BRANCH OFFICE SECURITY POLICY AND IMPLEMENTATION STANDARDS

For LPL Financial LLC

Effective September 30, 2023

Policy approved by:
Alex Russell – SVP, Chief Information Security Officer
Hillary Russell– SVP, Chief Privacy Officer

LPL Financial

LPL Financial Branch Office Security Policy and Implementation Standards

Policy Objectives

The purpose of the Branch Office Security Policy and Implementation Standards (referred to collectively herein as the "BOSP" or the "Policy") is to define the security requirements of LPL Financial LLC ("LPL Financial" or the "Firm") to: safeguard the security and confidentiality of Personally Identifiable Information ("PII"), Proprietary Corporate Information ("PCI") and Internal Information from unauthorized access, alteration or destruction; protect against anticipated threats or hazards to the security or integrity of the information; protect against unauthorized access to, or use of, the information that could result in substantial harm or inconvenience to a customer or LPL Financial; and ensure the proper disposal of the information.

Policy Scope

The Policy is designed to comply with the collection and processing of PII, PCI and Internal Information, which is subject to legal and regulatory requirements, including the Gramm-Leach Bliley Act, Regulation S-P adopted by the Securities and Exchange Commission ("SEC"), the federal Red Flags regulations under the Fair and Accurate Credit Transactions Act of 2003, applicable state laws and regulations, and security best practices as implemented by LPL Financial.[1]

This Policy applies to all individuals conducting LPL Financial business in Branch Offices, including without limitation, investment advisory representatives, registered representatives, sales assistants, employees, temporary employees, contractors, and consultants (referred collectively herein as "Covered Individuals").

Covered Individuals are required to adhere to the BOSP and to protect PII, PCI, and Internal Information from unauthorized disclosure.

All systems and devices in use by the Branch Offices must be in compliance with the standards set forth in this Policy.

The standards ("Standards") set forth in this Policy cover:

1.0 Information Classification and Definition
2.0 Information Handling and Disclosure
3.0 Physical and Administrative Security
4.0 Technology Security
5.0 Training
6.0 Use of Third-Party Service Providers
7.0 Compliance and Reporting
Addendum to the BOSP for Advisors with Licenses to Sell Insurance or Annuities in certain States

Policy Owners

The Privacy Office and the Information Security Office of LPL Financial share authority over all LPL Financial Standards outlined in the BOSP in accordance with the LPL Policy on Policies.

Policy

[1]Regulation S-P is a regulation promulgated by the SEC and can be found at 17 CFR Part 248. Section 248.30 of Regulation S-P requires every regulated entity to adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information. See http://www.sec.gov/rules/final/34-42974.htm. In addition, many states have statutes or rules requiring the implementation of "reasonable" or "appropriate" security measures. Some of these are more prescriptive than others; see Resource Center for more information about specific state laws.

Covered Individuals must safeguard the security and confidentiality of PII, PCI and Internal Information from unauthorized access, alteration or destruction; protect against anticipated threats or hazards to the security or integrity of the information; protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to a customer or LPL Financial; and ensure the proper disposal of the information.

Covered Individuals shall not disclose any PII, PCI or Internal Information except for a valid business purpose and shall limit disclosure to authorized persons on a need-to-know basis.

This Policy establishes standards for LPL Financial Covered Individuals to safeguard PII, PCI and Internal Information by:

- Requiring administrative, technical, and physical safeguards for the protection of PII, PCI and Internal Information.
- Mandating standards and procedures that define the required administrative, technical, and physical safeguards for the protection of PII, PCI, and Internal Information. The standards and procedures include the security safeguard requirements for:
    - Computer hardware and network systems used to conduct LPL Financial business
    - Laptops and desktops used to conduct LPL Financial business
    - Smartphones, tablets, and any other mobile devices used to conduct LPL Financial business
    - Security and virus protection software
    - Email communication
    - Secure connection and communication to the LPL Financial environment
    - Encryption of PII
    - Proper disposal of PII, PCI, and Internal Information
    - Proper disposal of hardware
    - Physical office security requirements
- Reporting to LPL Financial when actual or suspected unauthorized access to information occurs as set forth further below.
- Training Covered Individuals on information security program requirements.

Policy and Standard Violations, Exceptions, Cybersecurity Events, and Privacy and Cybersecurity Incidents must be reported as set forth in Section 7. For questions regarding the BOSP, please see section 7.

Roles and Responsibilities

It is the responsibility of the Office of Supervisory Jurisdiction (“OSJ”) to ensure that every Covered Individual read and adheres to the Policy and Standards and related communications.

For those branches under the supervision of the LPL Financial home office, it is the responsibility of each Covered Individual to read and adhere to BOSP and related communications.

Written procedures must be maintained within the Branch Office that instruct Covered Individuals on the appropriate methods for complying with Standards set forth in the BOSP. Branch Offices may be asked to provide evidence demonstrating compliance with these Standards during compliance examinations.

It is a violation of the BOSP to disable, bypass, circumvent, or otherwise attempt to negate the information security measures of LPL Financial. Violations increase the risk of Cybersecurity and Privacy Incidents/Events, and result in identity theft, and legal, regulatory and reputational harm. Any Covered Individual found in violation of this Policy may be subject to disciplinary action, including monetary penalties, termination of affiliation with the firm, or legal action depending on the severity of the violation.

Amendments

The LPL Financial Privacy Office and Information Security Office evaluate the effectiveness of the BOSP annually, but may jointly amend the BOSP at their discretion outside of the annual review schedule. Covered Individuals will be advised of such amendments in writing and are required to comply with the BOSP, as amended, at all times.

Branch Office Implementation Standards

The following Implementation Standards are designed to provide Covered Individuals with general instructions and direction on how to ensure Policy compliance. Some of these Policy changes require technical knowledge above and beyond a standard user's level of understanding. In these cases, the Branch Office may need to consult a local information technology (IT) professional. [2]

1.0 Information Classification and Definitions	
1.1 Personally Identifiable Information (PII)	PII is defined as information of a personal or financial nature; protected by legal and regulatory requirements. The examples listed below, combined with a first and last name, or first initial and last name, generally constitute PII. In addition, a username or email address in combination with a password or security question and answer that would permit access to an online account is also PII, even if it is not combined with the user's first and last name. While the sensitivity levels of PII may vary, regulations applicable to LPL govern all sensitivity levels of PII. Examples include, but are not limited to, the following: ▪ Social Security Number ▪ Driver's license number or state-issued identification card number ▪ Individual's date of birth ▪ Financial account number ▪ Credit or debit card numbers (with or without the security code) ▪ Personal identification number/password that permits access to a financial account ▪ Passport number ▪ Customer financial information such as net worth and annual income ▪ Protected Health Information ("PHI") and other medical information to include policy numbers, medical records relating to payment for the provision of healthcare, demographic information, medical history, health conditions and treatment ▪ Biometric data such as fingerprints and voiceprints ▪ RepIDs ▪ Internet Protocol Address ▪ Internet or other electronic network activity information which could be used to identify an individual, including information collected through a cookie, pixel or other tracking devices ▪ Geolocation data ▪ Postal Address ▪ Email Address

[2] For further Technical Support, please refer to section 7 for contact information.

1.2 Proprietary Corporate Information (PCI)	PCI is defined as information related to the business and activities of LPL Financial, the unauthorized disclosure, access or use of which would cause a material adverse impact to the business, operations, or security of LPL. PCI may also include information that is governed by a non-disclosure agreement or confidentiality agreement with a third-party service provider, and any information the confidentiality of which LPL Financial is contractually obligated to protect or maintain. This type of data must be protected in the same manner as PII. Covered Individuals must maintain a clean desk without any exposed information, inclusive of leaving their locked computers unattended. Examples include: ▪ Salary and succession structures ▪ Advisor or customer lists ▪ Strategic plans ▪ Proprietary systems and processes
1.3 Internal Information	Internal Information is defined as any information that is not PII or PCI, but its unauthorized release or access could cause harm or embarrassment to LPL Financial, its employees, or affiliates, or provide an advantage to competitors. Internal Information is deemed sensitive and must be protected against unauthorized access or release. Examples include: ▪ Policies and procedures ▪ Memos ▪ Inventories ▪ Training and systems manuals
1.4 Public Information	Public Information is information that does not fall into one of the previous three categories and would not negatively impact customers or LPL Financial and/or its affiliates if distributed. This includes information that can be freely disseminated as long as there is a valid business purpose to do so and there would be no impact if published on a website or other public area.

1.5 Information Security Event	Any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt, or misuse an Information System or information stored on such Information System. 'Information System' refers to a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching, private branch exchange systems, or environmental control systems. Reporting of Information Security Events is set forth in Section 7.
1.6 Information Security Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an Information System, the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Reporting of Information Security Incidents is set forth in Section 7.
1.7 Privacy Incident	The loss of control, compromise, unauthorized disclosure, or unauthorized acquisition of information, or any similar occurrence in which: a person other than the authorized user accesses or potentially accesses PII or a system containing PII; or an authorized user accesses or potentially accesses PII or a system containing PII for an unauthorized purpose. The term encompasses both suspected and confirmed incidents, whether intentional or inadvertent. Reporting of Privacy Incidents is set forth in Section 7.
1.8 Portable Media	Defined as any removable storage, flash drives, smart cards, USB drives, CDs, DVDs, and removable storage for smartphones.
1.9 Laptop	Includes but is not limited to: traditional laptops, Chromebooks, and tablet PCs.
1.10 Smart Devices	Defined as electronic devices that are connected to other devices or networks via different wireless protocols. Examples of smart devices can include but are not limited to: Apple devices (iPhones, iPads etc.), Windows Mobile/CE, and Android devices.
1.11 Privileged Access Accounts	Accounts used to manage a server or application. Unlike regular user account access, a privileged access account has elevated access privileges on servers or applications.

2.0 Information Handling and Disclosure	
2.1 Identification of PII	Covered Individuals are required to identify whether the records (paper and electronic), computing systems, storage media, and portable devices contain PII. If the Covered Individual is unable to make this determination, they must treat all records and devices as if they contain PII.
2.2 Collection of PII	Collection of PII must be limited to the amount that is reasonably necessary to accomplish the legitimate business purpose for which it is collected.
2.3 Record Retention & Storage	Information must be stored and retained in accordance with state and federal regulations and LPL Financial or affiliate policies for record retention. This information can be found in the Advisor Compliance Manual ("ACM") located on the ClientWorks Resource Center, or otherwise referenced in the ACM. All files, disks, and other media and documents containing PII must be stored in accordance with the electronic/encryption standard.
2.4 Encryption Standard	All PII stored on portable media or portable computers and devices must be encrypted using a National Institute of Standards and Technology ("NIST") approved encryption algorithm, and must utilize a minimum AES 128-bit. All mobile devices (i.e., laptops, phones, etc.) used for LPL Financial business must be encrypted with whole disk encryption installed locally on the device, and desktop computers if configurable. Encryption software must be installed and active at all times, and documentation indicating that the software uses a minimum 128-bit length key must be kept (e.g.), software manual.

2.5 Disposal of PII, PCI and Internal Information	In accordance with state and federal laws and regulations and applicable rules, PII, PCI and Internal Information must be disposed of securely when it is no longer needed. All documents, in any form, are required to be disposed of in accordance with the Record Retention Schedule and/or the Record Keeping section of the ACM and must be pre-approved by the LPL Financial Compliance, Legal & Risk ("CLR") Department. Secure disposal must be accomplished by one of the following means: ▪ Shredding paper records using cross-cut or confetti cut, not strip cut, so that reassembly is unlikely ▪ Destruction of electronic media so the information cannot be read or reconstructed ▪ Securely wiping hard drives and other electronic media that is no longer in service (including, but not limited to computers, copiers, fax machines, and scanners) A signed Non-Disclosure Agreement ("NDA") must be obtained from any third party that is contracted for the purpose of secure disposal as well as a digital data destruction certificate certifying that the information has been shredded, destroyed, and/or completely and securely wiped.
2.6 Information Sharing	PII, PCI, and Internal Information, including information relating to securities, insurance, investment advisory, or other financial service relationships must only be used for valid business purposes.

2.7 Access to and Viewing of PII, PCI and Internal Information	▪ Do not discuss PII, PCI or Internal Information with, or in the presence of, persons who have no legitimate business need for the information. ▪ Covered Individuals must maintain a “clean desk,” free of exposed PII, when leaving their workspace unattended. Do not leave completed applications and related information where others can read or copy such material. When not being used, this information must be securely stored. ▪ PII must not be accessed out of curiosity, for personal use or where the inquiring person does not have a valid business relationship with the customer that creates a business need to access the information. This includes, without limitation, information on paper documents in the office, and on computer screens, printers, copiers, and fax machines. Access must be limited to authorized persons on a need-to-know basis. ▪ Verify the identity of the person to whom PII is being disclosed to before that information is disclosed. ▪ Do not disclose in writing or orally any PII regarding a customer to anyone other than the customer, staff, or LPL Financial employees who have a legitimate business need to know the information. ▪ Do not disclose PII to a customer’s spouse, relatives, employer, or retained professionals (e.g., lawyers, accountants, etc.) without obtaining a signed Form F456 from the customer. ▪ Do not input PII, PCI and internal information into any Artificial Intelligence (AI) tools.

2.8 Emailing Information and Other Transmissions	All LPL Financial and securities business-related email must be transmitted through an lpl.com or approved DBA email address, or an email address journaled to LPL Financial, and is subject to review and supervision by LPL Financial. Emails containing PII in the body of the email or in attachments to the email must be encrypted by entering "[secure]" or "[encrypt]" (including brackets as shown) in the subject field of the message. Plug-ins may provide the option to add a "Send Securely" button to the ribbon. With the plug-in installed, it is no longer required to type encrypt or secure, within the brackets of the subject line. The "Send Securely" button must be selected when sending PII. If using a fax machine, eFax, VOIP, copy machine, scanner, printer or another machine with email capabilities to transmit PII, only LPL.com or approved DBA email addresses must be used. If these communications are stored in a cloud environment, they must be stored in accordance with section 6.5. Encrypted or password-protected attachments are prohibited because they interfere with the supervision process. Offices that maintain email addresses that are journaled to LPL must use LPL-provided email addresses to send PII or solutions that meet the below standards: ▪ Encrypted messages must be protected using a minimum 128-bit key cipher length. ▪ The encryption system must not interfere with the email journaling process or the LPL archival and supervision systems. ▪ Multi-factor authentication ("MFA") must be enabled and enforced for web-based email (i.e., Outlook Web Access, O365, etc.). Reference the Delegating Email section in the ACM for guidelines on delegating access to your email to another individual. Covered Individuals must utilize only LPL approved communication tools when communicating via other electronic means, to include text and instant messaging in accordance with the ACM. Similarly, any other transmissions of PII or materials containing PII over public networks or wirelessly must be encrypted in accordance with the standards
2.9 Data Minimization	All Covered Individuals must only collect, use, access, share, retain and process the minimum amount of PII, PCI and Internal Information to accomplish the valid business purpose, which includes masking or truncating PII, especially data elements which are particularly sensitive in nature, such as social security numbers and account numbers.

3.0 Physical and Administrative Security and Business Continuity	
3.1 Access to Physical Locations	Access to physical locations where PII is stored or used must be restricted to authorized persons with a legitimate business need. A signed NDA must be obtained from any contracted third party with physical access to the Branch Office (i.e., cleaning service, building/facility managers).
3.2 Lock and Secure Offices and Cabinets	Lock and secure all offices containing PII; keys and entry devices must be kept secure; prevent unauthorized individuals from accessing areas where PII, PCI and Internal Information are stored or readily accessible; client PII must not be left in an unlocked area overnight and must be locked in a file cabinet.
3.3 Secure and Control Access	Secure and control physical access to dedicated computers, printers, servers, copiers, and fax machines by, among other things, locking doors, installing, and maintaining high security locking mechanisms and security systems, isolating equipment to limit access to authorized persons, and creating and enforcing procedures to segregate Covered Individual responsibilities and access to equipment.
3.4 Protect Computer Equipment and Facilities	Safeguards must be implemented to protect computer equipment and facilities against fire, flood, and other environmental hazards. Such protections may include fire alarms, raising computer equipment off the floor if there is a reasonable possibility of flood, and installing air conditioners to keep computer equipment cool. Remote or online device backup may also be used for device data recovery in an effort to safeguard against environmental hazards. Refer to section 6 (Storage) for security requirements specific to data storage and backups.
3.5 Establish Procedures for the Secure Handling of Mail and Mail Forwarding	When mailing PII, PCI or Internal Information via outside carriers or contractors (e.g., United States Postal Service, Federal Express, etc.), maintain a precise inventory of the information being mailed, the tracking receipt, and ensure the enclosed materials are sufficiently protected during transit. Electronic media containing PII must follow the encryption requirements in section 2.4. PII contained on hardcopy documents must be redacted unless there is a valid business purpose for its inclusion. For example, truncate or mask a Social Security Number or Account Number unless its inclusion is necessary to either the recipient or sender. In the event the information is lost or stolen in transit, contact the Incident Hotline (866) 578-7011 or email PrivacyResponseTeam@lplfinancial.com. The Privacy Office will request the inventory of information included in the mailing in order to determine the next steps.

3.6 Shared Offices and Devices	There must be separate devices (i.e., printers, copiers, etc.) for each firm. The LPL devices must be in a secure area. Internet sharing, including Wi-Fi, with non-LPL affiliated entities is prohibited. Covered Individuals must maintain separate devices (i.e., computers) for use with LPL Financial business. Such devices must also be located in a secure area. PII must be kept secure when using copiers, scanners, or fax machines. Safeguards may include, but are not limited to: ▪ Enforce unique user identification. ▪ Data encryption at rest using a minimum AES 128-bit encryption and in-transit using TLS 1.2 or higher. ▪ Inbound documents may be sent to only the intended recipient's email. ▪ Secure archiving of all information sent or received. Do not copy, fax, or scan PII on public machines (e.g., FedEx, Staples, Office Depot, etc.). Advisors working in co-working spaces (i.e., WeWork) must utilize secure virtual private network ("VPN") services while using the provided shared Wi-Fi network. Advisors also have the option to use a personal hotspot and circumvent the use of a shared network. Advisors are prohibited from utilizing shared printers, copiers, and fax machines to print, scan, or transmit PII. Advisors utilizing a co-working space with a private, lockable office may utilize printers, copiers, and fax machines if the devices are within their private office.
3.7 Covered Individual Change Notification	Immediately notify the LPL Financial Home Office of any changes to Covered Individuals (terminations, new hires, or other changes within the office). Terminated Covered Individuals are expected to surrender all keys, IDs, badges, business cards, computer equipment, and other items which permit access to the LPL Financial and Branch Office physical premises and electronic systems on or before date of termination for on-site employees and as soon as possible for employees working remotely. Managers should ensure all applicable processes are followed at termination to remove access to systems.
3.8 Regulatory and Background Checks	All Covered Individuals that process PII will be subject to regulatory and background checks through LPL Financial. Background checks are conducted upon notification of onboarding.
3.9 Business Continuity	Branch Offices must create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption. Such procedures must be reasonably designed to enable the branch to meet its existing obligations to customers. Branches must also conduct an annual review of their business continuity plan and modify it as necessary to changes in operations, structure, business, or location.

4.0 Technology Security	

4.1 Password Security	▪ Passwords must meet or exceed the baseline password requirements listed below for computer devices:
	  ○ Passwords must be at least 8 characters in length
	  ○ Password must contain at least three of the following elements:
	  ▪ Numbers
	  ▪ Upper case letters
	  ▪ Lower case letters
	  ▪ Special characters (~!@#$%^&*)
	▪ Biometric authentication methods (e.g., fingerprint) are permitted so long as associated device password meets or exceeds the baseline requirements.
	▪ Authentication via PIN to a physical device is permitted so long as the character length is the minimum the device requires and the associated device passwords meet or exceed the baseline requirements listed above.
	▪ Credentials (ID and Passwords) must be kept confidential and must not be shared.
	▪ Users must not reuse the same credentials (ID and Passwords) for other accounts or systems outside of LPL Financial.
	▪ Passwords that provide access to applications containing internal information, PCI, or PII must be changed at least 120 calendar days in conjunction with MFA, if no MFA then 90 days.
	▪ Temporary passwords must be changed immediately upon receipt.
	▪ Passwords must be changed whenever there is an indication of possible system or password compromise.
	▪ Passwords must not be written down nor kept in or near a workspace.
	
	A password manager software or application may be used so long as the software requires a master password and encrypts the password in storage. Master passwords should meet or exceed the baseline password requirements listed above, and have MFA enabled.
	
	Windows OS and macOS computers must have a properly configured Local Security Policy that matches password complexity requirements.

4.2 Privileged Access	Privileged Access accounts adhere to Password Security Requirements and additional requirements below: ▪ Accounts must be renamed from the default administrator/root account. ▪ Accounts that have system-level privileges must have unique identities and passwords from other accounts. ▪ Accounts must automatically lock-out after 5 unsuccessful logins in 60 minutes. If account lockouts are not feasible, the account must have a minimum password length of 16 characters. Privileged Access Management ("PAM") tools may be used for managing and monitoring privileged access accounts. PAM master passwords must meet or exceed the baseline password requirements and have MFA enforced.
4.3 Firewalls	Any computer that accesses the internet must be protected by a software firewall. If an operating system has a firewall built within its framework, enabling it will satisfy this requirement. If multiple devices in an office share an internet connection, that connection must be protected by a hardware firewall, Endpoint Detection Response, or Managed Detection and Response solution in addition to the software firewall. If the firewall (router) has wireless capability that is not being used, it must be disabled.
4.4 Anti-malware Software	Anti-malware must be installed on all computers, including both PCs and Macs. The software used must be supported by its developers and configured to automatically check for, download, and install updates. Anti-malware programs must be configured to actively scan files in use and perform a full scan of all files at least once a week, or be monitored by a Managed Detection & Response service provider. If any computer or other device is infected with malicious software it must not be used until the infection is treated.
4.5 Operating Systems and Software Security Updates	Operating systems must be supported by its developers and configured to automatically check for, download, and install security updates. Operating systems no longer supported by its developers are commonly labeled as reaching "end-of-life" or "end-of-support." Covered individuals are not permitted to utilize devices with operating systems that have reached end-of-life or end-of-support and must update their operating system accordingly. Professional, Enterprise, or Education edition is required if utilizing Windows Operating Systems. Software applications must also be kept up to date with the latest security patches. Applications must be configured to automatically check for, download, and install security updates. Security updates that are not automatically installed must be installed as soon as possible. If automatic updates are not configurable, there must be a procedure in place to patch operating systems and software applications. Covered Individuals are responsible for actively monitoring the software programs installed on computers in their office to ensure the programs'

	compliance with the BOSP. It is up to each Covered Individual to ensure programs are installed appropriately, receiving updates/patches, and are supported by the developers.
4.6 Virtual Clients and Public Devices	Virtual Clients (e.g., Virtual Machines, etc.) must meet the following requirements: ▪ Data must not be stored on the device, only in the system or server connected. Ensure off-line saving functionality is turned-off as to disable local storage of data. ▪ Regular updates and patches must be performed on the device. Use of public devices (e.g., Hotel business center, etc.) for LPL Financial business is not allowed, including email use. All devices used for LPL Financial business purposes must comply with this Policy and are subject to audit.
4.7 Securing Smart Devices and Mobile Devices	Smart and/or Mobile Devices (e.g., smart phones, tablets, smart watches) that are used to view, process, store or transmit any LPL Financial data, including accessing ClientWorks, must have the following controls in place: ▪ All PII related to LPL business must be segregated from any personal information stored on the same device. PII should only be accessed, stored or transmitted in or through applications that meet LPL requirements. ▪ Devices must require a password to access the device. Passwords must the minimum length required by the device. ▪ Biometric authentication methods (e.g., fingerprint) are permitted so long as associated device passwords meet or exceed the baseline requirements listed above. ▪ Failure to provide a correct password to a mobile device after no more than 10 attempts, or minimum attempts as required by the device manufacturer if greater than 10, must cause all data stored on the device to be permanently deleted. ▪ Removable storage devices used for smart phones must be encrypted, using a minimum of 128-bit. ▪ Devices must be set to auto-lock after no more than 5 minutes for smart phones, or 15 minutes for tablets, and require a password to regain access to the device. ▪ Encryption must be activated and configured. ▪ When a smart phone or tablet is left unattended, the user must lock the device.

4.8 Device Screen Lock	All devices used to view, process, store, or transmit LPL Financial data must be configured to lock out their user interface after no more than 15 minutes of inactivity. The Covered Individual must be prompted to enter his or her password to regain access to the device. When leaving a device unattended, the Covered Individual must lock the screen.
4.9 Network and Wireless Use	Private networks (Office or Home) ▪ Office internet sharing, including Wi-Fi, with non-LPL affiliated entities, is prohibited. ▪ Maintain a separate wireless network for guests and clients with a separate password. Do not share the primary network password with guests. ▪ Do not use unsecured wireless networks. ▪ Use strong passwords to restrict access to wireless devices. ▪ Ensure traffic between the device and the Wireless Access Point is secure and encrypted using the most recent industry standard technology. Public Networks ▪ Use secure virtual private network (“VPN”) services when using Wi-Fi provided at hotels, airports and other places where the network poses higher risk to computers. Do not let other systems use a device as an access point. ▪ Use of a mobile phone hotspot is allowed so long as the hotspot is generated by a device under the control of Covered Individual and which is otherwise compliant with the password requirements for third-party applications set forth in this Policy. An advisor office guest network is required to have a password. Advisors sharing an office with a non-LPL business must maintain a separate network connection and may not allow the neighboring business to utilize their guest or main network.
4.10 Electronic Device Travel Restrictions	To protect electronic devices (e.g., laptops, tablet PCs, portable media, cell phones/smartphones etc.) during travel: ▪ Do not store electronic devices in checked baggage. ▪ Do not leave electronic devices in plain sight in vehicles. ▪ Do not leave electronic devices unattended in a public place.

4.11 Recording and Call Transcription in the Workplace	Audio and video recordings and photography, (even when utilizing personal devices) are prohibited regardless of the relationship of the parties and the format (meeting, telephone call, conference call, video conferencing webinar, photography, seminar, training, etc.), except as follows: Webinars or seminars which are defined as one presenter to multiple participant pre-recorded or live events generally intended for marketing, training or education purposes are permitted as long as the following requirements are met: ▪ All participants must be notified that the event is being recorded and for what purpose prior to the start of the recording. ▪ All participants must consent to being recorded for the specific purpose disclosed. ▪ A visual or audible indicator must be present to indicate that the event is being recorded. ▪ Recordings that will be used for client-facing purposes must be submitted, prior to first-use, to Marketing Regulatory Review ("MRR") for supervision as marketing/advertising content. Following these requirements will help ensure compliance with Federal and State regulations and LPL policy.

5.0 Training	
5.1 Security and Privacy Training	Covered Individuals must complete the Branch Office Privacy and Security training once per calendar year to learn how to identify and respond to threats to information systems. This training must be part of new hire orientation. Covered Individuals must be trained within 30-days of onboarding. Branch Office Managers are responsible for ensuring that all Covered Individuals receive and complete the Branch Office Security & Privacy Training once per calendar year.

6.0 Use of Third-Party Service Providers	
6.1 Evaluation	All third-party service providers with access to PII, which include cloud and on-premises, must have the capacity to protect PII. Branch Offices must enter into an agreement with those third-party service providers which includes the protection of PII and take reasonable steps to verify that each third-party service provider with access to PII and with whom the Branch Office has a relationship is capable of maintaining safeguards for PII. Advisors are generally permitted to use third-party service providers when in compliance with this section, however, the use of third-party service providers who facilitate services noted below are prohibited without the approval of LPL's Compliance Department as discussed within the ACM. Reference the ACM chapters noted here for third-party service providers that pertain to these categories: ▪ Communications and Advertising ▪ Electronic Communications ▪ Recordkeeping
6.2 Contracts	All contracts with third-party service providers, including consultants, with access to PII must: • contain provisions which require the third-party service provider to maintain a written Information Security Program in compliance with all applicable laws and regulations; • require the third-party service provider to use PII solely to perform the services under the agreement; • require that notice is provided prior to any changes in security or privacy policies that impact the protection or use of PII. • prohibit the third-party service provider from using or processing personal information for its own purposes; • include a process for incident or breach reporting notification. Copies of executed contracts and service agreements are required to be kept accessible for examinations or audits.

6.3 Risk Assessments	All advisors must conduct and document an annual Cybersecurity Risk Assessment of Information Systems sufficient to inform the design of their cybersecurity program. Risk assessments should be updated as reasonably necessary to address changes to the advisor's information systems, regulatory changes, nonpublic information or business operations. The risk assessment should consider the particular risks of the advisor's business operations related to cybersecurity, nonpublic information collected or stored, information systems utilized and the availability and effectiveness of controls to protect nonpublic information and information systems. All advisors must have a Security Incident Response Plan that outlines processes to Identify, protect, detect, respond, and recover from incidents.
6.4 Transmissions	All electronic transmissions of PII between the Branch Office and its service provider(s) must be secure. This is accomplished in several ways, for example: ▪ Use of a VPN connection ▪ Use of a dedicated line ▪ TLS 1.2 or higher encryption utilizing a minimum 128-bit key ▪ Use of Secure Cloud Services through LPL Financial (i.e., LPL Box)

6.5 Storage	It is critical to confirm the storage location of all PII before executing contracts with any third-party service provider. All PII must be stored within the United States and not offshore at a vendor location. If using cloud storage services, it is the user's responsibility to ensure that confidentiality, integrity, and availability is secured and handled when using the cloud storage service. It is a requirement that MFA is utilized to access cloud storage services. Messaging and links generated through the cloud storage tool are prohibited. Please note that cloud storage cannot be the primary source of books and records. Ensure that all books and records are stored in iDoc. See the Advisor Compliance Manual – Recordkeeping section for further information. All data must be encrypted, at-rest at a minimum, utilizing industry-approved algorithms utilizing a minimum 128-bit. If encryption is not offered, then the service provider must have in place adequate controls to prevent unauthorized access to their storage system. These controls must include: ▪ MFA ▪ Firewalls ▪ Intrusion Detection and Intrusion Prevention Systems ▪ Current Antivirus and Patch Management Procedure ▪ Physical access controls Back up / Recovery / Online Storage systems, which are approved by LPL Financial, must be used to store/backup/preserve data. Ensure that the following precautions are taken while configuring the online drives: ▪ Limit the number of user accounts which have access to this data ▪ Periodically verify the accounts ▪ Remove system access to departing employees / staff immediately on the day of departure ▪ Ensure that encryption, versioning, and MFA are turned on in the configuration ▪ Disable sharing files / folders containing PII, PCI and Internal Information

6.6 Due Diligence	It is the responsibility of the Covered Individual to perform due diligence on any cloud and/or on-premises third-party service provider prior to the execution of a contract for products or services to ensure appropriate security and privacy measures are in place for the protection of PII. At a minimum due diligence must include, but is not limited to: • Ensuring appropriate Information Security and Privacy policies are in place that govern the protection of PII and prohibit any reuse of such PII without consent. • A review of the Terms of Use for online services as they constitute a contract with the user of the service. Terms of Use containing provisions which allow or provide some type of license to the service provider to use information entered into the application or service (other than for the exclusive purpose of providing or improving the service) do not meet the requirements of this Policy. The same standards that are applicable to Covered Individuals are applicable to any third-party service provider that is handling PII. All questions related to this section are to be referred to the Privacy Office at privacy@lplfinancial.com.

7.0 Compliance and Reporting	
7.1 Compliance	Branch Managers are required to annually attest to the compliance of their respective branches with this Policy and must have procedures in place to ensure continual compliance.
7.2 Privacy Policy and Consumer Privacy Notice Compliance	Covered Individuals must adhere to LPL's Privacy Policy and Consumer Privacy Notice and be aware of their obligations to the Departing Advisor Opt-Out process, including obligations to clients in California, North Dakota, and Vermont who are, by default, considered opted-out. Additional information can be found on the Privacy Resource Center page.
7.3 Reporting of Information Security and Privacy Events/Incidents	Information Security and Privacy Events/ Incidents, including the loss, theft or unauthorized access of PII, whether confirmed or suspected, must be reported immediately to LPL Financial via the Incident Hotline 1-866-578-7011 or email PrivacyResponseTeam@lplfinancial.com before any further action is taken. Covered Individuals must respond to requests LPL Financial deems necessary to adequately investigate any Information Security and/or Privacy Events/Incident. Remediation steps may include, but are not limited to, client and/or regulatory notification, as well as providing credit monitoring services for affected clients, the costs of which will be transferred to the appropriate LPL Branch Office or Financial Institution. Covered Individuals are required to keep a record of all Information Security and Privacy Events/Incidents accessible for audit.
7.4 Policy Violations and Exceptions	It is a violation of this Policy to disable, bypass, circumvent, or otherwise attempt to negate the security measures of LPL Financial. Any Covered Individual found in violation of this Policy may be subject to disciplinary action, including possible monetary penalties, termination of affiliation with the Firm, or legal action depending on the severity of the violation. Policy violations should be reported to privacy@lplfinancial.com. If a Branch Office or a Covered Individual is unable to comply with one or more of the requirements in this document, an Exception request must be documented and approved, where appropriate. Exceptions must be assessed in accordance with the Advisor Security Exception Process. For additional information please contact BOSP@lplfinancial.com.

7.5 Questions	Answers to common questions are found in the Branch Office Security Policy FAQ located on the Resource Center. Additional questions about this Policy must be directed to the Home Office Compliance and Technical Support contacts listed below: LPL Financial (not Institution Services) Technical Questions: (704) 733 - 6600 Policy Questions: (844) 610-0009 LPL Financial Institution Services Technical Questions: 1 (866) 321-3640, option 3 Policy Questions: (844) 610-0009 Or email: security.mailbox@lplfinancial.com

Addendum to the Branch Office Security Policy and Implementation Standards for Advisors with Licenses to Sell Insurance or Annuities in Certain States

In addition to this Policy and implementation Standards, as well as LPL's Agent Service Provider Terms, advisors with licenses to sell insurance or annuities in certain states may be subject to specific cybersecurity rules and regulations.

This includes, but is not limited to, the following the NYDFS sections below:

- Section 500.02 Cybersecurity Program.
- Section 500.03 Cybersecurity Policy.
- Section 500.04 Chief Information Security Officer.
- Section 500.05 Penetration Testing and Vulnerability Assessments.
- Section 500.06 Audit Trail.
- Section 500.07 Access Privileges.
- Section 500.08 Application Security.
- Section 500.09 Risk Assessment.
- Section 500.10 Cybersecurity Personnel and Intelligence.
- Section 500.11 Third Party Service Provider Security Policy.
- Section 500.12 Multi-Factor Authentication.
- Section 500.13 Limitations on Data Retention.
- Section 500.14 Training and Monitoring.
- Section 500.15 Encryption of Nonpublic Information.
- Section 500.16 Incident Response Plan.
- Section 500.17 Notices to Superintendent.

With special attention to Section 500.11 Third Party Service Provider Security Policy, advisors shall:

- Implement written policies and procedures designed to ensure the security of Information Systems and Non-Public Information that are accessible to, or held by, the Third-Party Service Providers of advisor offices.
- Conduct a Cybersecurity Risk Assessment of its Information Systems sufficient to inform the design of a cybersecurity program
- Ensure policies and procedures are based on risk assessments and address all requirements of the rule to the extent applicable.

Depending on how a Branch Office is structured, it may be entitled to a full or partial exemption. The regulation doesn't permit LPL to certify on behalf of its agents. Failure to comply, and to certify compliance, may result in fines or penalties from NYDFS.

Other states have passed an Insurance Data Security Act. These laws generally contain similar requirements: subject to certain exemptions, they may require the implementation of an information security program based on a risk assessment, designation of an employee in charge of the program, and notification of certain cybersecurity events to the state insurance authority (in addition to specific safeguards, secure disposal of personal data, monitoring of the program, and security measures relating to the engagement of third-party service providers).

See the Resource Center for more information about specific state laws.