Security Incident Response Policy

Purpose

This document establishes the corporate policy and standards for responding to suspected or known breaches of the privacy or security of restricted and/or confidential information at Company Name.

Policy

All Landstar Title Agency, Inc. employees are responsible for immediately reporting to management suspected or known breaches of the privacy or security of restricted and/or confidential information.

The Landstar Title Agency, Inc. Legal and/or Compliance Officer determines when to convene an Information Security Incident Response Team (ISIRT); however, it will generally be necessary for all "significant" or "high-visibility" incidents. If an ISIRT is convened, the Landstar Title Agency, Inc.plan document must be consulted, and the elements appropriate to the individual incident must be used.

The Landstar Title Agency, Inc. Legal and /or Compliance Officer will notify the Department of Financial Services within 72 hours of determining that a cyber event materially harms normal operations. On February 15 of each year, we send a statement to the Superintendent of the Dept. of Financial Services covering the prior year. In this statement we certify that we are in compliance with the regulations set forth in section 500.17 of 23 NYCRR500.b

Furthermore,

Note: It is not necessary to convene an ISIRT for every privacy and information security incident since many incidents are small and routine, requiring only a single responder.

Significant or High Visibility Incidents

Classifying an information security incident as "significant" or "high visibility" is inherently subjective; however, examples of such incidents include, but are not limited to

- Incidents involving key Landstar Title Agency, Inc. personnel such as executive management
- Incidents for which a press release may or will be issued, or media coverage is anticipated
- Incidents likely to result in litigation or regulatory investigation
- Incidents involving criminal activity
- Any other incident that is likely to involve reputational, regulatory, and/or financial risk to Landstar Title Agency, Inc. of which senior/executive management should be aware

Security Incidents

A security incident may involve any or all of the following:

- A violation of information and/or electronic device security policies and standards
- Unauthorized information and/or electronic device access
- Loss of information confidentiality
- Loss of information availability
- Compromise of information integrity
- A denial of service condition against data, network, or electronic device
- Misuse of service, systems, or information
- Physical or logical damage to systems
- Web site defacement
- Social engineering incidents (physical or logical)

- Any incident that could undermine confidence and trust in the company

Examples: Security incidents may include the presence of a malicious application, such as a virus; establishment of an unauthorized account for an electronic device or application; unauthorized network activity; presence of unexpected/unusual programs; or electronic device or paper document breach or theft.

Legal Counsel

Legal counsel must be consulted to identify possible conflicts of interest in any ISIRT investigation. In particular, individuals or teams may not lead investigations within their own areas of responsibility. Legal counsel should be consulted to determine if the investigation will proceed under the direction of counsel and attorney-client privilege. If so, counsel may establish particular procedures for communication and documentation. Counsel should also be consulted regarding possible law enforcement involvement, and/or the need for forensic investigation.

Notifications

The ISIRT is responsible for notifying affected individuals and/or regulatory agencies based on data elements that are individually identifiable, and current international, federal, and/or state laws or regulations requiring notification. Landstar Title Agency, Inc.policy regarding breach notification must also be considered, as well as the risk of harm to the individuals impacted by the breach. In some cases, even though notification may not be required by law, it may be prudent to notify affected individuals. The rationale to notify or not to notify must be clearly documented.

Investigating Incidents

The ISIRT must ensure adequate resources are assigned to conduct the investigation, and that they are sufficiently independent to avoid the appearance of a conflict of interest. For electronic incidents, designated IT resources shall conduct the initial forensic investigation, and interact and coordinated continuously with the ISIRT.

Containment Strategy

A containment strategy must be implemented that will limit the damage to the organization. The containment strategy must include contact information for various personnel who may become involved in incident response. Containment may involve a combination of technical controls, such as network and system disconnects, as well as media and communications to the public and to staff, depending upon the scope of the breach.

Note: Although the preservation of evidence is important, while an incident is active, containment takes precedence.

Communication

Communication of incidents should be handled on a need-to-know basis, especially early in the process.

Preservation of Evidence

The ISIRT is responsible for ensuring that evidence is preserved and each incident is adequately documented. “Adequate” documentation stands on its own without requiring further explanation.

Proper preservation of evidence requires establishment of chain of custody procedures prior to an incident. Any electronic evidence should be properly tracked in a documented and repeatable process.

Preservation of evidence is also required for the purposes of insurance coverage and failure to do so may limit or impact insurance recovery.

Incident Documentation

A full-time resource should be dedicated to adequately document the decisions that are made, and the actions taken, particularly for larger incidents as soon as the need for an ISIRT is identified. Documentation should consider these objectives:

- Prove no other systems (forensic data) should be considered by the analysts and verify the complete inventory of systems that are in-scope.
- Validate potentially affected areas were identified and addressed using accurate and repeatable measures.
- Validate the details of notification clearly met due diligence.

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