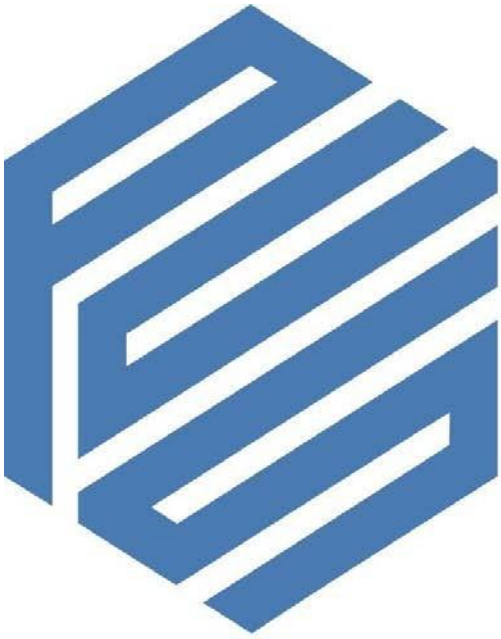

PRIVATE CLIENT SERVICES™

MEMBER FINRA, SIPC
A Registered Investment Advisor

Summary

Information Security Policy

Revised 1-25-2019

Section **Page**

Compliance with the following provisions is intended to ensure the confidentiality, integrity, and availability of corporate information assets. These provisions are excerpted from Private Client Services' Information Security Policy. If you have any questions or any recommendations regarding this document, please send them to PCSHelpdesk@pcsbd.net.

Private Client Services, LLC is committed to fulfilling its' regulatory responsibilities and believes the broad interpretation of this responsibility and articulation and adherence to our beliefs is part of our "Corporate Culture".

It goes beyond protecting customer data and includes as examples, in addition to many other responsibilities: promoting the high standards of adhering to software licensing agreements, aversion to sharing logon(s) and password(s), promotion of adhering to previous employment and registration agreements entered by prospective employees and registered representatives and their affiliated personnel.

The firm believes that all work product created by an employee of Private Client Services, LLC is intellectual property belonging to the firm. The intellectual property of the company should always be kept secured and confidential. This property of Private Client Services, LLC should not be used outside the firm, copied on any personal device and remains the property of the firm following the termination of employment of the individual who created it for the company while employed by the firm.

Corporate Information Protection Policy

- Private Client Services recognizes that information is its prime asset. Information provides the foundation for our business decisions; its accuracy, integrity and uninterrupted delivery is key in the ongoing and increasing success of this organization. Whether this asset is represented as "data", "information", or the "information systems" used to store, transmit, and process the asset, it will be protected and treated as a secure, trusted resource. Private Client Services will define a comprehensive information security program for the purposes of protecting, controlling, processing, storing, and communicating information. This policy, together with its associated standards, provides the framework for this program.

- All employees, contractors, and non-affiliated third parties are responsible for safeguarding Personally Identifiable Information (PII Data) (see below, "Information Classification Standard") and for protecting and respecting customer privacy. Individual and institutional customer Information is to be used only for the purpose for which it is intended, and *anyone accessing customer Information is prohibited from making personal use of such customer Information or providing it to unauthorized parties.*

- Employees, consultants, contractors, and vendors will adhere to a "clear desk" (also known as "clean desk" in some locations) policy to reduce the risk of unauthorized access, loss of, and damage to sensitive information. The "clear desk" policy will include the following provisions: - PII Data (see, "Information Classification") must always be safeguarded. In addition to the "clear desk" policy, electronic documents should remain in encrypted form and not copied to personal devices.

    - Documents containing PII Data must be placed in locked file cabinets, desk drawers, credenzas, or other secure locations at the end of each workday. Documents containing other classifications of information must be placed in a secure location at the conclusion of each workday, depending upon the sensitivity of the data.

    - Documents containing PII Data, when printed, should be cleared from printers immediately.

    - The "clear desk" policy will be enforced by local departmental, unit, or divisional management.

- An employee, consultant, contractor, or vendor who neglects to comply with the provisions of Information Security Policies and Standards will be subject to corrective action, up to and including termination, and, where appropriate, criminal or civil proceedings under applicable laws.

Information Classification Standard

Private Client Services will identify and classify information as Highly Confidential, Internal Use Only, or Public.

Highly Confidential Information

Highly Confidential Information includes information that, if improperly disclosed, could result in considerable harm to Private Client Services or its clients. In general, information of this nature is disclosed on a need-to-know basis only and is not widely circulated or

shared within Private Client Services. Types of Highly Confidential Information are described below.

A. Personally Identifiable Information (PII Data)

Private Client Services is committed to ensuring the privacy and confidentiality of personal information associated with employees and clients, as well as personal information provided to us by our institutional clients such as information concerning their customers, shareholders or beneficiaries. Our major objective is to ensure that PII Data is not disclosed to unauthorized parties and used to promote identity theft or other types of fraud. An additional objective is to facilitate compliance with privacy laws and regulations promulgated by federal, state, and local governments.

Within the United States, PII Data includes all information that meets the test shown below.

Within the United States, Personally Identifiable Information includes:[1]

• an individual's:
  ○ first and last name or
  ○ first initial and last name, or
• any personal identifier that could be used readily to identify an individual,

in combination with:	
any **one** of the following data elements:	**or** any **two** of the following:
• A full Social Security number • Driver's license number • Passport number • Alien registration number **Or** • A unique account identifier, electronic identification number, username or routing code together with any associated security code, access code, or password that is required for an individual to obtain money, goods, services or anything of value • A financial account number or credit or debit card number • Information pertaining to a financial transaction involving cash or securities **Or** Health information relating to the past, present, or future physical or mental health or condition of a specific individual, or the provision or payment of health care to an individual **Or** Compensation and benefits information relating to a specific individual	• Home address or telephone number • Mother's maiden name, if identified as such • Month, day, and year of birth • Email address

Highly Confidential Information includes PII Data as described above, and further includes, but is not limited to, the following:

B. Any material, non-public information pertaining to Private Client Services, our clients, or third parties, such as:

- Merger and acquisition activity prior to announcement.
- Any information concerning due diligence matters; - Private Client Services financial information prior to release

C. Information protected under attorney/client privilege.

D. Suspicious Activity Reports (SARS) and incident reports.

E. Results of regulatory examinations.

F. Findings of internal and external auditors.

G. Threat and vulnerability assessment findings.

H. Technical or security information the exposure of which might result in a breach of information defined in this category (e.g., passwords, documents pertaining to network/application security architecture or technical infrastructure).

Possession of some forms of Highly Confidential Information may make the holder liable to compliance with certain regulations.

[1] For the purposes of this policy, *individual* refers to any natural person, for example any PCS employee, a person who is a PCS client, or a person who is a client of or otherwise associated with an institution which is a PCS client.

Internal Use Only Information

Internal Use Only Information includes information that may be commonly shared or circulated within the Private Client Services; however, dissemination to external parties must be controlled.

Examples of ***Internal Use Only Information*** include, but are not limited to, the following:

- Lists of employees.
- Address books.
- Private Client Services telephone lists.
- Internal communications.
- Organization charts.
- Information available on Private Client Service's intranet sites.

Public Information

Public Information includes information pertaining to Private Client Services and its products and services and that management has specifically approved for public release. This category also includes research, and information gathered on clients, that is available in the public domain.

Examples of ***Public Information*** include, but are not limited to, the following:

- Published annual reports.
- Published press releases previously approved by senior management.
- Marketing brochures; - Information available at public websites of Private Client Services.

• Information included in all electronic applications, databases, and systems (including email, shared drives, and other electronic storage media) or in business processes (including printed

forms and computer-generated reports) will be classified in accordance with the categories described above. The results of this classification effort will be documented. Data Owners will be responsible for classifying information that they create and/or receive.

- In most instances, information consists of a "package" of specific data elements. Files, databases, applications, emails, reports and other sources of information will usually contain many kinds of data. Although each of these data elements may be associated with a specific classification type, the entire information package is also given a classification; it is this classification that will determine the applicable security controls (see above). If a "package" of information contains data elements with differing classifications, then the entire "package" will be classified at the level of the highest classification represented by the data contained within. Thus, if a report contains "Highly Confidential" information and contains "Internal Use Only" information, the complete report is classified as "Highly Confidential."

- If Data Owners are uncertain concerning the assignment of a level of classification to a specific "package" of information (see above), the information will be classified at the higher level of possible classifications.

Electronic Mail Policy

- Use of Private Client Services' electronic mail systems to copy and/or transmit documents, computer software, or information protected by copyright or in violation of license agreements is strictly prohibited. Use of the electronic mail systems to engage in illegal activities or communication that violates Private Client Services' policies, including but not limited to transmission of messages that are discriminatory, offensive, defamatory, sexual, pornographic, illegal or harassing in nature, is prohibited. The creation or distribution of chain letters or other messages that might interfere with the Private Client Services' use of its electronic mail facilities, or other companies' use of their electronic mail facilities, is prohibited. Employees, consultants, contractors, or vendors must not transmit any unsolicited bulk electronic mail (spam) or engage in activities that have the effect of facilitating spam. Collecting, or attempting to collect, personal information concerning third parties without their knowledge or consent is prohibited. Employees, consultants, contractors, and vendors should conduct electronic mail communication in the best overall interests of Private Client Services. All electronic mail is considered the property of Private Client Services, LLC.

- Private Client Services reserves the right to monitor the use of electronic mail facilities. Information associated with unauthorized use or illegal activities that is collected because of monitoring may be provided to law enforcement agencies, and information associated with inappropriate conduct, including communications inconsistent with Private Client Services policies and procedures, may form the basis of disciplinary action, up to and including termination.

- No employee, consultant, contractor, or vendor may publicly disclose information about Private Client Services or make representations on its behalf without proper authorization. No employee, consultant, contractor, or vendor may forward confidential, proprietary, or restricted information to any outside party or organization unless the individual has been authorized in writing by management to do so, and appropriate steps are taken to protect the information from unauthorized disclosure. This especially includes PII Data.

Internet Security Standard

- Internet access is restricted and monitored. Any usage deemed inappropriate is subject to corrective action including termination.

- Users must not copy nor distribute downloaded copyrighted materials unless permission for dissemination is granted by the copyright owner.

- Inbound connections from the Internet to any Private Client Services' computer or network are restricted to connections from Private Client Services-approved Internet service providers to secured systems attached to restricted areas of the Private Client Services network designated to receive such traffic.

- Transmission of PII data over an untrusted, open network (e.g., the Internet or lines of public carriers) must be encrypted.

Information Security Incident Reporting Standard

- An "information security incident" is any actual or perceived violation of information security standards, policies, or procedures that puts sensitive or customer data at risk. An incident must be reported immediately to either the Chief Compliance Officer or IT Manager if the violation exposes, or has the potential to expose, Private Client Services' information to unauthorized parties; or that results in the unauthorized alteration or destruction of information; or that attempts to or results in the unauthorized access of information processing resources. An information security incident may involve technical resources (e.g., an application, system, or computing device) or non-technical matters (e.g., lost tapes or hard copy reports).

- Questions concerning whether an incident should be reported should be directed to the CCO or IT Manager.

- Examples of information security incidents that must be reported include, but are not limited to, the following:
  - Unauthorized use of a user's logon id and/or password
  - Attempt to access data for which the user is not authorized
  - Inappropriate modification or deletion of data by an authorized user
  - Loss or theft of an electronic device containing Private Client Services information
  - Divulging the contents of Private Client Services information classified other than Public in an inappropriate manner or to an unauthorized individual
  - Unplanned, accidental, or unauthorized change to the existing security control environment (e.g., the accidental disabling of a network security control or of an authentication system)
  - Attempt to cause a system or network device to malfunction
  - Transmission of PII Data via an open network (e.g., the Internet) without the use of encryption
  - Touching or tampering with any desktop computing device containing material evidence relating to possible illegal activity, Code of Conduct violation, or serious security breach
  - Misuse or abuse of system or application privileges
  - Loss or theft of tapes or hard copy reports containing Private Client Services' information
  - Email messages that violate any Private Client Services' policies (see, "Electronic Mail Policy," for additional details)

Questions concerning to whether an incident should be reported may be directed to the IT Manager. Inappropriate or unauthorized disclosure of PII Data is a violation of federal privacy regulations and may also be a breach of state privacy laws. Inappropriate disclosure of this information may require reporting to regulators and/or notification of consumers affected by the breach. Persons reporting an actual or suspected incident involving the disclosure of PII Data must contact either the IT Manager, Chief Compliance Officer, President or CEO of Private Client Services.

- Incidents involving potential criminal or civil matters, including fraud, should be reported directly to Chief Compliance Officer.

- All employees are responsible for reporting actual or potential information security incidents directly to the IT Director. The reporting of lost and stolen electronic devices containing Private Client Services' data is paramount.

- All departments, brokers, and other grouped personnel must prepare documented procedures describing the processes by which regulatory authorities and consumers will be notified if PII Data has been lost or inappropriately disclosed.

- Loss or theft of the following electronic devices will be reported to IT Manager if the device contains Private Client Services' information of any kind:
  - Computers
  - Mobile Devices - Portable electronic storage media (for example, USB devices, CDs, floppy disks). Copying to portable storage devices has been disabled in the PCS network.

- Private Client Services-issued devices, as well as personally owned equipment, must be reported.

- Reports of information security incidents will be documented and include the following information:

  - Name, department, and telephone number of individual reporting incident
  - Date of report submission, and description of incident
  - Way violation was detected
  - Type of violation along with time, date and users involved
  - Securities involved (name and symbol)
  - Details of trades or unexpected orders
  - Application or system where violation occurred
  - Details of any wire transfer activity
  - Customer impact (accounts affected, will customer be reimbursed, if yes by whom?) - Regulatory compliance concerns
    - Potential impact to Private Client Services (financial or otherwise)

- Reports will be sent to the Information Security Group. All documents pertaining to the report will be considered Highly Confidential information and accorded appropriate security controls (see above, "Information Classification")

Media Destruction Standard

- The method of erasure, destruction, or disposal of electronic media (including hard drives, DVD's, cd's) or data must be approved by the IT Manager.

- The erasure, destruction, or disposal of media must be documented whether media is given, sold, or distributed to third parties (including third parties responsible for the disposal of media). Documentation will provide a record that erasure, destruction, or disposal has in fact, occurred. This record will be kept on a secure file by the IT Manager.

- Documentation of the erasure and/or destruction processes must be retained for no less than one year if the erased data (or the most sensitive data on a destroyed device) has been retained for the full period of time required to meet regulatory requirements. However, if the erased or destroyed data has not been retained for the time required by regulation (e.g., the destruction was caused by

an unforeseen event), documentation of the disposal must be kept for three years. Documents certifying the erasure or destruction of data must be removed to off-site storage following the required period of on-site retention; the total period for certifications of erasure or destruction is seven years.

- The IT Manager will establish procedures for the destruction of all media and the erasure of nonpublic personal, restricted, confidential, and proprietary data. These forms of sensitive information must be properly protected during the destruction/erasure process so that unauthorized access to data does not occur. Also, a verification process will be established by the management of business units to ensure that no residual nonpublic personal, restricted, confidential, or proprietary data can be identified after the data/media disposal process is complete. These precautions will apply to disposal processes conducted by Private Client Services' staff as well as by third parties, such as service providers, who are contracted to perform disposal services. Media will not be destroyed or disposed of or data erased until the media/data have been retained for the length of time required by regulatory or other legal requirements and as documented by the records retention schedule for each business unit, sector, or division. Also, media/data should not be destroyed if they contain information relating to pending litigation. Questions concerning the mandatory retention periods for specific types of information should be referred to the Records Management Department (or to an equivalent administrative entity) or to the appropriate Compliance Officer. Questions about information that may relate to pending litigation should be discussed with the Legal Division.

- If an old PC is being discarded/recycled, the hard drive must be removed from computer case. The hard drive may stay in possession of the IT Manager or the hard drive may be destroyed by local vendor.

Secure Transport and Storage of Physical Media

All PCS Personnel are responsible for determining the level of risk associated with physical media that is transported from one location to another. Data Owners of specific applications may assist in this risk assessment process. This determination should be based upon an analysis of risks associated with the loss, theft, or unauthorized disclosure, modification, or destruction of data resident on the transported media. All transported media must remain encrypted.

The type of data stored on transported or stored media is one significant factor to be considered when analyzing risk (see below).

- Highly Confidential Information requires the strongest security controls. (See, "Information Classification," for additional information concerning security controls that are appropriate for Highly Confidential Information.). If a specific physical medium, contains several types of data (e.g., Highly Confidential and Internal Use Only), then the level of control required to secure the information should correspond to the most sensitive data residing on the medium.

- When assessing the risk of potential disclosure of Highly Confidential Information, business units, divisions, data centers, and other relevant administrative entities must consider the content of the information contained in the media. If, for example, a paper report, optical disk, or other media contains sufficient information to permit consumer identity theft, then the data represents a high risk and must be protected accordingly. Thus, a paper report containing consumer name, account number, and account balance must be assessed as high risk. However, a report containing only account numbers will represent a lower risk; unauthorized disclosure of account numbers represents a risk to Private Client Services' reputation, but consumer identities cannot be comprised with this information alone. An additional factor could be the relative volume of information contained in the shipment.

Therefore, the assessment of risk must be based upon the specific kinds of information contained on media, the method of transportation, and the possible effects of unauthorized disclosure, modification, or destruction.

- For purposes of the survey (see above), risk will be assessed as High, Medium, or Low.

Types of Media and Appropriate Security Controls

Digital Data and Media

- Digital data may not be stored on unencrypted media (e.g., magnetic tape or disks, DAT or VHS cartridges, CD or DVD optical disks, or USB drives). If these media contain PII Data, then business units, working with their Technology support staff or data centers, should ensure that the data is encrypted where required by law or regulation, and also where the business unit deems appropriate after giving due consideration to the risks of unauthorized access. Where encryption is not used, business units must employ other appropriate control measures to protect the information. Consideration should be given to controls that would be deemed customary and reasonable practices; for example, using shipping companies that provide package tracking as opposed to regular mail service, and transporting media in sealed shipping containers. In addition, access to media may be protected by means of electronic and physical access controls.

- PCS Employees should avoid transport of electronic medium that contains PII Data. The electronic transmission of these data, with appropriate network and encryption controls, provides a more secure means of transport. However, where transportation is necessary, controls as listed under Non-Digital Media should be considered for risk mitigation.

Non-Digital Media

- Non-digital media include, most typically, paper, microfilm, and microfiche. These media cannot be encrypted or password-protected; they must be secured by ensuring that the container within which they are transported or stored is appropriately secured. Non-digital and digital media containing PII Data should be secured in a briefcase or other such item and stay near the PCS Employee. Media containing information of any type and transmitted by any means should be, at a minimum, shipped in containers sealed with tamper-resistant strapping and tamper-evident seals. Private Client Services' personnel, rather than external shippers, should secure containers. Media should be enclosed in bubble wrap prior to shipment. If media are transported in a box, the contents should be double boxed to secure against inadvertent loss if the outer container or seal is broken. An advisory message, securely attached to the inner container and clearly visible, should state: "IF YOU ARE NOT [Name of intended recipient], DO NOT OPEN. PLEASE CONTACT [Telephone number of sender] TO ARRANGE FOR THE APPROPRIATE RETURN OF THIS PACKAGE." Private Client Services will assume expenses for return shipment. Specific methods for ensuring the confidentiality and security of shipping containers should be selected based upon determination of what the potential impact could be if the media are lost or stolen, or if the content is compromised.

Vendors and Service Providers

- PCS Associates should review the security controls implemented by their current shipping or mailing methods (e.g., private courier, public shipper). If controls need to be upgraded to prevent loss, theft, or unauthorized access to sensitive Private Client Services data, negotiations should be conducted with the shippers; alternatively, it may be necessary to select another means of transport.
- PCS Employees and Associates at the Home Office are responsible for ensuring that the front double doors are closed at all times, and the Operations Door is secured against loss or theft of Private Client Services' property.
- Prior to engaging the services of a third party for the purpose of transporting data, business units and data centers should ensure that contractual agreements with vendors and service providers include provisions that ensure, at a minimum, the implementation of appropriate security controls. Contracts should require vendors to implement procedures designed to protect data. In addition, vendors and service providers should sign nondisclosure

agreements protecting the confidentiality of sensitive Private Client Services' information. Finally, vendors and service providers should be contractually required to promptly investigate and report the loss or theft of Private Client Services' information under their care.

Reporting Security Incidents Involving the Loss or Theft of Transported Media

- If media are lost, stolen, or accessed in an unauthorized manner while being transported from one location to another, the business unit or data center originating the transport must promptly report the incident to the IT Manager.

Securing Media While in Storage

- PCS Employees should review the security controls implemented by the sites that store media, including service providers that offer data archiving facilities. If controls need to be upgraded to prevent loss, theft, or unauthorized access to sensitive Private Client Services' data, negotiations should be conducted with current service providers; alternatively, it may be necessary to select another means of storage. Business units and data centers will verify the accuracy of the inventory of stored media on at least an annual basis. If specific media cannot be accounted for, the Information Security Group should be notified of the incident.

- Contracts with vendors and service providers responsible for the storage of Private Client Services' data should contain the same provisions as those previously mentioned for vendors/service providers that transport data.

Information Security Access Control Standard

- Access to any platform and/or network by anyone other than an employee of the Private Client Services must be requested through the email address PCSHelpdesk@pcsbd.net. Access is strictly regulated.

- Special system privileges (such as administrative rights) will be restricted to only those individuals directly responsible for system management and/or security.

- The PCS login account of a departing or suspended employee, consultant, contractor, or vendor will be suspended by the IT Manager. Access to the account, including emails, files stored on the file server and other such data will be determined by the CEO or reporting manager.

- PCS Employees, third party consultants, contractors, or vendors must not access, or attempt to access, the accounts of others.

Identification Standard

- All requests for identifiers will be authorized and approved through the Private Client Service's standard authorization process.
- All user accounts will be associated with a specific employee or other individual by means of a unique identifier assigned to the employee, consultant, contractor, or vendor.
- To reactivate a disabled account, authorization must come from CEO or President and is done by the IT Manager.
- When an employee, consultant, contractor, vendor, or other individual is separated from Private Client Services or transferred from or been reassigned within a business unit, the IT Manager will be notified immediately by reporting manager to remove all identifiers associated with the individual.
- Controls will be in place for the establishment of identifiers for non-employees (e.g., consultants, contractors, vendors, customers, service providers). These controls will ensure that each nonemployee user is provided an identifier by an authorized administrator and that each user is associated with a unique identifier, that the activities of non-employee users are tracked and monitored, and that each identifier is deleted when the non-employee user no longer requires access to Private Client Services' resources.

Authentication Standard

- Multi-factor authentication (the use of at least two forms of authentication to gain access to an application, network, or other system) must be utilized if risk assessment determines that compensating security controls for an application, network, or system are not sufficient to mitigate the potential for identity theft and/or risk of fraud.
- Passwords will be changed immediately when a breach of confidentiality is suspected.
- Passwords will be reset by the IT Manager only after the associated user has been positively identified.
- Sharing and/or disclosure of passwords and other authenticators are prohibited.
- Passwords and other authenticators will not be stored in hard copy.
- It is the responsibility of every user to protect the confidentiality of their passwords or other means of authentication.
- Passwords or other means of authentication will not be stored in any file, command list, procedure, or macro where they are susceptible to disclosure or use by anyone other than the owner.
- Password vault software can only be used with IT Manager's approval.

- To combat intrusion and increase security, passwords must be a minimum of 10 characters. It must include a combination of at least Three of the four characters: one alpha, one numeric, one special character, and capital letter. Do not make any part of your first or last name as part of the password.

- Associates will be prompted to change their passwords every 45 days.

Device Security Standard

- All data resident on Private Client Services-owned personal computing devices and equipment (including, *workstations, personal computers, PDAs, mobile devices, portable data storage devices)* are the property of the Private Client Services.

- Any Private Client Services-owned computing device or equipment containing material evidence relating to possible illegal activity, Code of Conduct violation, or serious security breach must not be physically touched or in any manner tampered with until the suspected activity has been investigated by PCS IT Technology

- All Private Client Services-owned computing devices, including laptops, PDAs, and mobile devices, will be equipped with up-to-date and fully operational anti-virus and firewall software and any other required security software. Disabling or interfering with any security software is prohibited.

- All Private Client Services owned devices will have full disk encryption.

- Use of mobile devices to transmit Private Client Services data must be encrypted.

- Consultants, contractors, and vendors that connect to the PCS/VPN network remotely must ensure that they are using the latest approved anti-virus and personal firewall software and that these software programs contain the latest update definitions.

- An automated lock feature associated with Private Client Services devices must be activated after 15 minutes of inactivity. Devices must require the user to put their password to resume the session after lockout. In addition, employees, consultants, contractors, vendors, and service providers must lock their systems anytime the system is left unattended.

- At the end of each workday, users will shut down/power off the PCS device

- Devices and equipment containing Private Client Services' information will be retained in a secured location while unattended.

- Software will not be copied unless such copying is consistent with relevant licensing agreements and has prior management approval.

- Individuals using Private Client Services-owned computing devices will not download software (including free and open-source software) from external communications network sources. Also, individuals using Private Client Services-owned computing devices will only use software that has been approved by the IT Manager.

- Users who download Private Client Services' information assume responsibility for the confidentiality of the data. These downloads may occur only if a clear business need has been

established, and the user has received approval for download privileges from the Data Owner. In addition, the device to which data is downloaded must be secure and information must be encrypted if warranted. “Secure”, in the context of this standard, means that devices must be (1) physically safeguarded against theft, (2) accessible only by means of a confidential password or other identification/authentication mechanism, and (3) equipped to provide data encryption.

- Private Client Services’ management authorization is required before devices and equipment (e.g., laptops, hard disks, floppy disks, other portable data storage devices, and hard copy reports) containing Private Client Services’ information are removed from Private Client Services’ premises.
- Any server or other system containing material evidence relating to possible illegal activity, Code of Conduct violation, or serious security breach must not be physically touched or in any manner tampered with until the suspected activity has been investigated by IT Manager.