Account Management Policy

Purpose

This document establishes the corporate policy and standards for managing user and administrator accounts and controlling access to the AREA Title network and any network owned by or operated on behalf of AREA Title.

Policy

Anyone who configures, creates, manages, or uses administrator or user accounts on any AREA Title 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 AREA Title 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 or administrator account or add additional access to existing accounts requires the employee's manager to send an e-mail request and approval to the appropriate IT support personnel defining the access required. The e-mail requests and approvals 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 AREA Title 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 AREA Title 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 AREA Title 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 AREA Title.

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 AREA Title, all console passwords must be changed.

Inactive Accounts

Any authentication account on the AREA Title 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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

Anti-Fraud/Corruption Policy

Purpose

This document establishes the corporate policy and standards for ensuring the highest ethical standards at AREA Title by providing a corporate framework aimed at the prevention, detection, and mitigation of known or suspected fraud, corruption, or related misconduct.

Policy

Fraud and corruption will not be tolerated by AREA Title employees either within the company or in conjunction with, or targeted towards AREA Title employees, customers, partners, suppliers, or vendors.

All complaints of suspected fraudulent behavior will be investigated.

Every effort will be made to ensure appropriate accountability for business processes and when fraud/corruption is suspected or detected, sufficient resources shall be employed to gather evidence to support disciplinary action, prosecution, and/or the recovery of losses and costs wherever possible.

Definitions

Corruption—Activity in which someone acts in an official capacity, contrary to the interests of their sponsoring company/organization, for personal gain or for some form of improper gain/advantage for someone else.

Fraud—Knowingly using false statements of fact with the intent to deceive resulting in financial or personal gain or damage to another individual or organization. The theft of property belonging to AREA Title, a person, or persons internal to the company, but where deception is not used is also considered *fraud* for the purposes of this policy.

The terms *fraud* and *corruption* are not restricted to monetary or material benefits.

Risk Assessments

On an as-needed, but no less than annual basis, the President, in consultation with AREA Title department managers, will generate a report reviewing the effectiveness of the policy concerning the company's susceptibility to fraudulent and/or deceptive practices.

Responsibilities

All AREA Title employees have a responsibility to

- Understand and apply all fraud-related policies/procedures
- Assist with the prevention and detection of fraud, corruption, or related misconduct
- Report suspected fraud, corruption, or related misconduct

Preventative Measures

Fraud prevention accounting procedures must be developed and maintained in relation to all escrow account reconciliations, cash management, credit card usage, and commercial transactions.

Fraud prevention/awareness strategies shall include, but are not limited to

- Requiring background checks for applicants where required by the duties of a particular position
- Contacting employment references
- Checking/verifying transcripts, qualifications, and other certification documentation
- Requiring on-boarding and continuing training/staff development on

  - Fraud prevention and detection
  - The protection of non-public personal information (NPPI)
  - Ethics
- Requiring vendors/contractors to abide by all AREA Title fraud-related policies/procedures

Detection and Reporting

AREA Title will cooperate with the police and/or appropriate governmental agencies in any investigation of suspected fraud or corruption. Irrespective of any police investigation or action, AREA Title management will form its own view under employment law as to what actions might be appropriate for those involved in the fraud or related misconduct.

All reports for suspected fraud, corruption or related misconduct should be made in good faith. Retaliation and retribution will not be tolerated against any employee who reports suspected fraudulent or corrupt activities. Persons who make reports which are malicious, knowingly false, or unjustly likely to damage the reputation of another may face disciplinary action.

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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

Anti-Virus/Malware Policy

Purpose

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

Policy

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

- Corporate-owned systems
- Systems that connect to the AREA Title 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 [Company Name] computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

Standards for Servers and Workstations

Approved Software

Microsoft Security Essentials is the only approved anti-malware software protection solution for servers and workstations (desktops and laptops) owned by AREA Title or connected to the AREA Title 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 Microsoft Security Essentials 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.

Microsoft Security Essentials 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 AREA Title or connected to the AREA Title network must use a messaging-level anti-virus protection package 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

Application Security Policy

Purpose

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

Policy

All applications developed or purchased at AREA Title 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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

General Requirements for All AREA Title 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 90 days 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 AREA Title 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 AREA Title 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.
- Credit card processing must be performed by an authorized third-party payment service.
- 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.

Background Investigations Policy

Purpose

This document establishes the corporate policy and standards for conducting background investigations at AREA Title.

Policy

Background checks will be conducted

- Using industry-recognized agencies and sources
- In accordance with federal and local laws, including confirming the individual's supplied
  - Employment authorization information
  - Date of birth
  - Full legal name

Prior to hiring, AREA Title will conduct background investigations

- On all employee candidates
- When appropriate, on contractors, sub-contractors, consultants, and temporary employees
  Note: AREA Title may require third party vendors to conduct the background investigations for contractors and temporary workers using the standards defined in this document.
- On officer appointees, required by customer contracts
- On employees who hold or are being considered (via transfers or promotions) for positions that include
  - Financial responsibilities
  - Increased access to sensitive/confidential data
  - Driving responsibilities

AREA Title evaluates the results of background investigations on a case-by-case basis.

Condition of Employment

Cooperation and compliance with all provisions of this policy is a condition of employment or continued employment with AREA Title.

These actions may result in disqualification from employment with AREA Title or, if discovered after the commencement of employment, may result in termination:

- Refusal to authorize a background investigation conducted in accordance with applicable law
- Falsification of an application or background check authorization document
- Failure to disclose a criminal conviction

Scope

AREA Title complies with the Fair Credit Reporting Act and applicable federal and state laws. Where permissible, background investigations may include, but are not limited to

- Consumer credit reports
- Criminal reports
- Department of Motor Vehicle or Department of Transportation checks
- Social Security Number validation
- Employment reports
- Education reports

Criminal Reports

Criminal background reports will reflect activity, at a minimum, of the 7 years prior to the date of the report. A longer time period may be reported where permitted by law. Where a candidate has resided in different national or international jurisdictions during the 7 year minimum investigation period, separate checks may be conducted for those territories to a minimum of the current and one previous jurisdiction.

All convictions are evaluated on a case-by-case basis and are reviewed for relationship to the job responsibilities based on certain criteria, as are applicable to the job responsibilities, which may include but are not be limited to

- Dishonesty
  - All fraud including, but not limited to
    - Credit card fraud
    - Embezzlement
    - Bad/worthless checks
  - Fraudulent trading
  - Possession of stolen property
  - Forgery and counterfeiting
  - Proceeds of crime offenses
  - Theft
  - Bribery and corruption
  - Money laundering
  - Concealment of property
  - Trespassing with intent to steal (burglary)
  - Blackmail/extortion
- Business
  - Any offense involving computer misuse
  - Organizing or engaging in illegal work
  - Economic/corporate/business espionage
- Other
  - Producing, supplying, importing, or trafficking controlled drugs/substances
  - Terrorism
  - Pretrial diversions (US) for disqualifying crimes
  - Deferred adjudications (US) for disqualifying crimes
  - Felony (US) or host country equivalent serious crimes

Rehires

Where employees end their employment with AREA Title and are subsequently rehired by AREA Title, the former employees shall be considered new candidates for employment (irrespective of the amount of time that has elapsed) and a new background investigation shall be required prior to rehiring.

Record Keeping

For audit and compliance purposes, AREA Title shall, where permitted by law, maintain and store (or shall cause to be maintained and stored) all background investigation documentation for a period of not less than 2 years, that verifies that background investigations were performed on candidates in compliance with the version of this policy then in effect and to the extent permitted by law.

Predicated upon pre-authorization from the candidate or employee, AREA Tilte may permit, upon reasonable request, the auditing of such documentation by AREA Title clients and customers, limited to the scope of the business engagement between AREA Title and such requesting client or customer and to candidates and employees directly involved in providing contractual services to such requesting client or customer.

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 AREA Tilte computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

Backup and Media Retention Policy

Purpose

This document establishes the corporate policy and standards for backup and media retention at AREA Title Agency, Inc.

Policy

To ensure the availability and reliability of data stored on backup media, all production and development servers located within any facility managed by or on behalf of AREA Title

- Must be backed up a minimum of 5 times per week
- Must have a full backup successfully completed at least once per month

All databases and application servers associated with production systems must be restored from backup media every 12 months without errors. Alternatively, a smaller list of systems to be restored may be approved by management.

Note: To validate the integrity of restores for databases that exceed one terabyte in size, partial restores of the databases will be conducted.

Offsite Storage Facility

Backup media must be sent to a management-approved, secure offsite storage facility at least twice per week. Media storage facilities must

- Be located at least 3 miles from the server(s) being backed up
- Include protection from
  - Explosion and fire
  - Magnetic fields
  - Theft and vandalism
  - Natural disasters (earthquakes, floods, hurricanes, tornadoes)
- Provide environmental controls for
  - Temperature
  - Humidity

Online Backup Services

Third-party online backup hosting providers storing AREA Title data via must meet the standards defined in this document where applicable.

Transporting Backup Media

Backup media containing confidential data must be encrypted or transported by a secured commercial data management transportation company, also approved by senior management. Backup media completed between offsite pickup dates must be protected in an access-restricted location, such as a fireproof safe on-campus, until the next backup media pickup.

Backup Logs

Backup logs must be reviewed daily Monday through Friday excluding official company holidays. Any unsuccessful scheduled backup must be reported the following business day along with the steps taken to resolve the unsuccessful backup. The last successful full and differential backup dates must be included in

each failed backup log entry. Any backup that fails 2 or more consecutive times must be escalated to the appropriate senior management group.

All backup logs and reports must be maintained for 12 months for audit purposes. Refer to this table for backup media retention requirements.

Backup	Server	Retention
Daily	Exchange-Hosted	Daily back-up off site
	Windows-Daily	Retain 3 weeks, then recycle

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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

Business Continuity Policy

Purpose

This document establishes the corporate policy and standards for ensuring continued operations of critical services in the event of a disruption to regular operations at AREA Title.

Policy

Each department at AREA Title is responsible for ensuring a detailed business continuity plan is in place for all services and mission critical applications.

Each office/division is responsible for creating and maintaining their individual business continuity plans. All plans must

- Provide detailed instructions for the resumption of critical operations for each business location (see Continuity Plan immediately below)
- Be reviewed, updated, and tested once per year to ensure accuracy

All third-party data centers must be Service Organization Control (SOC) certified.

Continuity Plan

Each continuity plan must include

- Detailed plans for resuming operations at a hot site or alternative office, including
  - Standby hardware and connectivity necessary to establish critical operations
  - Access to the most recent versions of business systems software required for critical operations
  - Access to the most recent data backups
- Contact information for all personnel, clients/customers, and vendors
- Business continuity plan training and maintenance schedules
- A list of the critical business functions and processes including
  - Recovery time objectives (RTO) for critical systems (that is, the amount of time required to recover critical systems)
  - Recovery point objectives (RPO) for critical data (that is, the maximum amount of critical data that can be lost)

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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

Customer Complaint Policy

Purpose

This document establishes the corporate policy and standards for responding to customer complaints made against AREA Title.

Policy

All AREA Title employees are responsible for promptly and seriously addressing any complaint made by a customer against AREA Title or its employees. Agents receiving a communication from a customer (via phone, fax, e-mail, or in person) with a complaint must

- Remain courteous at all times and, under all circumstances, refrain from engaging in argumentative behavior with the customer regardless of the nature of the complaint or the conduct of the customer.
- Completely and accurately document information pertinent to the complaint in writing
- Escalate the call to a senior call specialist, secondary support associate, or supervisor if
  - It becomes clear the customer wishes to pursue a formal complaint
  - The agent feels unable to further assist the customer
- Not confirm, discuss, or reveal the borrower's-specific information without confirmation of the caller's identity as the borrower in question and written authorization on file

Privacy

Federal privacy laws prohibit the release of borrower-specific information to anyone without

- The borrower's expressed, written authorization or
- Order of a court of competent jurisdiction

Documentation

All formal complaints against AREA Title or its employees must be documented using the AREA Title Customer Complaint Form.

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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

Data Retention Policy

Purpose

This document establishes the corporate policy and standards for retaining business documents at AREA Title.

Policy

All AREA Title employees are responsible for securely maintaining electronic and paper-based business documents, including both original documents and reproductions, for as long as they are needed to conduct business or as required by state retention laws, whichever is longer.

Legal Services and Human Resources reserve the right to extend retention periods when required for legal purposes or pending litigation.

Business Documents

Business documents are any electronic or paper-based business products or documents required during the course of business including, but not limited to, title, escrow, insurance, and claims documents.

Data Security/Disposal – See Non-Public Information Security and Disposal Policy

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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

External Audits Policy

Purpose

This document establishes the corporate policy and standards for coordinating all external audits performed at AREA Title.

Policy

All external audits, assessments, and reviews involving AREA Title must be coordinated with the Office president, who will assign a compliance liaison.

Compliance Liaison

The Compliance Liaison is responsible for

- Disseminating notifications to affected departments concerning audit purpose and scope
- Coordinating all external audit activities
- Ensuring that external auditors receive all information requested and the data gathered and reported on is complete, factual, and presented fairly
- Issuing coordinated responses on all audit reports and inquiries
- Keeping senior management fully informed of current external audit activities
- Minimizing the impact of audits on programs and operations
- Avoiding, to the extent possible, the redundancy of audit activity

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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

IT Security and Computer Usage Policy

Purpose

The availability, integrity, and confidentiality of computerized information is critical to the success of any company. This document establishes the corporate policy and standards for protecting all computerized communications, data, and information at AREA Title.

Policy

All communications, data, and information created on, received through, or sent over AREA Title information resources (including the Internet/intranet, phones, e-mail, and instant messaging (IM) systems) are the property of AREA Title and must be protected, commensurate with their value and sensitivity to disclosure, at all times according to the standards of behavior defined in this document. AREA Title reserves the right to determine the appropriate use and suitability of any of this information. Users have no rights to, title on, interest in or ownership of such information, nor should they have any expectation of privacy or confidentiality on any AREA Title information system.

Definitions

This list defines terms used within this document.

- **Electronic information** is any data or information stored or transmitted in electronic form, regardless of format.
- **Non-public information (NPI)** includes any paper or electronic record produced by or in the possession of AREA Title that contains
  - Competitive data including, but not limited to, proprietary financial information, source code for software applications, data on acquisitions or mergers, and customer lists
  - Legally sensitive data including, but not limited to, personnel information, legal investigations, and pending lawsuits
  - Personal technology data including, but not limited to, specific system architecture information, IP addresses, user names/IDs, personal identification numbers (PINs), market IDs, certificates, security codes, access codes, password information, and answers to password hint questions (for example, mother's maiden name)
  - Non-public and personally identifiable information about an individual including, but not limited to, date of birth, Social Security numbers, passport identification numbers, driver's license numbers, state identification card numbers, credit or debit card numbers and expiration dates, bank account numbers, bank routing information, credit information, loan numbers and applications, account histories, and related personal and financial information
  - Any other non-public, proprietary or secret information, or information identified as confidential
- **Information resources** include anything used to process electronic information including, but not limited to
  - Hardware (for example computers, fax machines, telephones, pagers, network communication devices, and communication wiring)
  - Media (for example hard drives, compact disks, tapes, USB drives, memory cards, and computer diskettes)
  - Software (any executable electronic code, ranging from large e-mail systems to small word processing macros)

Personal Use of Information Systems

AREA Title information resources are intended primarily for business purposes; however, incidental personal use of these systems is permissible if approved by management.

Personal use of information systems is strictly prohibited if it

- Consumes more than a trivial amount of resources that could otherwise be used for business purposes
- Interferes with work productivity
- Preempts any business activity
- Intentionally interferes with the normal operation of the network (including the propagation of computer viruses and sustained high-volume network traffic)
- Is associated with any for-profit outside business activity

Protection of NPI

NPI must be protected at all times by following these best practices:

- Electronic media and hardware, as well as portable computing devices (for example laptops and smart phones), that contain NPI, must remain under personal control when not secured by a locking device.
- Portable computing devices and computer media containing NPI must fully encrypt the disk or the files containing NPI.
- Computer accounts on AREA Title systems must be password protected.
- Computers must be logged off or password protected (locked) when unattended for more than 15 minutes.
- NPI must reside in protected directories while stored on any hardware device.
- Virus detection software must be installed on all computing devices and remain up-to-date.
- Critical files must be backed up on a routine basis to a network directory or encrypted removable media device.
- Any e-mail or documents containing NPI sent to recipients outside the AREA Title organization must be password protected or encrypted before being transmitted over the Internet. The password to open the document must be provided in a separate communication such as a new e-mail, phone call, or instant message or by using WinZip or Microsoft Office password protection.

Ownership

All items issued by AREA Title (for example computers, phones, ID badges, and credit cards) are the property of AREA Title and are to be returned immediately upon termination of the contract or employment.

Conditions of Use

Use of AREA Title information resources must always comply with federal, state, and local law and all AREA Title policies. Use of these resources is strictly prohibited if it involves

- Any purposes identified by AREA Title as being inappropriate and/or not authorized by AREA Title management
- Knowingly using the Internet/intranet, e-mail, or instant messaging (IM) to create, view, post, store, send, or receive any material that is inappropriate, indecent, offensive, hateful, vulgar, obscene, profane, defamatory, harassing, infringing, intimidating or discriminatory, or which is intended to annoy, harass, or intimidate another person

- Transmitting any unauthorized advertising, "junk mail," "spam," "chain letters," or "pyramid schemes," or any material that contains viruses or other computer code designed to interrupt, overload, destroy, or limit the functionality of any software, hardware, or equipment
- Falsifying or deleting any author attributions, legal or other proper notices, or proprietary designations of the origin or source of software or other material
- Soliciting non-company business for personal gain or profit (including the selling of products) or engaging in commercial activities other than those expressly permitted by AREA Title management
- Conducting AREA Title business using third-party Internet, e-mail, IM utilities, or any communication solution other than those approved and provided by AREA Title
- Sending, receiving, revealing, publicizing, or otherwise transmitting commercial software, copyrighted materials of any kind, trade secrets, proprietary information, or similar materials without prior approval from the General Counsel
- Impersonating any person or entity including, but not limited to, a AREA Title employee or officer, or falsely stating or otherwise misrepresenting an affiliation with a person or entity
- Examining, altering, or using another person's files, output, or other usernames or identifiers without explicit authorization
- Expressing or furthering individual personal opinions or political philosophies, representing personal opinions as those of AREA Title or purporting to represent AREA Title without explicit authorization, or holding one's self out in any way other than honestly or accurately
- Obtaining or attempting to obtain access to another company's systems or data without proper authorization
- Attempting to, or successfully altering, destroying, adding, or connecting to AREA Title resources without proper authorization

Unauthorized Software

All software must be approved by the appropriate AREA Title management before it can be loaded onto any company-owned equipment. Additionally, these types of software may only be utilized with the documented approval of the Director/Manager of Information Technology and/or Security:

- Security testing or hacking/cracking applications
- Network sniffing or packet capture utilities
- Spyware or forensics software
- Peer-to-peer data sharing software

Controlled Access to Information Systems

All access requests for information resources must be approved by the manager of the individual requiring access and submitted to the Information Technology (IT) department for processing. In all cases, the individual approving the access must be someone other than the individual making the system access changes, and a record of the approval must be kept for no less than one year for audit purposes. Users are directly responsible for all activity performed using their individually-assigned computer accounts.

Monitoring and Examination of Information

AREA Title business systems are considered private and not-for-public forum; therefore, guarantees of free speech under the First Amendment do not apply. At any time and without prior notice, AREA Title management reserves the right to access and monitor all communications and electronic files and to divulge this information to law enforcement officials and regulatory agencies as required by state and federal regulations.

In order to monitor or examine an employee's e-mail account or electronic files, a manager must request approval from AREA Title Human Resources (HR). HR will work with appropriate IT personnel to implement approved requests. All requests must be held in the strictest confidentiality by all personnel involved.

Reporting Incidents and Potential Violations

AREA Title encourages the reporting of all perceived incidents of misconduct (which includes potential violations of policy), regardless of the offender's identity or position. All reports of suspected incidents are taken seriously and investigated. To the extent practicable, AREA Title will keep reports confidential; however, absolute confidentiality is not promised and cannot be assured.

Any employee or other individual who believes he or she has been subjected to, witnessed, or made aware of misconduct should immediately report the incident to management along with violations related to information resources or information technology networks; however, if the reporting person is not identified, AREA Title might not be able to respond appropriately to the reported concern. There is no penalty for reporting an alleged incident in good faith.

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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

Managing Exceptions Policy

Purpose

This document establishes the corporate policy and standards for managing exceptions to policies at AREA Title.

Policy

Any exception to an approved AREA Title policy must be requested in writing by a senior manager and approved according to documented processes. Exceptions may not exceed 12 months in duration and then must be reevaluated for exception renewal.

A log of exception requests must be maintained for audit review and to insure eventual remediation.

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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

Managing Exceptions Process

Purpose

This document describes the process for managing exceptions to policies at AREA Title.

Applies To

All AREA Title employees are responsible for following this process.

Policy Exception Request Process

When an exception to a policy is needed, follow this process.

Stage	Description
1	Requestor completes a Policy Exception Request Form and e-mails it to their manager.
2	Requestor's manager reviews and approves or denies the request. If the request is • Denied, the manager informs the requestor. Process ends. • Approved, the manager e-mails it to the office president. Go to Step 3.
3	Office president reviews the request and e-mails approval or denial to the • Requestor's manager • Policy exception administrator
4	Requestor's manager informs requestor of final approval/denial by the office president.
5	Policy exception administrator files the request and final approval/denial decision in the policy exception request log.

Policy Exception Review Process

Once a month, the policy exception administrator reviews expired policy exceptions and

- Verifies that expired exceptions have been remediated and are no longer needed, or
- Informs the expired exception requester that the exception needs to be renewed

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

Policy Exception Request Form

Use this form to request policy exceptions and document final approval or denial of the request.

Requestor: (Individual initiating the request)

1. Complete the form and save it.
2. E-mail the completed form to your manager for approval.

Requestor's Manager:

1. Review the policy exception request.
2. If denied, inform the Requestor.
3. If approved, e-mail your approval statement with the form attached to the office president for approval.
4. Inform the Requestor of final approval/denial by the Office President.

Office President:

1. Review the policy exception request approved by the Requestor's Manager.
2. E-mail your approval or denial statement with the form attached to the policy exception administrator and the Requestor's Manager.

Policy Exception Administrator:

File the form and the final approval/denial decision in the policy exception request log.

IMPORTANT:

- Policy exceptions will NOT be renewed automatically.
- To renew a policy exception, the Requestor must submit a new exception request before the original granted policy exception expires.

Date of Request:		Request Type:	New ☐ Renewal ☐

REQUESTOR INFORMATION	
Requestor's Name:	

EXCEPTION INFORMATION
Policy or policies affected (mandatory field):
Application Name (if applicable):
Exception(s) requested:

Reason for exception(s):
Impact if the exception is denied (customer, hardware, software, business process, etc.):
Remediation plan to eliminate the need for exception(s) in the future:
Duration of exception-If approved, the exception will expire in
☐ 1 month ☐ 6 months
☐ 3 months ☐ 12 months
Estimated remediation date:

APPROVAL INFORMATION	
Name of Requestor's Manager approving exception:	
Type Name:	***Type Approval Date:***
Name of Office President reviewing exception:	
Type Name:	***Type Approval/Denial Date:***
☐ Approved	☐ Denied
I certify I have the proper authority to approve this request. I understand that approvals granted by unauthorized personnel may result in disciplinary actions up to and including termination.	

Use only if approved

- - - POLICY EXCEPTION ADMINISTRATOR USE ONLY - - -	
Date Received:	
Date Approved:	
Approved By:	
Expiration Date:	
Date to Review:	
Processed By:	

Use only if denied

- - - POLICY EXCEPTION ADMINISTRATOR USE ONLY - - -	
Date Received:	
Date Denied:	
Denied By:	
Processed By:	

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

Mobile Devices Policy

Purpose

This document establishes the corporate policy and standards for mobile devices, including any handheld device such as a smartphone or tablet used to communicate, transmit, or store electronic information belonging to AREA Title.

Policy

All AREA Title employees who synchronize data between AREA Title and a mobile device are responsible for following the standards defined in this document.

Mobile devices will enforce these controls:

- A power-on and an inactivity password
- A policy to wipe (erase all data from the device) after 10 invalid password attempts
- A maximum inactivity time-out of 15 minutes
- A minimum password length of 4 characters
- 256-bit AES full disk encryption
- Remote wipe capability
- Encrypted communication with AREA Title e-mail server
- Activity auditing
- Unsupported operating systems will not be allowed to connect to AREA Title systems
- Where configurable must only allow application installs from official vendor application store or mobile device management solution

Approved Devices

Only approved devices are allowed to connect to AREA Title systems. For information on the currently approved devices, contact the IT department.

Backups

The IT department will provide instructions or assist with initial backup setup. Users are responsible for verifying backups are occurring on a regular basis.

Lost or Stolen Devices

Any employee whose corporate-provisioned or personally-owned mobile device that has access to AREA Title systems is lost or stolen must

1. Contact the IT department or vendor and request the device to be remotely wiped
2. After receiving confirmation that the device has been wiped, contact the purchasing department or service provider to report the loss

Devices must be wiped to securely erase corporate data including but not limited to apps, media, and data. Regular backups will allow easy restoration of apps, data, and settings.

Transferring Devices

Before transferring ownership of any mobile device that has been connected to AREA Title systems, users must contact the IT department so a remote wipe can be initiated.
Note: Depending on device capabilities, wiping may completely erase all data including personal data.

Terminating Employment

Before an employee terminates employment and takes any mobile device that has been connected to AREA Title systems, the employee's manager must contact the IT department so a remote wipe can be initiated.
Note: Depending on device capabilities, wiping may completely erase all data including personal data.

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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

Non-Public Information Security and Disposal Policy

Purpose

This document establishes the corporate policy and standards for securing and disposing non-public information (NPI) at AREA Title.

NPI includes any paper or electronic records produced by or in the possession of AREA Title including, but not limited to, title, escrow, mortgage, insurance, and claims documents that contain

- Competitive data including, but not limited to, proprietary financial information, source code for software applications, data on acquisitions or mergers, and customer lists
- Legally sensitive data including, but not limited to, personnel information, legal investigations, and pending lawsuits
- Personal technology data including, but not limited to, specific system architecture information, IP addresses, user names/IDs, personal identification numbers (PINs), market IDs, certificates, security codes, access codes, password information, and answers to password hint questions (for example, mother's maiden name)
- Lender-supplied Disclosure Data including data transmitted on Good Faith Estimates, Truth-in-Lending Disclosures, and Closing Disclosure forms, when mandated by the Consumer Financial Protection Bureau, whether supplied in an electronic document or data format
- Loan-related documents including the FNMA 1003, Note, Deed of Trust, etc. known as "Loan Docs" transmitted by the lender to the settlement agent in preparation for borrower signing
- Non-public and personally identifiable information about an individual including, but not limited to, date of birth, Social Security numbers, passport identification numbers, driver's license numbers, state identification card numbers, credit or debit card numbers and expiration dates, bank account numbers, bank routing information, credit information, loan numbers and applications, account histories, and related personal and financial information
- Any other non-public, proprietary or secret information, or information identified as confidential

Policy

All AREA Title employees are responsible for following the standards defined in this document.

Physical Security

Physical security for NPI must adhere to these standards:

- Restrict access to NPI to authorized employees only.
- Institute a "clean desk" policy requiring employees to close and secure files containing NPI when they are away from their desks.
- Secure onsite documents, portable devices, and electronic media containing NPI in a desk, file cabinet, or locked room outside of normal business hours.
- Secure offsite documents in a commercial storage facility that is
  - Climate controlled
  - Equipped with a monitored security alarm
- Prohibit or control the use of removable media such as USB drives and external backup drives.
- Require USB drives and other removable devices storing company data to be encrypted.
- Prohibit NPI from being accessed with or stored on non-approved electronic devices.
- Use only secure delivery methods when mailing NPI. Secure delivery methods include
  - Inter-office mail—Sealed envelopes

  - External mail—Registered mail services (FedEx, UPS) with sealed envelopes and signature requirement
    Note: Large quantities of protected documents may only be shipped using a professional document management company that has been approved by management.
- Send faxes only to private or secure fax machines.
- Pick up and dispose of printer, fax, and copier output in a timely manner.
- Never leave documents, portable devices, or electronic media containing NPI in an unlocked vehicle or where they are visible from outside a locked vehicle.
- Never leave any item containing NPI unattended in a hotel room, conference room, reception area, or any other location that can be accessed by others.

Electronic Security

Electronic access or storage of NPI must adhere to these standards:

- Computer policies
  - Use strong passwords (8+ characters including numbers, symbols, and upper and lowercase letters) and require frequent password updates.
  - Require password-activated screen savers when employees leave their workstation.
  - Establish dedicated workstations for electronic banking.
  - Install and maintain up-to-date firewall, anti-virus, and other intrusion prevention systems.
  - Use data encryption for transmitting files containing NPI.
- Electronic communication such as e-mail, instant messaging, and texting.
  - NPI and money transmitted electronically must be protected in transit by 128-bit or stronger Advanced Encryption Standard (AES) encryption or via password-protected attachments or other secure methods.
  - Omit or obscure NPI.
  - Use secure methods of transmission such as secure e-mail offered by providers such as RPost, Barracuda Networks, Ironport, etc.
- Portable storage
  - Encrypt or password-protect documents containing NPI on portable devices such as laptops, smart phones, USB drives, and external backup drives.
  - Store portable devices securely to prevent theft or unauthorized access.
  - Secure portable devices as one would a computer.
- Websites
  - Enable encryption for company websites that collect NPI. When using trusted third-party websites, users should check for the padlock icon at the bottom right of the browser window or look for "https" instead of "http" in the address bar.
  - Avoid entering NPI in third-party websites that you do not trust. Especially when following links, users should always check the address bar to ensure that they have not been directed to a look-alike website.
  - Do not use public file storage or transfer services such as LeapFILE, FindMyFile, SendSpace, or DropBox for any files containing NPI.
  - Download, install, and update computer software only when instructed by the company's IT department.
- File servers
  - Physically secure all servers in a locked room with limited and controlled access.

- Limit access to directories, file shares, databases, and critical applications containing NPI to only those persons who require access for legitimate business purposes.
- Ensure that server backups are encrypted.

Disposal

Federal law requires companies that possess NPI for a business purpose to dispose of the NPI, after business and regulatory retention requirements have been met, in a manner that protects against unauthorized access to or use of the information in connection with its disposal.

Some examples of appropriate disposal policies include

- Establish a document retention period that sets timelines for the disposal of NPI based on state requirements.
- Burn, pulverize, or shred hard copy records using a commercial shredder or a shredding company that has been approved by management.
- Destroy, degauss, or securely overwrite with a multiple-pass process all electronic files on decommissioned equipment including, but not limited to, computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, and cell phones.

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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

Notary Services Policy

Purpose

This document establishes the corporate policy and standards for ensuring consistent business practices in the notarization of documents required in the business operations at AREA Title.

Policy

All AREA Title employees and managers specifically designated by AREA Title to perform notarial acts in connection with AREA Title business practices are responsible for following the standards defined in this document.

Bonding/Licensing Fees

Notaries shall maintain licensing in good standing and comply with all requirements according to the statutes of the state of Ohio (and Michigan) and provide evidence of such licensing and compliance to AREA Title upon request.

Notaries must be bonded for the current statutory requirement. Additional errors and omissions coverage is not required with the bond for AREA Title.

Fees for bonding and licensing of AREA Title designated notaries will be paid for by AREA Title; however, notary employees who perform notary services other than as a designated notary for AREA Title must procure a separate bond and errors and omissions policy at their own expense.

Duties of Notaries

Notaries will acquaint themselves with publications outlining standard notary procedures and all processes and requirements set forth by AREA Title.

The primary function of the notary is to prevent fraud; therefore, these practices will be followed at all times.

- The document signer must appear before the designated notary for the purpose of the notarization.
- The designated notary must
  - Review the document
  - Properly verify the identity of the signer
  - Place the signer under oath or affirmation
  - Determine the signer's awareness and understanding of the transaction
  - Ensure the signer personally signs the document (signature stamps are not permitted)
  - Have the signer sign the record/journal book
  - Record all details ot the transaction in the record/journal book
  - Fill in, sign, and stamp/seal the document with a notarial certificate

Notaries must decline notarizing documents presented by persons lacking proper identification or documents of questionable origin or purpose.

Non-Company Documents

Notaries may notarize documents not related to AREA Title business purposes at their discretion if the act is occasional and does not interfere with the performance of company business.

Record Keeping

Notary publics are required to maintain a record/journal of every notarial act performed. AREA Title has the right to, and shall regularly inspect designated notary publics' record/journal entries.

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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

Password Policy

Purpose

This document establishes the corporate policy and standards for passwords at AREA Tile.
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 AREA Title

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 telephone 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-AREA Title account.
- When an employee with administrative access to routers, switches, and firewalls terminates employment with AREA Title, 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 AREA Title 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 strongest supported encryption

- 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

Telephone 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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

Privacy and Information Security Audit and Oversight Policy

Purpose

This document establishes the corporate policy and standards for audit and oversight of company activities to ensure information and data remains secure at AREA Title.

Policy

Privacy and information security procedures at AREA Title must be reviewed as needed, or at a minimum, annually in an effort to prevent the improper use and/or disclosure of confidential information. Information security issues include, but are not limited to

- Evaluating current risk assessment, management, and control activities
- Addressing service provider arrangement concerns
- Addressing known security breaches, violations, or other concerns
- Analyzing summary results of security testing procedures
- Providing recommendations for program modifications or enhancements

Risk Assessment

The President continually monitors and evaluates confidential corporate and customer data to account for business process changes, technology changes, emerging vulnerabilities and threats, and other relevant factors that may impact the security or integrity of this information. These assessments are designed to

- Identify technical and business process vulnerabilities
- Determine the effectiveness of existing company policies and procedures

Additionally, the President maintains a risk assessment system comprised of various anticipated risk factors, weighted with their forecasted probability, resulting in a calculated risk value for a variety of technology systems, business processes, and data sources. The risk assessment system is reviewed and updated on a quarterly basis.

Oversight

To ensure that due diligence is exercised in selecting Service Providers, the President verifies that

- All agreements with third-party service providers
  - Are reviewed by legal counsel
  - Include provisions for safeguarding AREA Title company and customer information
- All service provider contracts include a corporate confidentiality agreement
- Service providers provide proof that they have met the requirements of the Gramm-Leach-Bliley privacy act and any other state or federal regulatory privacy requirements that may apply
  Note: Acceptable forms of proof are service provider audit reports, Service Organization Control (SOC) reports, or compliance tests performed by AREA Title.

Monitoring

AREA Title will monitor its systems and applications to reasonably ensure that safeguards are being followed and to quickly detect and correct breakdowns in security. An appropriate level of monitoring will be based on the potential impact and probability of the risks identified, as well as the sensitivity of the information provided. Monitoring will include

- Sampling
- Performing system checks
- Reviewing system access reports
- Reviewing logs
- Conducting audits
- Performing any other reasonable measures to adequately verify that information security controls, systems, and procedures are working

Auditing

AREA Title will periodically conduct audits of

- Activity logs
- Performance data
- Unauthorized access
- Viruses and other malicious code
- Any other indicators of integrity loss

AREA Title and its third party contractors shall cooperate with and avail themselves of any central services providing support for and/or review of these activities as well as perform more sophisticated procedures such as penetration testing and real-time intrusion detection.

Vulnerability Testing

Because the loss of integrity of any device or server on a network provides a platform for launching attacks on the integrity of the entire network, AREA Title will periodically scan the AREA Title network and network servers for vulnerabilities using software tools designed for this purpose.

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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

Remote Access Policy

Purpose

This document establishes the corporate policy and standards for management of all remote access to any network owned by or operated on behalf of AERA Title.

Policy

All remote access tools must be approved by management.

Only Virtual Private Network (VPN) solutions approved by management may be used for remote access to the AREA Title network.

Applications may not be administered remotely via any public access solution, unless the connection is through a secure VPN using 2-factor authentication.

Use of remote access is restricted to the support of legitimate business work. Remote access should only be granted on a case-by-case basis and may be monitored or audited.

Files transferred during the remote viewing process must not be saved to personal computer drives.

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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

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 AREA Title.

Policy

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

The AREA Title 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 AREA Title plan document must be consulted, and the elements appropriate to the individual incident must be used.

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 AREA Title 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 AREA Title 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. AREA Title 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 coordinate 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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

Security Training and Awareness Policy

Purpose

This document establishes the corporate policy and standards for security training and awareness to mitigate information security risks at AREA Title.

Policy

All AREA Title employees with access to protected data and information assets must participate in information security awareness training. No less than annually, information security training will be provided to individuals whose job functions require specialized skill or knowledge in information security.

The President is responsible for managing and implementing the AREA Title information security program which includes, but is not limited to

- Promoting the understanding and importance of information security and individual responsibilities and accountability
- Developing general information security standards, procedures, and guidelines and targeted, product-specific information where necessary
- Ensuring background checks and credit reports are conducted before hiring employees who will have access to non-public information. See Non-Public Information Security & Disposal Policy.
- Requiring employees and independent contractors to sign an agreement to follow AREA Title information security policies
- Ensuring access to non-public personal information (NPI) is limited to employees and independent contractors who have a business reason to see the information
- Developing policies governing the appropriate use of company technology
- Training employees on appropriate security measures and responses to attacks or suspected attacks
- Imposing disciplinary measures for breaches of company policies and processes concerning NPI
- Developing procedures preventing terminated employees from having access to confidential information

Security Training and Awareness

The President promotes on-going information security awareness via

- Distribution of employee manuals to all employees requiring annual sign-off of agreement and compliance
- Regular articles published in corporate newsletters
- Information security bulletins distributed to all employees to address security policy modifications, security alerts, and other urgent security issues

Note: When necessary, the information security program must provide or coordinate training for individuals whose job functions require special knowledge of security threats, vulnerabilities, and safeguards. This training must focus on expanding knowledge, skills, and abilities for individuals who are assigned information security responsibilities.

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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

Social Media Policy

Purpose

This document establishes the corporate policy and standards for social media use at AREA Title and defines the requirements for professional and personal use of social media.

Social Media

Social media is a form of interactive electronic communication used to create and share content through text, images, audio, and/or video and enable people to socially interact online. Social media consists of web-based and mobile technologies that facilitate interaction, information-sharing, and relationship-building among users.

Social Media may include, but is not limited to

- Social networking sites (such as Facebook, Myspace, LinkedIn, Bebo, Yammer)
- Video and photo sharing websites (such as Flickr, YouTube)
- Blogs, including corporate blogs and personal blogs
- Blogs hosted by media outlets
- Microblogging services (such as Twitter, Tumblr)
- Wikis and online collaborations (such as Wikipedia)
- Forums, discussion boards and groups (such as Google Groups)
- Podcasting
- Online multiplayer gaming platforms (such as World of Warcraft, Second Life)
- Instant messaging (including SMS)
- Geo-spatial tagging (Foursquare)

Policy

All AREA Title employees and contractors are responsible for following the standards defined in this document when using social media for personal or professional use.

Reporting Inappropriate Use

Employees or contractors who notice inappropriate or unlawful content online relating to AREA Title, or content that may have been published in breach of this policy, should immediately report the circumstances to Michael Repass by phone at (419) 242-5485 or e-mail at documents@areatitle.com.

Professional Use of Social Media

Before engaging in social media as a representative of AREA Title, employees or contractors must be authorized to comment. To become authorized to comment in an official capacity, employees and contractors must have been through a trial usage period, obtained approval from their manager and/or from Michael Repass.

Once authorized to comment as a company representative, employees or contractors *must*

- Disclose they are an employee or contractor of the company, and use only their own identity, or an AREA Title approved official account or avatar
- Disclose and comment only on information classified as public domain information
- Ensure that all content published is accurate and not misleading and complies with all relevant departmental policies

- Ensure they are not the first to make an announcement unless specifically given permission to do so
- Comment only on their area of expertise and authority
- Ensure comments are respectful of the community in which they are interacting online
- Adhere to the Terms of Use of the relevant social media platform/website, as well as copyright, trademark, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws

Those authorized to comment as company representatives, ***must not***

- Post or respond to material that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright or trademark, constitutes a contempt of court, breaches a Court suppression order, or is otherwise unlawful
- Use or disclose any confidential or secure information including, but not limited to
  - Personal or transactional information about consumers (buyers, sellers, borrowers)
  - Personal, transactional or contractual information about customers (lenders, real estate agents)
  - Non-public information (NPI) of any kind (loan numbers, social security, etc. – see NPI policy)
- Make any comment or post any material that might otherwise cause reputational damage or cause disrepute to AREA Title, its customers (Lenders, Realtors, Attorneys, etc.) or their employees and agents, or consumers (buyers, sellers, borrowers)

Moderation of Company-Produced Social Media

The site owner must ensure the moderation policy is clear when inviting comments from the public on a company website or social media platform.

All company website activity including any social media must be approved by the Michael Repass.

Personal Use of Social Media

AREA Title recognizes that employees and contractors may wish to use social media in their personal lives. This policy does not intend to discourage or unduly limit their personal expression or online activities.

Employees and contractors should

- Recognize the potential for damage that could be caused directly or indirectly to AREA Title in certain circumstances from personal use of social media by those that can be identified as a company employees or contractors
- Comply with this policy to ensure that the risk of such damage is minimized

Employees and contractors are personally responsible for the content they publish in a personal capacity on any form of social media platform. When in doubt, they should seek guidance from the AREA Title on how to comply with these obligations:

Where comments or profiles can identify someone as a company employee or contractor, company employee and contractors ***must***

- Only disclose and discuss publicly available information
- Ensure that all content published is accurate and not misleading and complies with all relevant departmental policies
- Expressly state on all postings identifying them as a company employee the stated views are their own and are not those of the company
- Be polite and respectful to all people interacted with
- Adhere to the Terms of Use of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment, and other applicable laws

Where comments or profiles can identify someone as a company employee or contractor, company employee and contractors ***must not***

- Post material that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright or trademark, constitutes a contempt of court, breaches a court suppression order, or is otherwise unlawful
- Imply they are authorized to speak as a representative of the company or give the impression that the views they express are those of the company
- Use their company e-mail address or any company logos or insignia
- Use their company email address or any company logos or insignia that may give the impression of official support or endorsement of their personal comments
- Use the identity or likeness of another employee, contractor or other member of the company
- Use or disclose any confidential information obtained in their capacity as an employee or contractor of the company
- Imply they are authorized to speak on behalf of the company, or give the impression that any views they express are those of the company
- Use or disclose any confidential information or personal information obtained in their capacity as an employee or contractor of the company
- Post material that is, or might be construed as, threatening, harassing, bullying, or discriminatory towards another employee or contractor of the company
- Make any comment or post any material that might otherwise cause damage to the company's reputation or bring it into disrepute

Reasonable and Unreasonable Personal Use of Company Resources

When accessing social media using the AREA Title Internet, intranet, or extranet systems, employees and contractors must use these resources in a reasonable manner that does not interfere with their work, that is appropriate, and that does not constitute excessive access.

Examples of *reasonable use* include

- Participating in working groups on the company's intranet
- Updating Facebook status and posting messages during a lunch break

Examples of *unreasonable and/or unacceptable use* include

- Posting any material that is fraudulent, harassing, threatening, bullying, embarrassing, sexually explicit, profane, obscene, racist, sexist, intimidating, defamatory, or otherwise inappropriate or unlawful.
- Spending hours using social media that is not related to work, during work hours.

Copyright

Employees and contractors must respect copyright laws and fair use of copyrighted material and attribute work to the original author/source wherever possible.

Harassment and Bullying

Workplace bullying and harassment includes any bullying or harassing comments employees make online, even on their own private social networks or outside of work.

Abusive, harassing, threatening, or defaming postings are in breach of AREA Titles Policy, and may result in disciplinary action up to termination.

All employees are expected to treat their colleagues with respect and dignity and must ensure their behavior does not constitute bullying and/or harassment.

Defamation

Employees and contractors should refrain from publishing material that may cause injury to another person, organization, association, or company's reputation, and should seek further guidance if publication of such material is thought to be necessary.

Offensive or Obscene Material

Material may be offensive or obscene and may infringe relevant online classification laws if it is pornographic, sexually suggestive, harassing, hateful, racist, sexist, abusive, or discriminatory. Employees and contractors must refrain from accessing offensive or obscene material.

Contempt of Court

Employees and contractors must obtain approval before referring to pending court proceedings to avoid publishing material that may have a tendency to prejudice those proceedings, in particular, material that will be part of the evidence in those proceedings.

Employees and contractors must make enquiries about any applicable court suppression orders before commenting on any court proceeding (past, pending, or current).

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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Depending on the circumstances, non-compliance with this policy may constitute a breach of employment or contractual obligations, misconduct, sexual harassment, discrimination, or some other infringement of the law.

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

Standards of Conduct Policy

Purpose

The Standards of Conduct Policy is designed to detect and prevent unethical conduct and violations of laws/regulations at AREA Title.

Policy

All AREA Title employees are responsible for following the standards defined in this document.

Attendance

Each employee is required to be present and ready to work on time from the start to the end of each workday, according to his or her work schedule assigned by management. If an employee is unable to report to work for any reason, he or she is required to inform the manager or designee no later than 30 minutes from the commencement of the scheduled start time, unless otherwise directed by management. An employee must also notify the manager or designee as soon as possible if he or she needs to leave for any reason before the conclusion of the scheduled workday.

If an employee fails to report to work without proper notice for 3 consecutive scheduled workdays, AREA Title will presume the employee has voluntarily resigned and the employee will be terminated from employment, unless state or local law defines a longer period prior to termination.

Attire and Personal Representation

All AREA Title locations observe a business casual dress code unless otherwise directed by management. With appropriate notice, professional business attire may be required (for example, for special events, closings or customer meetings). Employee attire must project an appropriate image for conducting business with customers. Management reserves the right to determine the appropriateness of the attire and personal representation.

Each employee must maintain proper hygiene and utilize good judgment in determining dress and appearance. If an employee's personal representation poses an issue (for example, inappropriate attire, body odor, or offensive perfume/cologne), management may address the concerns with the employee. If an employee is asked to leave work to address a personal representation issue, time lost is not considered paid work time.

Confidentiality

Each employee is responsible for using his or her best judgment to safeguard and manage confidential information at all times. Examples of appropriate behavior related to protecting confidential information include, but are not limited to

- Only disclosing confidential information to individuals with an authorized business need for access (for example, to perform job responsibilities)
- Holding conversations including sensitive information in enclosed areas
- Using sealed envelopes to mail confidential information with acknowledgement of receipt requested
- Disposing of confidential information through appropriate method (for example, shredding printed documents and wiping computer media) when no longer needed to support operations and/or to meet state, legal, or tax requirements

Discrimination

Each employee is required to abide by all state and federal equal employment opportunity regulations.

Harassment

Harassment is prohibited and will not be tolerated in the workplace or in any work-related setting including, but not limited to

- Business trips
- Business meetings
- Business-related social events

Harassment may consist of conduct including, but not limited to verbal, non-verbal, or physical conduct designed to threaten, intimidate, or coerce other employees to the extent that the conduct is regarded as unwelcome, impairs the employee's ability to perform his or her job, or creates a hostile work environment. Examples of harassing conduct include offensive epithets; slurs or negative stereotyping; threatening, intimidating, or hostile acts; and jokes or written/graphic material that denigrates or shows hostility or dislike toward an individual or group.

Sexual Harassment

It is against AREA Title policy for any employee, male or female, to sexually harass another employee by making unwelcome sexual advances or making sexual favors or other verbal or physical conduct of a sexual nature as a condition of an employee's continued employment; making submission to or rejections of such conduct the basis for employment decisions affecting the employee; or creating an intimidating, hostile, or offensive work environment by such conduct.

Misconduct

Violation of any policy at AREA Title (whether stated herein or provided elsewhere by AREA Title) is considered misconduct. Although it is impossible to identify every possible instance of misconduct, the following is a partial list of infractions that AREA Title considers misconduct:

- Unprofessional or otherwise inappropriate behavior
- Falsification of any documentation required for employment including, but not limited to, employment applications and time reporting records (one's own or another's)
- Theft, fraud, gambling, or carrying prohibited weapons or explosives as defined in the Weapons section of this document, or violation of criminal laws on company premises
- Interfering with the performance of fellow employees
- Falsification of any claims of inappropriate conduct
- Insubordination or refusal to comply with instructions or failure to perform reasonable duties as assigned
- Excessive unauthorized absenteeism or abuse of attendance, paid time off, or leave of absences
- Unauthorized or improper use of business expenses
- Failure to adhere to any rules designated by management regarding pets (other than service animals), dependents, or other visitors in the work place
- Impersonation of any person or entity including, but not limited to, a AREA Title employee or officer, or false statement or misrepresentation of an affiliation with a person or entity
- Representation of personal opinions as those of AREA Title or purporting to represent AREA Title without explicit authorization
- Failure to comply with AREA Title procedures or standards

Retaliation

An employee may not retaliate or attempt to retaliate against an employee who has, or who is associated with an employee who has

- Reported a suspected or alleged misuse of company property or assets at AREA Title
- Appeared as a witness, cooperated in, acted as investigator, or otherwise supported the investigation of any complaint against the company
- Filed or made a good faith complaint of alleged discrimination, harassment, sexual harassment, or violations of other federal, state, or local laws

Reporting Incidents and Potential Violations

AREA Title encourages the reporting of all perceived incidents of discrimination, harassment, misconduct, or retaliation, regardless of the offender's identity or position. All reports of suspected incidents shall be taken seriously and investigated. To the extent practicable, AREA Title will keep reports confidential; however, absolute confidentiality is not promised and cannot be assured.

Any employee or other individual who believes he or she has been subjected to, witnessed, or made aware of discrimination, harassment, sexual harassment, misconduct, or retaliation should immediately report the incident to management. Complaints may be anonymous, if so preferred; however, if the reporting person is not identified, the AREA Title might not be able to respond appropriately to the reported concern. There is no penalty for reporting an alleged incident in good faith.

Any employee who has been found by the AREA Title to have engaged in conduct inconsistent with policy will be subject to disciplinary and/or legal actions, up to and including termination.

Media Inquiries and Press Releases

Requests from media outlets should be immediately forwarded to the management. Under management discretion, officers of the company may have a direct relationship with local publications about positive community issues, articles, and advertisements where employees have assurance that adverse issues, claims, or investigations of the company or the closing or real estate industries are not involved.

All press releases must be managed by AREA Title and approved by the appropriate parties. All information released to the public must meet the standards for AREA Title strategies, management philosophies, style, and material concerns.

Outside Employment

Outside employment requires prior written management approval. Outside employment must not interfere with job performance or efficiency, involve the use of AREA Title resources or time, pose a conflict of interest, or in any way harm the business or reputation of AREA Title.

Security, Access, and Identification

Access needs for each employee are determined by management. If provided, employees are required to wear security badges while on work premises for identification and/or access purposes. Employees must follow any precautions provided to ensure security badges and AREA Title keys are protected and secure at all times. Where available, access may be monitored by card readers, video cameras, or other monitoring devices.

Smoking

Smoking is not allowed in any AREA Title buildings. Employees may only smoke in designated areas and must adhere to local and state regulations regarding smoking.

Social Media

While using social media outlets during or outside of work hours and on AREA Title or AREA Title equipment, employees must comply with all AREA Title policies.

These actions are permitted only with explicit prior written permission from management and AREA Title Marketing:

- Maintaining or posting social media content that implies AREA Title sponsorship or support
- Using AREA Title time, facilities, resources, or supplies to maintain or post content to social media outlets
- Maintaining or posting any logos or trademarks of AREA Title or related entities on social media outlets

Actions of prohibited behaviors related to the use of social media include, but are not limited to

- Concealing or attempting to conceal one's identity, such as through the use of an alias, while making any reference to AREA Title, its Officers, members of the Board of Directors, related entities, employees, or clients
- Expressing views on behalf of AREA Title, unless the content is provided verbatim from materials approved by the AREA Title for that purpose

Management reserves the right to require an employee to cease maintaining or posting to any social media outlet containing content in any way associated with AREA Title that it deems inappropriate.

Solicitation

An employee may not solicit for personal causes or events or distribute non-work-related information during work time or using company resources without prior management approval. Each employee should avoid making any other employee feel uncomfortable or compelled to participate or contribute through solicitation, and no employee should feel obligated to participate in these efforts. In addition, information posted on AREA Title bulletin boards, including electronic bulletins, must be of interest to the workplace, appropriate, limited to designated areas, and approved by management.

Phone and Mobile Device Usage

Each employee must limit phone usage for personal reasons (for example, calling, texting, emailing, and Web browsing) during working hours and comply with all applicable rules established by management. Whenever possible, personal use should be restricted to meal or rest periods. On work premises, disruptive ringers that may be overheard by customers or employees must not be used and professionalism must be maintained while on calls. Using AREA Title landlines to make personal long-distances calls is prohibited.

While driving a vehicle, employees are discouraged from using a mobile device (for example, calling, texting, emailing, and Web browsing) to conduct AREA Title business, and are responsible for using their best judgment in compliance with state and local laws. For safety reasons, an employee should pull off the road to a safe location before taking or making a call, retrieving or sending messages, and reading or responding to e-mails.

Camera and Video Recorder Usage

In restricted-access or other areas where there is an expectation of privacy (such as restrooms), every employee is prohibited from using a camera or video recorder including those available as mobile phone features. Unauthorized or unwelcome recording or photography of any AREA Title business, information or individuals is prohibited on work premises or work events.

Video cameras may be operated on work premises to help ensure the safety and security of individuals and business operations.

Weapons

Consistent with applicable law, every employee is prohibited from carrying a weapon during the course of performing their jobs, whether or not they are on AREA Title property. This applies even if employees are licensed to carry a handgun. Furthermore, this policy prohibits weapons at any company-sponsored function such as a party or picnic.

With approval of the highest ranking official of AREA Title, management may grant an exception to an employee to carry a weapon while working.

Any form of weapon or explosive restricted under federal, state, or local law is prohibited. Where required by law, AREA Title permits storage of firearms in personal vehicles.

An employee should contact his or her manager or AREA Title Human Resources with any questions about whether an item is considered a weapon under this policy. An employee is expected to verify ahead of time that an item is not defined as a weapon under this policy before having it in his or her possession while working, and the employee is solely responsible for any prohibited item.

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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary

Title Insurance and Settlement Services Policy

Purpose

This document establishes the corporate policy and standards for handling/processing title insurance and settlement documentation at AREA Title.

Licenses

State-mandated insurances/business licenses, registrations, corporate registrations (as applicable), or similar requirements must be effective and current.

Escrow Trust Accounts

All AREA Title employees are responsible for following these standards when processing real estate settlement transactions:

- Three-way reconciliation (escrow trial balance/book balance/reconciled bank balance) must be used at least once monthly when processing escrow trust accounts.
- State-mandated insurances/business licenses, registrations, corporate registrations (as applicable), or similar requirements must be effective and current.
- AREA Title must maintain appropriate written procedures and controls for escrow trust accounts allowing for electronic verification of reconciliation.
- Only those employees approved to authorize bank transactions may do so. If possible, dual authorizations should be implemented.
- Accounts must be properly identified as "escrow" or "trust" accounts.
- Outstanding file balances must be documented.
- Escrow funds and other funds must be separately maintained.
- Unless directed by the beneficial owner, escrow trust accounts must be maintained in federally insured financial institutions.
- Positive pay, Automated Clearing House (ACH) blocks, and international wire blocks must be used, if available.

Background Checks and Credit Reports

Background checks must be completed for all employees at least once every 3 years, going back 5 years for all employees who have access to customer funds. Credit reports must also be obtained at least once every 3 years for all employees who have access to customer funds.

Recording Documents

AREA Title will submit or ship documents for recording to the county recorder (or equivalent) or the person or entity responsible for recording within 2 business days of settlement, using electronic recording and shipment tracking when available. AREA Title will also verify that recordation actually occurred and maintain records of the recording information.

Title Policies

Title insurance policies should be delivered within 30 days of settlement if terms and conditions of title insurance commitment have been satisfied.

Professional Liability Insurance, Fidelity Coverage, and Surety Coverage

AREA Title will possess an amount of professional liability insurance from a carrier that is acceptable to the underwriter and in an amount not less than agreed to by the company's underwriting agreements.

When required by state law or contractual obligations, AREA Title will possess the required amount of fidelity bond coverage and/or surety bond coverage from a carrier that is acceptable to the underwriter in an amount not less than the amount required by state law or agreed to in the company's underwriting agreements.

AREA Title also ensures that closing protection letter coverage, where mandated by statute, will be issued in connection with the disbursement or that a statutory indemnity fund will be established to cover fidelity losses not otherwise covered by the protections afforded by the underwriter.

Complaint Resolution

AREA Title will maintain a standard complaint process that identifies the nature, scope, and specific transaction associated with the complaint as well as the resolution.

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 AREA Title computer network or business systems
- Formally reporting the incident to AREA Title senior management
- Termination of employment
- Any other action deemed necessary by AREA Title senior management

Review

AREA Title 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

Michael D. Repass

Attorney at Law

President

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary