

- Accounts must be automatically locked after 5 failed logon attempts.
- Accounts must be unlocked by telephone system administrators.
- PIN Reset Failed Sign-In Attempts for voice mail access must be set to 30 minutes or longer.

Auditing:

System administrators must perform periodic password protection audits on all systems with the findings reported to management.

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