Computer Accounts Management Policy

Purpose

This document establishes the corporate policy and standards for managing user and administrator accounts and controlling access to the Landstar Title Agency, Inc network (any network owned by or operated on behalf of Landstar Title Agency, Inc).

Policy

Anyone who configures, creates, manages, or uses administrator or user accounts on any Landstar Title Agency, Inc system or network device (including, but not limited to databases, routers, OS, or e-mail) is responsible for following the standards defined in this document.

User account access on the Landstar Title Agency, Inc network must be based on the principle of least privilege. All users at all times should operate with as few privileges as possible, having access to only information and resources that are necessary. Any such access must be based on an individual's demonstrated need to view, add, change, or delete data.

Authorization

To set up a user account, the employee's manager must send an e-mail request to the appropriate IT support personnel defining the access required. The e-mail request must be archived for 12 months for audit purposes.

All Windows resource, service, firewall, router, domain, and Exchange accounts with administrative privileges must be reviewed and approved by an IT Senior Manager

- Before they are set up
- Quarterly

All Landstar Title Agency, Inc administrators must have a satisfactorily completed background check and a signed non-disclosure agreement maintained by Human Resources (HR).

Enterprise Administrators

Employees with IT administrative roles must have a separate account containing the privileges required to administer network systems. The account should

- Be named with the existing user ID and a suffix of AD (for example, USERIDAD)
- Only have permissions to administer IT resources and must not be used for routine work or personal use

For more information, see Password Policy.

Transfers

Employees who transfer within Landstar Title Agency, Inc are allowed to keep their Windows account. Any permissions that were previously assigned to the account must be removed and new permissions assigned based on the employee's new access requirements.

Rehires

Any employee who leaves Landstar Title Agency, Inc and then is rehired must have a new Windows account created.

Separation of Employment

Managers must immediately notify HR when an individual separates employment from Landstar Title Agency, Inc.

HR should notify IT Management promptly as account disabling for separation of employment must be completed immediately to disallow unauthorized access.

Revocation of Access by HR

HR reserves the right to contact managers and the parties directly involved with revoking access to cancel an employee's access at any time.

Password Requirements – see Password Policy

Routers, Switches, and Firewalls

IT senior management approval is required when granting employees administrative access to firewalls, routers, and switches. When an employee with administrative access to routers, switches, and firewalls terminates employment with Landstar Title Agency, Inc, all console passwords must be changed.

Inactive Accounts

Any authentication account on the Landstar Title Agency, Inc network that has not been accessed within the last 60 days is considered inactive and will be automatically disabled.

Authentication accounts that remain inactive for 120 days will be deleted.

This table describes actions taken based on the duration of account inactivity.

Inactivity Duration	Actions
61–120 days	User accounts are automatically disabled. **Note:** User-specific data (for example, e-mail and files on the home directory) are detached from the account and preserved up to 60 days. Resource and service accounts are automatically disabled, unless the account was placed on a pre-approved exceptions list by IT senior management.
More than120 days	Accounts are deleted. All related user-specific data is automatically deleted.

Re-Enabling Accounts

This table describes when inactive accounts can be re-enabled.

If account status is…	And employee status is…	Then account…
Disabled	Active	Can be re-enabled with manager approval
	Terminated	Can be re-enabled with HR and/or Compliance approval
	Rehired	Cannot be re-enabled; new account must be created
Deleted	Active	Cannot be re-enabled; new account must be created

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