ALTA’s Best Practices -- Sample Policies and Procedures

Pillar #3 – Information and Data Privacy

**INSERT LAW FIRM NAME HERE**

**Security Statement**

The Firm has taken measures to guard against unauthorized or unlawful processing of personal data and against accidental loss, destruction or damage. This includes:

* Adopting this information security policy
* Taking steps to control physical security (projects and staff records are all kept in a locked filing cabinet)
* Putting in place controls on access to information (password protection on files and server access)
* Establishing a business continuity/disaster recovery plan (including, at a minimum taking regular back-ups of its computer data files and this is stored away from the office at a safe location)
* Training all staff on security systems and procedures
* Detecting and investigating breaches of security should they occur

|  |  |
| --- | --- |
| **Policy** | **Best Practice Pillar #3: INFORMATION AND DATA PRIVACY – Adopt and maintain a written privacy and information security plan to protect Non-public Personal Information as required by local, state and federal law.** |
| **Name of Procedure** | Information Security (IS) Program Management |
| **Reference Number** | 3.01 |
| **Applicable Parties** | Firm ManagementPractice Manager[Privacy Officer]Firm IT ManagerEmergency Management Team[Third Party Service Providers – Attached Addendum] |
| **Effective Date** | Highlight this text, then type effective date here |
| **Supporting Documentation** | Add to, delete and/or modify the sample text below to describe documentation that evidences your firm’s compliance with this best practice. Delete the preceding sentence and this one before finalizing.Written policies including:* Network Usage Policy and user permissions for all employees and all systems,
* Clean Desk and Clean Office Policy
* Retention and Destruction Policy
* Data Breach Incident Reporting
* Business Continuity and Disaster Recovery
* Employee Training and Management
* Hardware and software maintenance
* Third party providers
* Website, social media and other Firm public sites

Vendor contracts and privacy statements for SaaS, software, hardware, email, shared document, records destruction and other services |
| **Procedures** | Add to, delete and/or modify the sample text below to describe the procedure followed by your firm to assure compliance with this best practice. Delete the preceding sentence and this one before finalizing.**3.01 Information Security (IS) Program Management**The Firm Manager has responsibility to for ongoing management, monitoring and implementation of policies and procedures adopted by Firm Management, and to make recommendations to Firm Management for updates and changes to data and information security policies and procedures as needed (at least annually), including:* Network Usage Policy (3.04 below), including
	+ logical access restrictions and user permissions for all employees and all systems (hardware, software and removable media),
	+ password access requirements
* Clean Desk and Clean Office Policy (3.04 below)
* Retention and Destruction Policy (3.05 below)
* Data Breach Incident Reporting (3.07 below)
* Business Continuity and Disaster Recovery (3.08 below)
* Employee Training and Management (3.03below)
* Hardware and software maintenance (3.04 below)
* Third party providers (3.06 below)
* Website, social media and other Firm public sites (3.04 below)
* Privacy Policy to be posted on Firm website and provided to all clients (3.04 below)
* Ongoing systems risk analysis, maintenance and review (3.02 below)

The Firm Management, in consultation with the Practice Manager and Firm IT Manager, will review all of the above data and information security policies and procedures:* at least annually,
* upon any significant change in available technology, industry requirements, Firm hardware or software, offices or procedures,
* in the event of a security breach or
* as required by significant clients of the Firm.

The Firm IT Manager will:(1) Maintain electronic records (below).(2) Maintain, monitor and continually update an electronic list, the Network Usage Policy, identifying:* All hardware (servers, computers, laptops, tablets, mobile devices, scanners, facsimile machines, copiers, etc.)
* All software (including closing, banking, email, data storage, firewalls, encryption, cloud storage, shared document, scanning, among others)
* The authorized uses for business purposes by job position
* The authorized user-employees with their individual levels of authority, dates of training
* Access to and control of network access and client information, including removable media (USB ports, CD/DVD drives, laptops) and
* Any records of violations or breaches.

(3) Monitor and enforce the requirements of the Firm’s data and information security policies and procedures and maintain applicable electronic records.(4) Assure that antivirus software runs automatically, along with real-time intrusion detection on all computers.(5) Assure that software (especially antivirus) patches and updates are installed timely when available.(6) Assure constant maintenance of network intrusion detection and prevention systems (firewall) to detect unauthorized intrusion to the systems from unknown sources, to automatically detect and log the event and notify the Firm IT Manager.(7) Assure that all computer processes are backed up to remote off-site storage at least daily.(8) Assure that all NPI information is permanently deleted from all hardware when decommissioned.(9) Monitor and maintain all Firm websites and social media sites |
| **Approved by / Date** | Highlight this text, then type name of person approving here | Highlight this text, then enter date of approval here |

|  |  |
| --- | --- |
| **Policy** | **Best Practice Pillar #3: INFORMATION AND DATA PRIVACY – Adopt and maintain a written privacy and information security plan to protect Non-public Personal Information as required by local, state and federal law.** |
| **Name of Procedure** | Risk Identification and Assessment |
| **Reference Number** | 3.02 |
| **Applicable Parties** | Firm ManagementPractice Manager[Privacy Officer]Firm IT ManagerEmergency Management Team[Third Party Service Providers – Attached Addendum] |
| **Effective Date** | Highlight this text, then type effective date here |
| **Supporting Documentation** | Add to, delete and/or modify the sample text below to describe documentation that evidences your firm’s compliance with this best practice. Delete the preceding sentence and this one before finalizing.Written policies including:* Network Usage Policy and user permissions for all employees and all systems,
* Clean Desk and Clean Office Policy
* Retention and Destruction Policy
* Data Breach Incident Reporting
* Business Continuity and Disaster Recovery
* Employee Training and Management
* Hardware and software maintenance
* Third party providers
* Website, social media and other Firm public sites

Vendor contracts and privacy statements for SaaS, software, hardware, email, shared document, records destruction and other services |
| **Procedures** | Add to, delete and/or modify the sample text below to describe the procedure followed by your firm to assure compliance with this best practice. Delete the preceding sentence and this one before finalizing.**3.02 Risk Identification and Assessment**The Firm Manager will report to Firm Management at least quarterly on review of Firm’s data and information policies and procedures and the status of internal and external risks which may affect protection of Firm NPI, including:* Location, storage, access, usage of NPI
* Analysis of any violations identified by firewalls, vulnerability / penetration testing, and mitigation efforts
* Employee training, monitoring and violations
* Network, software and hardware status and updates needed
* Updates recommended on Firm’s data and information policies and procedures

The Firm Manager will, at least monthly, or more frequently upon any breach or significant change in risk, obtain outside independent IT professional vulnerability or penetration testing for review of the Firm’s systems, and methods of storing, processing, transmitting and disposing of NPI, including internal and external potential threats or risks of unauthorized disclosure, misuse, alternation or destruction of NPI or other client information.The Firm Manager, in consultation with the Firm IT Manager, will monitor for risks or breaches on an ongoing basis.Any vulnerabilities will immediately be either remedied , mitigated or discussed with and addressed by Firm Management. |
| **Approved by / Date** | Highlight this text, then type name of person approving here | Highlight this text, then enter date of approval here |

|  |  |
| --- | --- |
| **Policy** | **Best Practice Pillar #3: INFORMATION AND DATA PRIVACY – Adopt and maintain a written privacy and information security plan to protect Non-public Personal Information as required by local, state and federal law.** |
| **Name of Procedure** | Employee Training, Management, and Responsibilities |
| **Reference Number** | 3.03  |
| **Applicable Parties** | Firm ManagementPractice Manager[Privacy Officer]Firm IT ManagerEmergency Management Team[Third Party Service Providers – Attached Addendum] |
| **Effective Date** | Highlight this text, then type effective date here |
| **Supporting Documentation** | Add to, delete and/or modify the sample text below to describe documentation that evidences your firm’s compliance with this best practice. Delete the preceding sentence and this one before finalizing.Written policies including:* Network Usage Policy and user permissions for all employees and all systems,
* Clean Desk and Clean Office Policy
* Retention and Destruction Policy
* Data Breach Incident Reporting
* Business Continuity and Disaster Recovery
* Employee Training and Management
* Hardware and software maintenance
* Third party providers
* Website, social media and other Firm public sites

Vendor contracts and privacy statements for SaaS, software, hardware, email, shared document, records destruction and other services |
| **Procedures** | Add to, delete and/or modify the sample text below to describe the procedure followed by your firm to assure compliance with this best practice. Delete the preceding sentence and this one before finalizing.**3.03 Employee Training, Management, and Responsibilities**The Firm Manager is responsible for the following:(1) Maintain a list of all employees, the Firm’s systems, software or Third Party Service Providers (see attached Addendum) for which the Firm has authorized access to records containing current or archived NPI, and the authorized purpose for which each such employee has such access based upon the legitimate business purpose for their job function. Each employee must have a unique user identification and strong password.(2) Conduct five year Background Checks at hiring and every 3 years thereafter for all employees with access (or potential access) to NPI, and assure access is not provided to any other employee. (3) Maintain electronic records, including completed background check reports, on each employee. Assure access is not allowed to any other employees.(4) Immediately terminate access to all internal and external data and information, as well as notify Third Party Service Providers, upon the employee’s termination.(5) Assure that all employees attend the appropriate mandatory training, at time of hiring and at least annually for all employees with access to NPI regarding * the importance of information security and Personal Information
* the ethical obligations for confidentiality of client files and information
* the proper use of Firm computer resources, information and passwords
* the control of information and procedures to prevent Personal Information disclosure to unauthorized parties and to prevent “snooping”
* mandatory Firm procedures for maintaining data and information security (3.04 below). file retention / destruction (3.05 below), data breach reporting (3.07 below) and business continuity / disaster preparedness (3.08 below)

(6) Annual update of employee signed agreement that they understand the Firm’s security procedures and agree to comply with them.(7) Monitor ongoing operations to assure that employees who violate the procedures will be disciplined and, when necessary, terminated. |
| **Approved by / Date** | Highlight this text, then type name of person approving here | Highlight this text, then enter date of approval here |

|  |  |
| --- | --- |
| **Policy** | **Best Practice Pillar #3: INFORMATION AND DATA PRIVACY – Adopt and maintain a written privacy and information security plan to protect Non-public Personal Information as required by local, state and federal law.** |
| **Name of Procedure** | Information Security |
| **Reference Number** | 3.04  |
| **Applicable Parties** | Firm ManagementPractice Manager[Privacy Officer]Firm IT ManagerEmergency Management Team[Third Party Service Providers – Attached Addendum] |
| **Effective Date** | Highlight this text, then type effective date here |
| **Supporting Documentation** | Add to, delete and/or modify the sample text below to describe documentation that evidences your firm’s compliance with this best practice. Delete the preceding sentence and this one before finalizing.Written policies including:* Network Usage Policy and user permissions for all employees and all systems,
* Clean Desk and Clean Office Policy
* Retention and Destruction Policy
* Data Breach Incident Reporting
* Business Continuity and Disaster Recovery
* Employee Training and Management
* Hardware and software maintenance
* Third party providers
* Website, social media and other Firm public sites

Vendor contracts and privacy statements for SaaS, software, hardware, email, shared document, records destruction and other services |
| **Procedures** | Add to, delete and/or modify the sample text below to describe the procedure followed by your firm to assure compliance with this best practice. Delete the preceding sentence and this one before finalizing.**3.04 Information Security****Physical security for each location:*** The Firm maintains secure points of entry to the building and any interior offices where NPI may be stored.
* A Visitor logbook is maintained. All visitors who will have access to areas containing NPI must enter their name, signature, organization represented, purpose of visit or name of person visited, date/time of arrival and date/time of departure.
* Security systems includes individual access codes or personal keys/fobs, as appropriate
* Vendors and visitors are escorted when passing through areas which may have NPI.
* Areas containing NPI are accessible only by employees who have undergone background checks or those escorted by them for legitimate Firm purposes only.

**Clean Desk Policy:*** Maintain a neat work environment during business hours:
	+ Store non-essential items when not in use
	+ Do not leave handwritten notes containing NPI outside of related files
	+ Securely store all files, documents and electronic media containing NPI when away from workstation for extended absence (i.e. lunchtime, break, meeting, vacation, outside office hours)
	+ Take all items to be destroyed to locked shredding bin when away from workstation for more extended absence (i.e. lunchtime, break, meeting, vacation, outside office hours)
	+ Whiteboards, planners, notepads or other items containing NPI must not be viewable from windows or doorways, must be secured when employee is away for extended absence (i.e. lunchtime, break, meeting, vacation, outside office hours)
* Close paper and electronic files containing NPI and lock workstations when employees are away from their desks
* At the end of the work day, all files, documents, portable devices, and electronic media containing NPI should be locked in a desk, file cabinet, or secure room overnight

**Data / Computer Security:*** Only authorized persons can access company servers, workstations, laptops or other mobile devices, copiers, printers, scanners and fax machines, as determined by the Network Usage Policy. The telecom-equipment room, IT/server closet, mailroom, financial office are restricted to those employees with legitimate business responsibilities requiring access.
* Servers are stored in locked facilities with access limited to employees identified, from time to time, in the Network Usage Policy.
* Paper files are never removed from the office except as needed for a legitimate business purpose.
* All devices, data and files containing NPI must have Password-protection or encryption. Passwords must be strong – at least eight characters using a combination of numbers, uppercase and lowercase letters and special characters. Separate accounts and passwords are established for each user. Passwords must be changed at least every 90 days or more frequently. Passwords may not be shared. None of last 6 passwords may be used.
* Workstations must be located so they are not visible to the public (including through clear windows or doorways) and are locked when the employee leaves their desk or must be set to lock automatically on no more than 15 minutes of inactivity
* No unauthorized software can be downloaded onto Firm hardware without Firm Manager approval
* All NPI must be stored on encrypted devices and never on personal devices
* Access to network with wireless devices is only allowed for legitimate business purposes and requires user authentication , i.e. virtual private network (VPN) or multifactor authentication (MFA)
* Employees are required to report compromised passwords and to change possibly compromised passwords immediately.
* Employees are required to report Security Program violations (perceived or actual) to the Firm Manager
* Only authorized persons can access any Firm hardware under the Network Usage Policy (above), including:
	+ Computers
	+ Servers
	+ Laptops
	+ Tablets
	+ Mobile devices
	+ Fax machines
	+ Copiers
	+ Scanners
	+ Printers

All data on the network is protected by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ anti-virus software that runs on servers, workstations and laptops, and is updated automatically with on-line downloads from the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ website. This includes alerts whenever a virus is detected. Any viral infection that is not immediately dealt with by said software is notified to the Firm Manager and immediately addressed.**Data / Email, Internet & Website Security:*** Email containing NPI may only be handled over the Firm’s true business domain email account and address. Private employee email is prohibited for handling business issues.
* Spam filters and firewalls must be used on email servers
* Emails containing NPI must be encrypted. The Firm Manager will communicate with customers and vendors about which encryption services can be utilized based on various system requirements and considerations
* Email attachments containing NPI must be password protected
* For title order placement, closing package delivery, etc. sites utilizing secure file and data transmission encryption will be used, typically indicated by *https* at the beginning of the website address, not just *http.*
* Internet usage is limited to business-related purposes only.

**Removable Media Security (USB ports, CD/DVD writeable drives, laptops, smartphones, external hard drives):*** If NPI must be stored on removable media or a portable device:
	+ The device must be encrypted
	+ Employee must not leave documents, portable devices or electronic media containing NPI in a non-secured location (unlocked vehicle, hotel room, etc.) accessible to others
	+ Employee is responsible for protecting the portable devices in their possession from theft or unauthorized access
* NPI must not be stored on personal electronic devices.
* Employees are required to report, immediately, the loss or theft of a laptop or other supported media device to applicable the Firm Manager. (See. 3.07 below)

**Firm website**:The Firm website contains a Privacy / Confidentiality Statement consistent with the Firm’s actual practices. |
| **Approved by / Date** | Highlight this text, then type name of person approving here | Highlight this text, then enter date of approval here |

|  |  |
| --- | --- |
| **Policy** | **Best Practice Pillar #3: INFORMATION AND DATA PRIVACY – Adopt and maintain a written privacy and information security plan to protect Non-public Personal Information as required by local, state and federal law.** |
| **Name of Procedure** | Retention and Destruction of Personal Information |
| **Reference Number** | 3.05  |
| **Applicable Parties** | Firm ManagementPractice Manager[Privacy Officer]Firm IT ManagerEmergency Management Team[Third Party Service Providers – Attached Addendum] |
| **Effective Date** | Highlight this text, then type effective date here |
| **Supporting Documentation** | Add to, delete and/or modify the sample text below to describe documentation that evidences your firm’s compliance with this best practice. Delete the preceding sentence and this one before finalizing.Written policies including:* Network Usage Policy and user permissions for all employees and all systems,
* Clean Desk and Clean Office Policy
* Retention and Destruction Policy
* Data Breach Incident Reporting
* Business Continuity and Disaster Recovery
* Employee Training and Management
* Hardware and software maintenance
* Third party providers
* Website, social media and other Firm public sites

Vendor contracts and privacy statements for SaaS, software, hardware, email, shared document, records destruction and other services |
| **Procedures** | Add to, delete and/or modify the sample text below to describe the procedure followed by your firm to assure compliance with this best practice. Delete the preceding sentence and this one before finalizing.**3.05 Retention and Destruction of Personal Information**NPI is to be collected only if relevant and necessary for the purpose specified. Closing files and client information are to be retained in compliance with the NC State Bar Revised Rules of Professional Conduct, Rule 1.15-3(g), RPC 209 and RPC 16, for a period of six (6) years since the file became inactive, unless either the client consent to destruction of the file or, after notice to the client that the lawyer intends to destroy the file, the client either retrieves the file or fails to do so within a reasonable period of time.Within 30 days of closing:* Files are promptly scanned into the Firm’s secure server and paper copies are shredded
* Files are moved to locked files in a secure location [in the Firm’s office(s) or off-site storage]

All user data is backed up to tape automatically on a daily basis, to [to Firm off-site server, off-site storage or cloud location: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_] location, using an appropriately secure system for fast indexing and data restoration.A full server backup to [to Firm off-site server, off-site storage or cloud location: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_] is completed [daily, weekly].The Firm Manager or Privacy Officer will regularly review and updated disposal dates on records.Disposal Certificates will be obtained from all Third Party Service Providers handling media and paper destructions. Service Level Agreements will be maintained current. |
| **Approved by / Date** | Highlight this text, then type name of person approving here | Highlight this text, then enter date of approval here |

|  |  |
| --- | --- |
| **Policy** | **Best Practice Pillar #3: INFORMATION AND DATA PRIVACY – Adopt and maintain a written privacy and information security plan to protect Non-public Personal Information as required by local, state and federal law.** |
| **Name of Procedure** | Overseeing Third Party Service Providers |
| **Reference Number** | 3.06  |
| **Applicable Parties** | Firm ManagementPractice Manager[Privacy Officer]Firm IT ManagerEmergency Management Team[Third Party Service Providers – Attached Addendum] |
| **Effective Date** | Highlight this text, then type effective date here |
| **Supporting Documentation** | Add to, delete and/or modify the sample text below to describe documentation that evidences your firm’s compliance with this best practice. Delete the preceding sentence and this one before finalizing.Written policies including:* Network Usage Policy and user permissions for all employees and all systems,
* Clean Desk and Clean Office Policy
* Retention and Destruction Policy
* Data Breach Incident Reporting
* Business Continuity and Disaster Recovery
* Employee Training and Management
* Hardware and software maintenance
* Third party providers
* Website, social media and other Firm public sites

Vendor contracts and privacy statements for SaaS, software, hardware, email, shared document, records destruction and other services |
| **Procedures** | Add to, delete and/or modify the sample text below to describe the procedure followed by your firm to assure compliance with this best practice. Delete the preceding sentence and this one before finalizing.**3.06 Overseeing Third Party Service Providers**The Firm Manager will investigate and recommend any Third Party Service Provider for approval by the Firm Management prior to retaining their services. In compliance with Revised Rule of Professional Conduct 5.3(a) and 2011 FEO 6, the Firm must obtain adequate assurance that:* The vendor is aware of the lawyer’s obligation of confidentiality
* NPI will be preserved in a manner compatible with the lawyer’s professional obligations
* Background checks are obtained by the vendors and updated every 3 years on any employees who may have access to areas or equipment containing NPI.
* Vendor employees are trained on the importance of maintaining security of NPI.
* Security acknowledgment form and non-disclosure agreement (NDA) is obtained from the vendor

The Firm Manager’s investigation should include:* The experience, stability, and reputation of the vendor.
* The vendor’s website, terms of service, service contract and other assurances regarding:
	+ measures for safeguarding security and confidentiality, including, but not limited to, firewalls, encryption techniques, socket security features, and intrusion-detection systems
	+ ability of the Firm to retrieve the data in a non-proprietary format and the vendor’s destruction of their copy of any data on termination of the contract
	+ extent to which the vendor backs up hosted data and uses generally accepted encryption protocols
	+ the vendor’s business continuity plan and disaster preparedness (such as remote backups of information)
* The reputation of the vendor

The Firm Manager must confirm appropriate procedures with any outside couriers, title examiners and or other providers to protect against unauthorized disclosure of NPI.The Firm Manager will maintain a list of all Third Party Service Providers (see attached Addendum) for which the Firm has authorized access to records containing current or archived NPI, and the authorized purpose for which each such Third Party Service Provider has such access based upon the legitimate business purpose for their service.The Firm Manager must monitor the service provider's performance on a regular basis to determine whether the provider is continuing to provide the contracted service and meet privacy and security requirements.Disposal Certificates will be obtained from all Third Party Service Providers handling media and paper destructions. Service Level Agreements will be maintained current.The Firm Manager will maintain the list of Third Party Service Providers of the Firm, their relevant contact information, dates of agreement(s) and latest nondisclosure agreements, on the Attached Addendum, including: [Identify specifically on attached Addendum]:* Software
* Hardware (copiers, fax, other equipment)
* Telephone
* Email
* Off-site (physical) storage
* Cloud storage
* Shared document sites
* Couriers
* Title examiners
* Outside or associated counsel
* Janitorial staff
* Landlord
* Water and coffee suppliers
* Background investigation providers
* Trust account reconciliation services
* On-site shredding
* Training vendor (if access to NPI)
* [other]
 |
| **Approved by / Date** | Highlight this text, then type name of person approving here | Highlight this text, then enter date of approval here |

|  |  |
| --- | --- |
| **Policy** | **Best Practice Pillar #3: INFORMATION AND DATA PRIVACY – Adopt and maintain a written privacy and information security plan to protect Non-public Personal Information as required by local, state and federal law.** |
| **Name of Procedure** | Data / Security Breach Incident Reporting |
| **Reference Number** | 3.07  |
| **Applicable Parties** | Firm ManagementPractice Manager[Privacy Officer]Firm IT ManagerEmergency Management Team[Third Party Service Providers – Attached Addendum] |
| **Effective Date** | Highlight this text, then type effective date here |
| **Supporting Documentation** | Add to, delete and/or modify the sample text below to describe documentation that evidences your firm’s compliance with this best practice. Delete the preceding sentence and this one before finalizing.Written policies including:* Network Usage Policy and user permissions for all employees and all systems,
* Clean Desk and Clean Office Policy
* Retention and Destruction Policy
* Data Breach Incident Reporting
* Business Continuity and Disaster Recovery
* Employee Training and Management
* Hardware and software maintenance
* Third party providers
* Website, social media and other Firm public sites

Vendor contracts and privacy statements for SaaS, software, hardware, email, shared document, records destruction and other services |
| **Procedures** | Add to, delete and/or modify the sample text below to describe the procedure followed by your firm to assure compliance with this best practice. Delete the preceding sentence and this one before finalizing.**3.07 Data / Security Breach Incident Reporting**Employees are required to report, immediately, the loss or theft of a laptop or other supported media device to the Firm Manager.Employees and Third Party Service Providers are required to report any data or security breach immediately. The Firm Manager will immediately report any data breaches to Firm Management.The Firm Manager will take immediate action to consult with the parties involved, retain additional services if needed, secure any ongoing breach, investigate the source and extent of the breach, take appropriate action to address any issues and prevent its recurrence. The Emergency Management Team, including Firm Manager and senior attorneys and staff, will immediately report all data breaches as required by state and federal law and assure compliance with G.S. 75-60 *et seq.* notification requirements. |
| **Approved by / Date** | Highlight this text, then type name of person approving here | Highlight this text, then enter date of approval here |

|  |  |
| --- | --- |
| **Policy** | **Best Practice Pillar #3: INFORMATION AND DATA PRIVACY – Adopt and maintain a written privacy and information security plan to protect Non-public Personal Information as required by local, state and federal law.** |
| **Name of Procedure** | Business Continuity and Disaster Recovery |
| **Reference Number** | 3.08  |
| **Applicable Parties** | Firm ManagementPractice Manager[Privacy Officer]Firm IT ManagerEmergency Management Team[Third Party Service Providers – Attached Addendum] |
| **Effective Date** | Highlight this text, then type effective date here |
| **Supporting Documentation** | Add to, delete and/or modify the sample text below to describe documentation that evidences your firm’s compliance with this best practice. Delete the preceding sentence and this one before finalizing.Written policies including:* Network Usage Policy and user permissions for all employees and all systems,
* Clean Desk and Clean Office Policy
* Retention and Destruction Policy
* Data Breach Incident Reporting
* Business Continuity and Disaster Recovery
* Employee Training and Management
* Hardware and software maintenance
* Third party providers
* Website, social media and other Firm public sites

Vendor contracts and privacy statements for SaaS, software, hardware, email, shared document, records destruction and other services |
| **Procedures** | Add to, delete and/or modify the sample text below to describe the procedure followed by your firm to assure compliance with this best practice. Delete the preceding sentence and this one before finalizing.**3.08 Business Continuity and Disaster Recovery**Electronic, off-site backup of critical software and data are as provided in 3.01 – 3.07 above.Firm Management will adopt a Business Continuity and Disaster Management / Recovery Plan and an Emergency Evacuation Plan. The Practice Manager will:* maintain and advise on updates as needed, at least annually or if any potential risk event.
* provide training to all employees at least annually.

Firm Management must maintain an Emergency Evacuation Plan that accounts for all personnel and clearly sets forth procedures to protect life safety in the event of an evacuation, heart attack, bomb threat, etc.The Firm’s Disaster Management and Recovery Plan must be documented, readily available to all employees and affected individuals who would require them in an emergency, audited and tested annually (and results documented), identifying:* Roles of each employee
* Recovery strategies for critical processes – client files, data that is stored locally and remotely, client funds, representation
* Contacts list for emergency personnel, clients, critical vendors (software, SaaS, phones) and disaster assistance
* Business continuity plans of critical vendors

Firm Management must maintain a Local Crisis Management Team with predestinated and well defined roles and responsibilities, tested annually |
| **Approved by / Date** | Highlight this text, then type name of person approving here | Highlight this text, then enter date of approval here |

# ALTA BEST PRACTICE 3 - ADDENDUM

# Information and Data Privacy

|  |  |
| --- | --- |
| **Practice Manager** | Insert Name of Practice Manager |
| **Person Responsible for Plan Maintenance:** | Practice Manager |
| **Next Review Due** | Insert Next Review Date |
| **Next Review Date Tickler Added to Practice Manager’s Calendar: (Insert Yes when added)** | State Yes when added |
| **Comments:** | Add Comments, if any |

**CLE/CPE & OTHER TRAINING ATTENDED RELATED TO INFORMATION AND DATA PRIVACY:**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Course Title/Sponsor/Relevant Overview | Date |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| **Review/Revision History for Information and Data Privacy Policies and Procedures:**Each time the above information pertinent to these Policies and Procedures is:* Reviewed for accuracy and no changes made, enter the date of the review, the person doing the review and a brief description such as “Reviewed by \_\_\_\_\_\_\_\_\_\_\_\_. No revisions needed.”
* Reviewed for accuracy and revision(s) made, enter the date of the revision(s), the name of the person making the revision(s), and a detailed description of the change(s) such as “Reviewed by Sally Doe. Employment status of Notary Elizabeth Watson updated to Inactive.”
 |
| Date of Review/Revision | Person Reviewing/Revising | Description |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**ADDENDUM: THIRD PARTY SERVICE PROVIDERS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name of Service ProviderPrincipalsAddress | Service Provided(Attach contract to electronic file, especially Non-disclosure agreement) | Firm Employee Responsible for Regular Review of Service Provider | Last Renewal Date | Next Renewal Date |
|  | (Website) |  |  |  |
|  | (IT consultant) |  |  |  |
|  | (Shredding company) |  |  |  |
|  | (Cleaning staff) |  |  |  |
|  | (Storage warehouse) |  |  |  |
|  | (Supply services / deliveries) |  |  |  |
|  | (BCO consultant) |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| **Review/Revision History of Relationship with Third Party Service Providers:**Each time the above information pertinent to Third Party Service Providers is:* Reviewed for accuracy and no changes made, enter the date of the review, the person doing the review and a brief description such as “Reviewed by \_\_\_\_\_\_\_\_\_\_\_\_. No revisions needed.”
* Reviewed for accuracy and revision(s) made, enter the date of the revision(s), the name of the person making the revision(s), and a detailed description of the change(s) such as “Reviewed by Sally Doe. John Wilson removed as Wire Initiator and added as Wire Approver.”
 |
| Date of Review/Revision | Person Reviewing/Revising | Description |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |