Anti-Virus/Malware Policy

Purpose

This document establishes the corporate policy and standards for anti-virus/malware protection on any system owned by Landstar Title Agency, Inc or connected to the Landstar Title Agency, Inc. network (any network owned by or operated on behalf of Landstar Title Agency, Inc).

Policy

Current corporate-approved virus/malware protection software must be installed and enabled on all

- Corporate-owned systems
- Systems that connect to the Landstar Title Agency, Inc network, regardless of physical location (for example, VPN and remote associates)
- Messaging systems (message-level and server-level protection) Internet proxies/Secure Web Gateways

Users will not remove or disable virus/malware protection software from running on any system. All anti-virus/malware security measures must be implemented according to the standards defined in this document.

Standards

Refer to these sections in this policy for system-specific standards:

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

Standards for Servers and Workstations

Approved Software

AVG and Malwarebytes are the only approved anti-malware software protection solution for servers and workstations (desktops and laptops) owned by Landstar Title Agency, Inc or connected to the Landstar Title Agency, Inc network. Anti-malware products include software such as anti-virus, anti-spyware, and host intrusion prevention.

With prior approval from management, special purpose anti-malware tools may be installed to handle unique situations, provided [Sophos Endpoint] existing anti-malware tools are not removed or disabled and the special purpose tool is uninstalled after use.

Exception: With approval from the management and IT Security management, non-company owned systems can run with a current anti-malware solution other than the company approved solution.

AVG and Malwarebytes Configuration

An approved solution must be installed on all servers and workstations and configured through the management console to

- Perform a complete local drive scan of all files once per 7-day period
- Automatically update to the latest anti-virus signature file and engine once per day
- Prevent inadvertent/deliberate disablement
- Protect against buffer overflow attacks
- Auto-disinfect (auto-clean) a virus upon detection, when possible
- Log all virus incidents
- Alert in real time
- Automatically scan actively accessed files (via an on-access scanner)
- In addition to the requirements above, workstations must perform an e-mail scan of all actively accessed e-mail messages and attachments
- Perform a start-up scan of memory, master/boot records, and system files

Host intrusion prevention software must be configured to

- Enable intrusion prevention system functionality
- Prevent high severity attacks
- Log all detections
- Alert in real time

Standards for E-mail Servers

Approved Anti-Virus Software

Any enterprise e-mail server owned by Landstar Title Agency, Inc or connected to the Landstar Title Agency, Inc network must use a messaging-level anti-virus protection package known as Sophos to protect individual e-mail accounts and public folders at the messaging level.

Updating Messaging-Level Anti-Virus Software

Messaging-level anti-virus software must be updated on a regular basis. In the event of a virus outbreak, more frequent updating than regularly scheduled may be required.

Upgrading Messaging-Level Anti-Virus Software

Messaging-level anti-virus software must be upgraded on all e-mail servers within 5 days of a new engine release. This upgrade will be tested and coordinated by IT e-mail system administrators.

Application upgrades, which may occur once or twice each year, are deployed in phases across all e-mail servers after their stability has been verified by IT e-mail system administrators.

Messaging-Level Anti-Virus Software Configuration

Messaging-level anti-virus software must be configured to

- Automatically scan e-mail inbound to and outbound from the server (via an on-access scanner)
- Automatically update to the latest anti-virus signature file once per 24-hour period
- Automatically check for anti-virus engine upgrades on a weekly basis
- Prevent inadvertent/deliberate disablement
- Delete a virus-infected e-mail upon detection, when possible
- Log all virus incidents
- Alert in real time
- Allow filtering of incoming e-mail traffic by subject line or header or attachment

Standards for Internet Proxies/Secure Web Gateways

Approved Anti-Virus Software

All Internet proxies must have at least one commercial anti-virus engine enabled. Multiple engines are preferred.

Updating Internet Proxy/Secure Web Gateway Virus Definitions

Virus definition files must be updated at least once per 24 hour period.

Internet Proxy/Secure Web Gateway Configuration

Internet proxies/secure Web gateways must be configured to

- Use Web reputation scoring to
  - Block sites with very poor reputations
  - Allow sites with very good reputations
  - Scan all content for threats for sites with reputations in between very poor and very good
- Log all detections
- Automatically check for virus definition updates