Branch Office Security Policy and Implementation Standards

for LPL Financial LLC

September 30, 2017

Policy approved by Jim Powell – SVP, Chief Information Security Officer
Hillary Russell-Pelletier – SVP, Chief Privacy Officer

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 to safeguard the security and confidentiality of personally identifiable information ("PII") from unauthorized access, alteration or destruction; to protect against anticipated threats or hazards to the security or integrity of the information; to 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 Regulation S-P[1] adopted by the Securities and Exchange Commission ("SEC"), the federal Red Flags regulations under the Fair and Accurate Credit Transactions Act of 2003 and any applicable state laws and regulations as well as security best practices, and apply to all LPL Financial branch office staff members.

With certain exceptions as noted in the Policy, LPL Financial and its financial advisors, sales assistants, employees, temporary employees, contractors and consultants are required to protect and not disclose PII.

This Policy applies to all individuals and computers involved with conducting LPL Financial business.

The standards ("Standards") set forth in the 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 3rd Party Service Providers
7.0 Compliance and Reporting

Policy Owner
The Privacy Office and the Information Security Office of LPL Financial share authority over all LPL Financial security policies and standards outlined in the BOSP.

Policy
Branch office staff members must safeguard the security and confidentiality of PII 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.

A branch office staff member must not disclose any PII regarding a customer to anyone other than the customer or staff members who have a legitimate business need to know the information, or as contained in the policies and standards of LPL Financial.

Any violation of this Policy and its Standards, intentional or unintentional, must be promptly reported immediately to the Privacy Office of LPL Financial via the Security Incident Hotline: (866) 578-7011.

This policy establishes a standard LPL Financial branch office approach to safeguarding PII by:

[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. 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.gob/rules/final/34-42974.htm

- Requiring administrative, technical, and physical safeguards for the protection of PII.
- Mandating standards and procedures that define the required administrative, technical, and physical safeguards for the protection of PII. The standards and procedures include the security safeguard requirements for:
    - Computer hardware and network systems used to conduct LPL Financial business
    - Laptops and portable data devices used to conduct LPL Financial business
    - Security and virus protection software
    - Email communication
    - Secure connection and communication to the LPL Financial environment using multiple layer authentication, strong password rules, and access restrictions
    - Encryption of data
    - Proper disposal of information
    - Physical office security requirements
- Reporting to LPL Financial when actual or suspected unauthorized access to information occurs.
- Training branch office staff on information security program requirements.

Roles and Responsibilities
It is the responsibility of the Office of Supervisory Jurisdiction ("OSJ") to ensure that every staff member reads and adheres to the Policy and Standards and related communications. LPL Financial will evaluate the effectiveness of our BOSP annually or when there is a material change in its business practices or in the business practices of its branch offices.

OSJs are required to annually attest to the compliance of their respective branches and should have procedures in place to ensure continual compliance.

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

Written procedures must be maintained that instruct office staff on the appropriate methods for complying with these standards. You may be asked to provide these procedures and other evidence demonstrating compliance with these standards during compliance examinations.

It is against the BOSP to disable, bypass, circumvent, or otherwise attempt to negate the information security measures of LPL Financial. Any individual found in violation of the 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.

Please address all questions and comments concerning the BOSP to the LPL Financial Privacy Office at security.mailbox@lpl.com.

Amendments
LPL Financial may amend the LPL Financial BOSP at its discretion from time to time. You will be advised of such amendments in writing and are required to abide by the BOSP (including the policy and implementation standards), as amended, at all times.

Branch Office Implementation Standards and Guidelines

The following Implementation Standards and Guidelines are designed to provide you with general instructions on how to ensure that your business complies with the Policy. Some of these Policy changes require technical knowledge above and beyond a standard user's level of understanding. In these cases, you may need to consult a local information technology (IT) professional. For further Technical Support, please refer to section 7.4 for the correct contact phone numbers.

Standard	Implementation Standards and Guidelines
1.0 Information Classification and Definition	
1.1 Personally Identifiable Information (PII)	*Standard:* PII is defined as all customer information of a personal or financial nature and is protected by legal and regulatory requirements and is highly sensitive information and/or could cause significant harm to customers or LPL Financial if mishandled. PII includes information covered by Title V of the Gramm-Leach-Bliley Act, SEC Regulation S-P, HIPAA, and state privacy and information security laws (including without limitation, Massachusetts Data Protection regulations and the cybersecurity requirements of the New York Department of Financial Services). Examples include: first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to a customer: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a client's financial account. PII may also include passport number, customer financial information, such as net worth and annual income; and private health information such demographic information, medical history, test and laboratory results, insurance information and other data collected by healthcare professionals to identify an individual and determine appropriate care.
1.2 Internal Information	*Standard:* Internal Information is defined as any information that is not PII, but its unauthorized release or access could cause harm or embarrassment to LPL Financial, or provide an advantage to competitors. Internal Information is deemed sensitive and must be protected against unauthorized access or release. Examples of Internal Information include internal documents, such as policies and procedures, memos, inventories, training and system manuals; and proprietary business information, such as merger and acquisition data, key business initiatives, financial information prior to public release, strategic information, business partner data held in confidence, and advisor name in combination with advisor rep ID.
1.3 Public Information	*Standard:* Public Information is information that 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 reason to do so and there would be no impact if published to a website or other public area. Examples of public information include job opportunity bulletins, marketing brochures, and press releases.
2.0 Information Handling and Disclosure	
2.1 Identification of PII	*Standard:*

Standard	Implementation Standards and Guidelines
	You are required to identify the paper, electronic and other records, computing systems and storage media, including laptops and portable devices that contain PII. If you are unable to do so, you must treat all records and devices as if they contain PII.
2.2 Collection of PII	*Standard:* Collection of PII must be limited to the amount that is reasonably necessary to accomplish the legitimate purpose for which it is collected.
2.3 Record Retention & Storage	*Standard:* 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 located on the ClientWorks Resource Center. All files, disks, and other media and documents containing PII must be stored securely.
2.4 Electronic PII Storage/Encryption Standard	*Standard:* Encryption standards must meet the National Institute of Standards and Technology ("NIST") approved encryption algorithm, such as the Advanced Encryption Standard ("AES") using a minimum 128-bit (256-bit preferred) length key. Unlike file access restrictions, disk encryption protects information even when the operating system is not active. Disk encryption can prevent unauthorized access when physical security has been compromised, or when the device has been lost or stolen. To demonstrate you are in compliance with this encryption standard, one must: 1. Demonstrate that encryption software is installed and active. 2. A copy of the software manual, screen shot, or other document indicating that the encryption software uses at least a 128-bit length key. Specific Standards for these devices may be found in sections 4.6-4.8.
2.5 Disposal of Personally Identifiable Information and Internal Information	*Standard:* PII must be disposed of securely and in accordance with state and federal laws and regulations, and rules of applicable self-regulatory organizations, when it is no longer needed. Destruction of any books and records documents required to be retained in accordance with the Record Retention Schedule and/or the Record Keeping section of the Advisor Compliance Manual must be pre-approved by LPL Financial Compliance, Legal & Risk Department ("CLR"). Safe Disposal must be accomplished by one of the following means: ▪ Shredding paper records (cross cut or confetti cut versus strip cut) so that reassembly is extremely unlikely. ▪ Destruction of electronic media so the information cannot be read or reconstructed ▪ Contracting with a third party that is engaged in the business of record destruction to dispose of the information
2.6 Information Sharing	*Standard:* All information must only be used for valid business purposes with respect to securities, insurance, investment advisory or other financial service relationships.

Standard	Implementation Standards and Guidelines
2.7 Access to and Viewing of Personally Identifiable Information and Internal Information	*Standard:* ▪ Do not discuss PII with, or in the presence of, persons who have no legitimate business need to know the information. ▪ Do not leave completed applications and related information where others can read or copy such material. When not being used, this information should be securely stored. ▪ PII about customers must not be accessed out of curiosity, for personal use or where a person does not have a valid business relationship with the customer that creates a business need to know the information. These include, 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. ▪ Branch office staff must verify the authenticity of the person to whom they are disclosing PII before that information is disclosed. ▪ Staff must 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, or as contained in the LPL Financial policies and procedures. ▪ Staff must not disclose PII to a customer's spouse, relatives, employer, or retained professionals (e.g., lawyers, accountants, etc.) without the written permission of the customer. ▪ A customer's account number must not be disclosed to non-affiliated third parties. If a customer wants his or her account number given to a third party, the customer must provide such information directly or provide written authorization to do so. PII received from a non-affiliated financial institution may not be directly or indirectly disclosed to any non-affiliated third party unless that disclosure would have been lawful if made directly by the non-affiliated financial institution.
2.8 Emailing Information	*Standard:* All email that is transmitted through an lpl.com email address or an email address journaled to LPL Financial is subject to review and supervision by LPL Financial. Email that includes PII in the body or the attachments must be encrypted when traveling over the public internet; however, encrypted or password protected attachments are prohibited, as they interfere with the supervisory process. The subject line of an email cannot be encrypted and, therefore, may not contain PII. If you use an LPL.com or LPL hosted email address to send PII to a non-LPL.com email address, you must enter " [secure]" or "[encrypt]" (including brackets as shown) in the subject field of the message. **Self- Hosted Journaling Firm Encryption Solutions** Journaling firm's encryption solution must meet the below encryption standards or obtain an exception from the CLR Email Team. • The encryption process must be triggered by a unique key word in the message subject or a unique entry in the message header. • Unique key word or header entries must be pre-approved by LPL Financial. • Encrypted messages must be protected using a key cipher length of at least 128 bit, though 256 bit is preferred. • The firm's encryption system must not interfere with the email journaling process or the LPL archival or supervision systems. For a full list of journaling encryption requirements, please refer to the Electronic

Standard	Implementation Standards and Guidelines
	Communications Chapter of the Advisor Compliance Manual.
3.0 Physical and Administrative Security and Business Continuity	
3.1 Access to Physical Locations	*Standard:* Access to physical locations where PII is stored or used shall be restricted to authorized persons with a legitimate business need.
3.2 Lock and Secure Offices	*Standard:* Lock and secure all offices containing PII; keep keys and entry devices secure. Where possible, prevent unauthorized individuals from accessing areas where sensitive information is stored or readily accessible.
3.3 Secure and Control Access	*Standard:* Secure and control access to dedicated computers, printers, copiers and fax machines. This includes locked doors, card access readers, security systems, isolating the location of equipment so that only appropriate staff has access to it, and procedurally segregating staff responsibilities and access to equipment, etc.
3.4 Protect Computer Equipment and Facilities	*Standard:* Protect computer equipment and facilities against fire, flood and other environmental hazards. Such protections 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.
3.5 Establish Procedures for the Secure Handling of Mail and Mail Forwarding	*Standard:* If you ship sensitive information using the United States Postal Service (USPS) or outside carriers or contractors, keep an inventory of the information being shipped; and ensure material is sufficiently protected during transit. Electronic media containing PII sent via the USPS, outside carriers or contractors must follow the encryption guidelines in section 2.4. Unnecessary PII on hardcopy documents should be "blacked out" or masked if possible. Be sure you know what information is being shipped. In the unfortunate event the information gets lost, you will need to contact the Security Incident Hotline (866) 578-7011 or security.mailbox@lpl.com and report exactly what information was lost. The Privacy Office will help you identify the appropriate next steps during the loss of a shipment of sensitive data.
3.6 Shared Offices	*Standard*: There must be separate printers and fax machines for each firm. The LPL fax machine and printer must be in a secure area.
3.7 Personnel Change Notification	*Standard:* Immediately notify the LPL Financial home office of any branch office personnel changes (terminations, new hires or other changes within the office). Physical and electronic access to PII must be blocked immediately upon termination, including ensuring passwords, user names, email, internet access, and voicemail of terminated personnel are deactivated. Terminated personnel are required to immediately surrender all keys, IDs, badges, business cards, computer equipment or PDA's and other items which permit access to the LPL Financial physical premises and electronic systems.
3.8 Regulatory checks	*Standard:*

Standard	Implementation Standards and Guidelines
	Regulatory and background checks through LPL Financial are required for all personnel that may come into contact with PII. LPL Financial performs these checks automatically once notified of personnel hires.
3.9 Business Continuity	*Standard*: 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 to determine whether any modifications are necessary in light of changes to the branch's operations, structure, business, or location.
4.0 Technology Security - Every advisor is accountable for <u>actively</u> monitoring the software programs installed on computers in your office for compliance with the BOSP. It is up to you to ensure programs meet the standards in this section by ensuring they are installed appropriately, receive updates/patches, and are supported by the developers. Failure to do so is a violation of the BOSP. **In addition to the standards listed below we strongly recommend whole disk encrypting desktop computers. Failure to do so may result in breach notification costs to your office if an unencrypted desktop is misplaced or stolen.**	
4.1 Password Security and Expiration	*Standard:* ▪ Passwords to decrypt a computer or access a desktop must be kept confidential and should never be shared, whether at home or at work. ▪ Passwords that provide access to applications containing internal information or customer PII must be changed at least once every 90 calendar days. ▪ If passwords must be emailed they should never be included in the same communication as their corresponding username or file that they will be used to access. ▪ Temporary passwords must be changed immediately upon receipt. ▪ Password manager software may be used so long as the software requires a master password and encrypts the passwords in storage. ▪ Password lists can be saved on a written document stored in a locked drawer. ▪ Storing or caching passwords in your internet browser is prohibited. ▪ One Time Password (OTP) devices, such as tokens, must use passwords at least five characters in length and must not change in a predictable way. ▪ The use of fingerprint scans or biometric authentication may not be used in lieu of a password. ▪ Passwords must be changed whenever there is an indication of possible system or password compromise. ****LPL Financial will never ask you to reveal your password**** *LPL Financial Baseline Standards for Password Strength:* Access to any application containing or providing access to PII must have a minimum password strength that is at least eight characters containing at least three of the following elements: ▪ Numbers

Standard	Implementation Standards and Guidelines
	▪ Upper case letters ▪ Lower case letters ▪ Special characters (Characters not classified as numbers or letters such as "~!@#$%^&*") Eight character password requirements pertain to desktops, laptops, and third party applications, while a four character password is sufficient for accessing voicemails. However, if third party applications cannot support the LPL Financial password requirements then the password configuration must be as strong as the application allows. Enforce a strong password standard on all computers and/or your entire windows domain using windows local and group policies. You must be able to confirm upon examination that you are compliant with this password standard.
4.2 Server Administration	*Standard:* Server Administrator accounts are used to manage a server or an application. Unlike a regular user account access, an administrator account has elevated privileges on the server or application. Server administrator passwords have the additional requirements of being unique from all other passwords held by an administrator's personal account. These accounts must automatically lock-out after three unsuccessful logins. If account lockouts are not feasible, the account must have a minimum password length of 16 characters.
4.3 Firewalls	*Standard:* Any computer that accesses the internet must be protected by a software firewall. If your operating system comes with a firewall, enabling it will satisfy this requirement. If multiple computers in an office share an internet connection, that connection must be protected by a hardware firewall as well. If the firewall (router) has wireless capability that is not being used, it must be disabled.
4.4 Antivirus and Anti-spyware Software	*Standard:* Antivirus and anti-spyware software must be installed on **all** computers, including both PC's and Macs, be supported by their developers and configured to automatically check for, download and install updates. Antivirus programs must be configured to actively scan files in use and perform a

Standard	Implementation Standards and Guidelines
	full scan of all files at least once a week. Check your software instruction manual for instructions on how to verify that your virus and spyware definitions are up to date and how to configure the software to automatically update.
4.5 Operating Systems and Software Security Updates	*Standard:* Operating Systems must be supported by their developers and configured to automatically check for, download and install security updates. Software applications must also be kept up to date with the latest security patches. Many vendors provide auto-update functionality in their products to facilitate this process whereas others require their users to manually download updates from their web site. Check with your software manufacturers to ensure your products are receiving security updates. Ensure that updates are compatible with your operating environment. Security updates that are not automatically installed must be installed as soon as possible.
4.6 Encryption of Data on Portable Media	The LPL Financial definition of portable media: Portable media includes removable storage, flash drives, Smart cards, USB drives, CDs, DVDs, and removable storage for cell phones and personal digital assistants (PDAs). *Standard:* PII stored on any portable media or portable computers and devices must be encrypted. If you are unsure of how to buy and/or install encryption software you should consult a local information technology consultant for assistance.
4.7 Laptop Encryption Requirement	LPL Financial definition of laptops: traditional laptops, tablet PCs, and Ultra Mobile PCs (UMPC). *Standard:* All laptops used for LPL Financial business must be encrypted with full or whole disk encryption installed locally on the laptop. The vendor shall guarantee a secure, tamper-proof environment external to the operating system as a trusted authentication layer with pre-boot authentication (see FAQs for further details relating to compliance with this requirement). Only technically/developmentally supported software will be considered compliant.
4.8 Securing Smart Phones, tablets, and PDAs	LPL Financial definition of smart phones, iPads and PDAs, includes but is not limited to: RIM Blackberries, Apple iPhones and iPads, Windows Mobile/CE, and Android devices. *Standard*: Devices that are used to view, process, store or transmit LPL Financial data, confidential or otherwise must have the following controls in place: 1. Devices must require a password to access the device.

Standard	Implementation Standards and Guidelines
	2. Passwords must be four characters or greater in length. 3. Failure to provide a correct password to a mobile device after no more than 10 attempts must cause all data stored on the device to be permanently deleted. 4. Removable storage devices used for smart phones and PDAs must be encrypted using a minimum 128- bit (256 preferred) length key. 5. Devices must lockout their user interface after a period of time and require a password to regain access to the device. The lockout must occur after no more than 5 minutes for smart phones and no more than 15 minutes for tablets. 6. Encryption must be activated and configured 7. When a smart phone, tablet or PDA is left unattended, the user must lock the device.
4.9 Computer Virus	*Standard:* If any computer or other device is infected with a virus or other form of malicious software it must not be used until the infection is fixed.
4.10 Computer Screen Lock	*Standard:* All computers which have the capability to, or can be modified to, lockout their user interface shall be configured to automatically do so after no more than 15 minutes of inactivity and require a password to regain access to the device. This standard applies to all computers used to view, process, store, or transmit LPL Financial data. When leaving a workstation unattended the user must lock the screen (e.g. press Control+Alt+Delete, then Computer Lock).
4.11 File-Sharing (Peer to Peer)	*Standard:* Peer to Peer file sharing between branch office computers and computers on the internet is not allowed; however transferring files between branch office computers is allowed. Installing such peer to peer file sharing applications and inadvertently enabling the office's network drive to be shared can make it accessible to unauthorized users not affiliated with your office.
4.12 Public Computers	*Standard:* Use of public computers (internet cafe, hotel business center, etc.) for LPL Financial business is not allowed (including checking email). All computers used for LPL Financial business purposes must comply with this policy and are subject to audit.
4.13 Wireless Use	*Standard:* Public Networks ▪ When connecting to the internet, a physical connection with a network cable is always preferred to a less secure wireless connection. o At no time should a public wireless (WiFi) access point be used, such as those found in coffee shops and airports. Even wireless security protocols like WEP and WPA will not protect you from other users authenticated to the same access point. Remember, anyone can use an access point as long as they put in the same amount of effort into connecting that you did. o Use of a mobile phone hotspot is compliant so long as the hot spot is generated by a device under your control and which is

Standard	Implementation Standards and Guidelines
	otherwise compliant with the password requirements for third party applications set forth in this Policy. Private networks (Office or Home) ▪ Do not use unsecured wireless networks. Use strong passwords with at least 16 characters to restrict access to wireless devices. ▪ Ensure traffic between your laptop and the Wireless Access Point (WAP) is secure and encrypted using at least WPA encryption standards (IEEE 802.11i). WPA2 using AES/CCMP is preferred. The WAP is the device that broadcasts a wireless signal enabling your device to connect to it. The WAP is then attached to the internet and/or the local network, thus enabling your device to connect to the internet and/or the local network. WPA2 is an encryption standard that provides enhanced wireless security. ▪ Wired equivalent privacy standard (WEP) should not be used. There are known weaknesses with this security standard that hackers can exploit. Data is not secure when using WEP. ▪ Disable any wireless radio connections when not in use.
4.14 Bluetooth Connections	*Standard:* Bluetooth and short-distance wireless devices are permitted provided they do not accept unsolicited incoming connections. Device "pairing" must be initiated from a device in your control. Disable any Bluetooth service when not in use.
4.15 Mobile Device Use and Travel	*Standard:* Reasonable measures should be taken to protect mobile devices (e.g. laptops, tablet PCs, portable media, cell phones/smart phones, Personal Digital Assistants (PDAs), etc.) during travel. Such measures include (without limitation): ▪ Do not store mobile devices or other electronic equipment containing PII in checked baggage. ▪ Do not leave mobile devices in plain sight in vehicles. ▪ Do not leave mobile devices unattended in a public place.
4.16 Copiers, Scanners and Fax Machines	*Standard:* Client PII must be kept secure when using copiers, scanners or fax machines. Do not copy, fax or scan personally identifiable information on public machines (e.g. FedEx, Kinko stores, Staples, Office Depot, etc.). The information could be retrieved from the hard drive.
4.17 Use of ClientWorks on Mobile Devices	*Standard:* Only approved mobile devices may be used to access ClientWorks. Approved mobile devices include smart phones and tablets. Use of wearable devices, such as Apple watches or Google Glass, and nontraditional devices, such as internet capable home appliances, are not permitted to access ClientWorks.
5.0 Training	
5.1 Branch Office Staff	*Standard:*

Standard	Implementation Standards and Guidelines
Training	▪ Branch Office Managers are responsible for ensuring that all branch office staff receive the Privacy and Security Training once per calendar year. ▪ Privacy and Security training must be part of new hire orientation; new registered and non-registered employees must be trained within 30-days of employment.
6.0 Use of 3rd Party Service Providers	
6.1 Evaluation	*Standard:* All third party service providers with access to PII must have the capacity to protect PII. As such, you must take reasonable steps to verify that each third party service provider with access to PII and with whom you have a relationship is capable of maintaining safeguards for customers' PII.
6.2 Contracts	*Standard:* All contracts with third party service providers with access to PII must contain provisions requiring that the third party service providers maintain a written information security program in compliance with all applicable laws and regulations. Copies of executed contracts and service agreements are required to be kept accessible for examinations or audits.
6.3 Transmissions	*Standard:* All electronic transmissions of PII between the branch office and the service provider must be secure. This may be accomplished in several ways, for example: ▪ Use of a VPN (virtual private network) connection, ▪ Use of a dedicated line, ▪ SSL or TLS encryption utilizing a minimum of 128 bit (256-bit preferred) key.
6.4 Storage	*Standard:* It is critical to confirm the storage location of all customer PII before executing contracts with any third party service provider. All customer PII should be stored within the United States, and not offshore at a vendor location. When data is stored with a service provider, and that service includes encryption capability, the data must be encrypted utilizing industry approved algorithms utilizing a minimum of 128-bit (256-bit preferred) length encryption key. 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 include: ▪ Multifactor Authentication ▪ Firewalls ▪ Intrusion Detection and Intrusion Prevention Systems ▪ Current Antivirus and Patch Management Procedure ▪ Physical access controls
6.5 Due Diligence	*Standard:* It is the responsibility of the Branch Office to perform due diligence on any service provider prior to executing a contract and engaging them to provide services to assure that appropriate security measures are in place with regard to the protection of PII.

Standard	Implementation Standards and Guidelines
	Service providers shall have appropriate information security and privacy policies in place that govern the protection of customer PII and prohibit any reuse of such customer PII without the consent of the customer. Service providers should also provide prior notice to any changes in their security or privacy policies that would impact the customer's business. Terms of Use for online services should be carefully reviewed, as they may constitute a contract with the user of the service. Terms of Use containing provisions allowing or providing some type of license to the service providers 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. This Policy should be consulted for guidance on what to look for when engaging a service provider since the same standards that are applicable to advisors ought to be applicable to any service provider that is handling customer PII. All questions related to these procedures should be referred to the Privacy Office.
7.0 Compliance and Reporting	
7.1 Compliance	*Standard:* Branch Managers are required to annually attest to the compliance of their respective branches with this Policy and should have procedures in place to ensure continual compliance.
7.2 Reporting	*Standard:* Any security incident or violation, whether confirmed or suspected, of this Policy should be reported immediately to the Privacy Office via the Security Incident Hotline 1-866-578-7011. If you lose PII, as defined in this Policy, you should not take any action until you speak with the Privacy Office. You are required to cooperate with the Privacy Office, which will work with you to take the necessary actions to respond to any security incident. **Remediation steps may include client and/or Attorney General notification and providing credit monitoring services for affected clients, the costs of which will be transferred to the appropriate LPL Branch Office or Financial Institution.** Branch Offices are required to keep a record of all security incidents accessible for audit. Financial services firms are some of the organizations that suffer the most from a security breach. On average, the per capita cost of a data breach for a financial services organization is $336* per compromised client account record. This cost includes things such as lost business, client notification costs and resources allocated to respond to the breach. ** Data acquired from a June 2017 report published by Ponemon Institute, LLC study.*
7.3 Policy Violation	*Standard:* It is a violation of this Policy to disable, bypass, circumvent, or otherwise attempt to negate the security measures of LPL Financial. Any individual found in violation of this Policy may be subject to disciplinary action, including possible monetary penalties, termination of affiliation with the

Standard	Implementation Standards and Guidelines
	firm, or legal action depending on the severity of the violation.
7.4 Questions	*Standard:* Answers to common questions may be found in the Branch Office Security Policy FAQ located on the Resource Center. Additional questions about this Policy should be directed to your home office Compliance and Technical Support contacts listed below: **LPL Financial** Technical Questions: (800) 877-7210, ext. 6357 Policy Questions: (800) 877-7210, ext. 6835 **LPL Financial Institution Services** **Technical Questions:** 1 (866) 321-3640, option 3 **Policy Questions:** 1-(866)-321-3640, option 4