



Memorandum

TO: ALL CONTINGENT WORKERS
FROM: STAFFING (NON – FTE)
RE: CONTINGENT WORKER POLICY AND RESTRICTIONS DOCUMENT

.....

TABLE OF CONTENTS

Contingent Worker – Introduction to Wellington 2

Code of Ethics Policy 9

Policy on Property and Confidential Information 24

Error Resolution Council – Annual Update 26

Mobile Devices Standard Policy..... 27

Information Security Policy..... 29

Required Information Security Practices and Restrictions for Contingent Workers 31

Policies and Restrictions Signature Page 38

Please review all of the above documents and sign page 38 to confirm your acceptance and understanding.

Memorandum

TO: All Contingent Workers (Consultants and Temps)
FROM: Staffing
RE: Contingent Worker - Introduction to Wellington

INTRODUCTION

Welcome to Wellington Management Company LLP (Wellington Management). This document details many of the Wellington Management policies and procedures that you will be responsible for following while on assignment. You will need to **sign this document**, acknowledging that you have read through and understand what is required of all contingent workers. Please return this signed document to your vendor, and retain a copy for yourself, prior to beginning work at Wellington Management.

SOLUTIONS CENTER

Please contact the Solutions Center at extension 6-8400 (or externally 617-790-8400) for computer or phone related issues. For non-urgent matters you may also send an email to [#ServiceRequest@wellington.com](mailto:ServiceRequest@wellington.com) or alternatively enter a request through the service catalog in the ServiceNow application found on the intranet.

BUSINESS HOURS

Standard U.S business hours are 8:00 a.m. to 5:00 p.m, however please check with your manager for business hours in global locations. You are expected to work approximately 40 hours per week, unless otherwise previously discussed. Flextime needs should have been addressed prior to accepting your assignment.

BUILDING ACCESS POLICY

When you arrive onsite at Wellington Management you will receive your security badge, it provides access into the Wellington Management office area. As a contingent worker, your badge will allow you to enter the Wellington Management offices between the hours of 6:45 a.m.to 6:00 p.m., Monday through Friday unless otherwise required and approved.

It is important to schedule a time to have your picture taken within 24 hours of your arrival to avoid problems gaining building access.

- If you are in Marlborough contact [#MarlboroughReception@wellington.com](mailto:MarlboroughReception@wellington.com) to schedule a time to have your picture taken.
 - If you are a Boston based contingent worker contact GM-security@wellington.com to schedule a time to have your picture taken.
 - For all locations outside of Massachusetts please contact [#StaffingNonFTE@wellington.com](mailto:StaffingNonFTE@wellington.com) to be pointed in the right direction to schedule a time to have your picture taken.
 - When ready, your picture will be sent to you from the Wellington Management Security Office. (The picture is actually a sticker that you will adhere to your badge). Until you receive your photo, you will need your own photo ID (e.g. license, passport, etc.) to obtain access to the buildings.
-

The Wellington Management Security Office can also provide you with keys for your desk and file cabinets where applicable. If you have any questions or concerns regarding your badge, picture, manual keys, or any security related matters, please feel free to contact the Wellington Management Security Office at extension (617) 236-4357 or via email at GM-security@wellington.com. Please take note of the following:

- Proper authorization is required prior to accessing any Wellington Management facility.
 - All visitors must sign-in at reception.
 - Restricted areas require authorization prior to access being granted, i.e. Data Centers, Wiring Closets, Equity Trading Floor, etc.
 - You may request a loaner badge at reception if you have forgotten your badge. A loaner badge must be returned the same day it is borrowed.
 - In the event your security badge has been lost please contact Wellington Management Security (extension 63150) immediately.
 - The default access for contingent workers is Monday through Friday from 6:45 a.m. to 6:00 p.m. Extended building access may only granted by a formal request made through your Wellington Management Manager.
 - In Marlborough, contingent workers will require an additional badge to access the buildings on evenings and weekends. If this is required please have your Wellington Management contact approve and send the request by emailing #Marlborough Reception.
 - Directories are not be removed from the premises.
-

VISITORS

You are restricted from having personal (non-Wellington Management) visitors within Wellington Management facilities. Please meet with non-Wellington Management visitors (on your own time) outside of Wellington Management offices. This includes meetings with your agencies, friends, and non-Wellington Management co-workers. When your manager requests a meeting with an external party on Wellington Management premises for business purposes, you or your manager must follow the procedure for all Wellington Management visitors:

- You must pre-register visitors with reception (email; #Access – 100 Federal, #Access – 280 Congress, #Access - Marlboro) or as otherwise provided.
 - Visitors must sign in at the lobby security desk and then reception every day that they are on the premises.
 - Visitors must not “piggy back” into Wellington Management offices.
 - Visitors may only be on Wellington Management premises when necessary to conduct Wellington Management business.
 - Visitors must wear their visitor sticker/tag given to them by the building security in a visible place the entire time they are on Wellington Management property.
-

DRESS CODE

Wellington Management is business professional dress. Wellington Management Marlborough is business casual. You are expected to dress in the same professional manner required of employees for each location. Please consult with your Wellington Management manager regarding dress code expectations.

COMPLIANCE AND LEGAL

The Wellington Management Code of Ethics policy is accessible via the Wellington Management Intranet ([NAVIGATE Wellington Central > FIRM > Code of Ethics](#)) and is update periodically. **Please read the policy upon receipt of this document.**

Code of Ethics Requirement for New Hires

The Code of Ethics Compliance (COEC) Team will add all contingent workers who will be on assignment for more than 90 days, to the Code of Ethics Compliance System at the time of their estimated start date. You have **10 calendar-days** upon joining the firm **to file** an Initial Holdings Report and Disciplinary Action Disclosure form, as well as complete the Code of Ethics and Global Anti-Money Laundering Program Training. Missed deadlines are considered a violation of our policy and will be reported to your Wellington Management manager and vendor/employer.

If you are a new hire you must also sign the **Acknowledgement of Wellington Management Code of Ethics** and **return to your vendor/employer**, along with this signed Policies document. If you have any questions about the Code of Ethics document, they should be directed to the COEC team at extension (617)790-8330 or via email to #COECTeam@wellington.com.

IT TIMESHEETS

If you are required to submit timesheets through Innotas, you will receive a notification from #Innotas_Support@wellington.com with information on how to do so. Please make sure to submit all timesheets in a timely manner. Timesheets submitted after close will not be accepted.

ADMIN, TEMP, PROFESSIONAL (NON-IT) TIMESHEETS

Unless otherwise required by your employer, You are required to submit timesheets, supplied by Starpoint, to your manager for approval. Please email wellingtontime@Starpoint.com with any questions or concerns.

END OF ASSIGNMENT

Upon completion of your assignment, all electronic work products should be stored on the agreed upon network drive. Personal drives (i.e C : \) are not intended for document storage. All hardcopy work products must be returned to your Wellington Management manager.

Timesheets must be completed at the end of your assignment (if applicable) and security badges must be turned in to your manager or Wellington Management Security.

SCHEDULED ABSENCES

Please provide your employer/vendor with as much advanced notice as possible of any anticipated time off so alternative arrangements can be made, if necessary, to cover for the absence. We require a minimum of two weeks notification.

UNANTICIPATED ABSENCES

Please endeavor to communicate any unplanned absences as early as possible. Depending on the circumstances and your role, you should be in touch with your employer/vendor first, but if that is not possible escalate to Wellington Management or Staffing through email or phone, as necessary.

CLEAN DESK

You are expected to maintain your desk space in the same professional manner required of employees. Please remove and/or lock away all Wellington Management sensitive/confidential materials whenever you leave your desk.

FACILITIES

Please direct any environmental needs (e.g. change in temperature, need for changes in furniture, ergonomic adjustments, and supplies) to your Wellington Management manager.

Supply rooms are located in all production rooms unless otherwise noted. Kitchen facilities are for the benefit of all. Feel free to help yourself to the items provided and the equipment, but remember to be respectful of others and help to maintain a clean, uncluttered space.

SEATING ASSIGNMENTS

Wellington Management Real Estate has assigned you a specific seat. You are expected to sit in your assigned seat for the duration of your work assignment and not sit in another contingent worker seat or employee seat or office, unless instructed otherwise by Wellington Management Real Estate. Additionally, we ask that you do not remove or disassemble any equipment from its assigned location. If you need a different piece of equipment (cord, wire, keyboard, monitor, etc.) please contact the Solutions Center. The Solutions Center will ensure that you have the appropriate tools that you need to be successful.

It is important that you adhere to this request, and if you have any questions please do not hesitate to contact the Staffing team.

DRUG-FREE WORKPLACE

It is prohibited for any contingent worker of Wellington Management to unlawfully manufacture, distribute, dispense, possess, or use a controlled substance in the workplace. If you are found to have engaged in any conduct prohibited by this policy, you will be subject to immediate termination of your assignment. We will reconsider our contract with your employer for any violations to this policy.

HARASSMENT POLICY

Harassment of any kind is unacceptable behavior at Wellington Management. It is unlawful and may lead to sanctions up to and including termination of contract.

Harassment is any conduct, subtle and not-so-subtle, verbal or physical, in or out of the workplace, which has the intent or effect of unreasonably interfering with an individual's performance at Wellington Management or which creates an intimidating, hostile or offensive work environment. Both men and women can engage in and experience harassment.

Harassment, which can take many forms, may include the following:

- Telling jokes which explicitly or implicitly belittle an individual's sex, race, creed, color, religion, sexual orientation, handicap or disability, national origin, ancestry, marital, veteran or citizenship status or age
 - Making verbal or physical innuendoes that explicitly or implicitly belittle an individual's sex, race, creed, color, religion, sexual orientation, handicap or disability, national origin, ancestry, marital, veteran or citizenship status or age
-

- Verbal or physical conduct of a sexual nature including, without limitation, conduct that expressly or implicitly constitutes a sexual advance or a request for sexual acts or favors
- Creating an intimidating, hostile, humiliating or offensive work environment by means of verbal or physical conduct of a harassing nature
- Subjecting others to obscenity or offensive language

PRIVACY

There may be instances when it is necessary to examine a contingent worker's workspace, desk or systems, including email, voice mail and fax, in order to conduct Wellington Management's business.

SAFE WORK ENVIRONMENT

As part of the Wellington Management organization's commitment to ensuring a safe work environment, violence or threats of violence in the workplace are prohibited. Violence includes physical altercations, fighting, the use of weapons, firearms, or explosives of any kind, or any other conduct, which could cause injury or other damage. Violence also includes deliberate destruction of the firm's property or the property of others. Threats include verbal or physical conduct which suggests the possibility of violence. Threats can be direct threats, as well as more subtle conduct such as intimidating remarks or gestures, and other menacing behavior. The possession of any weapons, firearms, explosives or other dangerous substances is strictly prohibited on any company premises, at any company function or gathering, or while on company business.

SMOKING

The firm demands that contingent workers refrain from smoking within the office premises.

SOCIAL MEDIA

Communication of all matters related to Wellington Management's business, clients, and personnel will not be transmitted through social networking sites including LinkedIn or other social media profiles. Avoid connecting with clients in your personal use of social media. Use care when connecting with colleagues and suppliers.

REFERENCES

Wellington Management prohibits posting, seeking or providing recommendations or referrals from current or former, temps, contingent workers (collectively contingent workers), Wellington Management employees, customers or service providers.

USE OF WELLINGTON MANAGEMENT NAME

Wellington Management prohibits any contingent worker's use of Wellington Management Company LLP as their employer –either stated or implied – on any contingent worker's resume or on LinkedIn or other social media profile. **Make sure to lay out your resume so that it's clear that you were a contingent worker and not employed by Wellington Management.**

TELEPHONE USAGE

Telephones are provided for business use only. In the event you must make a personal non-toll call, you should use a personal cellular phone in a private room. Non-business long distance calls are prohibited. Please consider those working around you when talking on the phone. Do not make personal calls in the rest rooms or other common areas.

MOBILE DEVICE POLICY

Wellington Management reserves the right to access and manage material on any mobile device with access to Wellington Management data, even if the device is personally owned. By obtaining access to Wellington Management data through your mobile device, you consent to Wellington Management's exercise of such management rights. Wellington Management reserves the right to remotely delete the content on a mobile device in the event of device theft, loss, or when the individual leaves Wellington Management.

POLICY ON PROPERTY AND CONFIDENTIAL INFORMATION

All Property of Wellington Management Company LLP (including its subsidiaries and affiliates, "Wellington Management") that Employees access or use during their employment at Wellington Management, is and shall remain the sole and exclusive property of Wellington Management.

The full policy can be found here (or attached hereto):

<http://wmcintranet.wellmanage.com/policies/BusinessPoliciesCommittees/Policy%20on%20Property%20and%20Confidential%20Information.pdf>

For copies of your signed Non-Disclosure Agreement, please reach out to your employer or Staffing(Non-FTE)

SYSTEMS ACCESS AND USAGE

- Use of any application or service accounts to gain production access, is strictly forbidden, except by authorized appropriate personnel.
 - Requests for read access to production databases requires an active change control or open incident and Wellington Management manager approval. Default production access will not be provided.
 - Stage and production SUDO access to any system or application account must be approved by a user's manager or their designee and forwarded to the Solutions Center. Default SUDO access will not be provided.
 - Making copies of security files or otherwise abusing the spirit of this memo is strictly prohibited.
-

INTERNET USAGE

Internet access is provided for the sole purpose of conducting company business. Wellington Management monitors, logs, and audits web sites accessed from its systems, files that are downloaded, time spent on the Internet, and other related information. Internet access can be revoked at any time. Any abuse of this access is grounds for termination. Additionally contingent workers are not to communicate or share information over the internet related to Wellington Management's business *unless* explicitly authorized to do so from Wellington Management.

EXTERNAL WEBMAIL USAGE

Access to external webmail services via Wellington Management systems and the Wellington Management network is prohibited. This includes services such as those provided by contingent worker agencies as well as commercially available solutions such as Gmail or Hotmail. Using such services from Wellington Management devices leads to the increased likelihood of vulnerabilities being introduced to the Wellington Management network and is also prohibited for regulatory reasons. Any access to external webmail services must be restricted to personal devices over cell networks.

EMAIL USAGE

The use of Wellington Management's systems, including email and Internet, is not private or confidential. For the avoidance of doubt, you should have no expectation of privacy with regard to your use of Wellington Management's systems. You should assume that any email that you send from your Wellington email address can and will be read by your colleagues, our regulators and third parties.

- Email is for Wellington Management business purposes only and should not be used for personal communications.
 - Personal email accounts may not be used to conduct firm business.
 - Proper conduct must be observed at all times when using email.
 - You must not join or subscribe to any internet email lists with your Wellington Management provided email address.
 - You must report all chain messages and junk messages as "SPAM" or "Phishing" using the Report Phishing Icon
 - You must use "WMC..INTERNAL" (all one word no periods) on all confidential documents or email.
 - Email will auto-delete after 60 days. Please make sure you review the **Quick Reference Guide** (included in your welcome packet).
-

INFORMATION SECURITY POLICY

You are required to follow the information security policy and standards. Please review the policy and standards outlining your responsibilities for handling confidential data, securing of Wellington Management managed devices and remote access standards at (or attached hereto):

[Information Security Policy](#)

INFORMATION SECURITY REQUIRED PRACTICES AND RESTRICTIONS

In addition to the policies outlined in this document and the Information Security Policies, Wellington provides detailed required security practices and restrictions for Contingent Workers to protect Wellington information and systems. All contingent workers must review and sign off on the [Required Information Security Practices and Restrictions](#) document and follow the practices and restrictions on a daily basis.

[Required Information Security Practices and Restrictions for Contingent Workers](#)

(or attached hereto)

~SIGNATURE PAGE TO FOLLOW~

Code of Ethics

Personal investing

Gifts and entertainment

Outside activities

Client confidentiality

*The reputation of a thousand years may
be determined by the conduct of one hour.*

– Ancient proverb

A message from our CEO



Brendan J. Swords
Chairman and Chief
Executive Officer

Our business is built on a foundation of trust — the trust of our clients, earned over many years. It is our most valuable asset, and if lost, it cannot easily be regained. There are examples across our industry of companies that have lost sight of this lesson, and they serve as strong reminders that our business requires a mindset of eternal vigilance.

Each and every one of us has a role to play in sustaining our clients' trust. We must test every decision we make, no matter how small, against our fiduciary obligations and our high ethical standards. If there is the slightest doubt about whether a decision is in the best interests of our clients, then bring it to someone's attention — your manager, the Legal and Compliance team, or any of my direct reports. But don't just let it go. This is what it means to be a fiduciary: complete dedication to conscientious stewardship of client assets.

To support this mandate, our Code of Ethics sets out standards for our personal conduct, including personal investing, acceptance of gifts and entertainment, outside activities, and client confidentiality. Please take the time to read the Code, familiarize yourself with the rules, and determine what you need to do to comply with them. Remember, too, that while our Code of Ethics is reviewed and updated regularly, no set of rules can address every possible circumstance. And so I ask you to remain vigilant, exercise good judgment, ask for help when you need it, consider not just the letter but the spirit of the laws that govern our industry, and do your part to safeguard our clients' trust.

Sincerely,

A handwritten signature in black ink that reads "Brendan J. Swords". The signature is fluid and cursive, with the first letters of the first and last names being capitalized and prominent.

Brendan J. Swords
Chairman and Chief Executive Officer

Before you get started

The Code of Ethics System is accessible through the intranet under Applications or direct access:

<https://fs.wellington.com/adfs/ls//ldpInitiatedSignIn.aspx?loginToRp=ptaconnect.com>

Contents

Standards of conduct	1
Who is subject to the Code of Ethics?	1
Personal investing	2
Which types of investments and related activities are prohibited?	2
Which investment accounts must be reported?	3
What are the reporting responsibilities for all personnel?	5
What are the preclearance responsibilities for all personnel?	6
What are the additional requirements for investment professionals?	7
Gifts and entertainment	8
Outside activities	9
Client confidentiality	9
How we enforce our Code of Ethics	10
Exceptions from the Code of Ethics	10
Closing	10

Standards of conduct

Our standards of conduct are straightforward and essential. Any transaction or activity that violates either of the standards of conduct below is prohibited, regardless of whether it meets the technical rules found elsewhere in the Code of Ethics.

1. **WE ACT AS FIDUCIARIES TO OUR CLIENTS.** Each of us must put our clients' interests above our own and must not take advantage of our management of clients' assets for our own benefit. Our firm's policies and procedures implement these principles with respect to our conduct of the firm's business. This Code of Ethics implements the same principles with respect to our personal conduct. The procedures set forth in the Code govern specific transactions, but each of us must be mindful at all times that our behavior, including our personal investing activity, must meet our fiduciary obligations to our clients.
2. **WE ACT WITH INTEGRITY AND IN ACCORDANCE WITH BOTH THE LETTER AND THE SPIRIT OF THE LAW.** Our business is highly regulated, and we are committed as a firm to compliance with those regulations. Each of us must also recognize our obligations as individuals to understand and obey the laws that apply to us in the conduct of our duties. They include laws and regulations that apply specifically to investment advisors, as well as more broadly applicable laws ranging from the prohibition against trading on material nonpublic information and other forms of market abuse to anticorruption statutes such as the US Foreign Corrupt Practices Act and the UK Bribery Act. The firm provides training on their requirements. Each of us must take advantage of these resources to ensure that our own conduct complies with the law.

Who is subject to the Code of Ethics?

Our Code of Ethics applies to all employees of Wellington Management and its affiliates around the world. Its restrictions on personal investing also apply to temporary personnel (including co-ops and interns) and consultants whose tenure with Wellington Management exceeds 90 days and who are deemed by the Chief Compliance Officer to have access to nonpublic investment research, client holdings, or trade information.

All Wellington Management personnel receive a copy of the Code of Ethics (and any amendments) and must certify, upon joining the firm and annually thereafter, that they have read and understood it and have complied with its requirements.

Adherence to the Code of Ethics is a basic condition of employment. Failure to adhere to our Code of Ethics may result in disciplinary action, including termination of employment.

If you have any doubt as to the appropriateness of any activity, believe that you have violated the Code, or become aware of a violation of the Code by another individual, you should consult the manager of the Code of Ethics Team, Chief Compliance Officer, General Counsel, or Chair of the Ethics Committee. You also have the right to report violations of law or regulation directly to relevant governmental agencies. You do not need the firm's prior authorization to make any such report or disclosures and are not required to notify the firm that you have done so.

General questions regarding our Code of Ethics may be directed to the Code of Ethics Team via email at **#Code of Ethics Team** or through the Code of Ethics hotline, **617-790-8330 (x68330)**.

Personal investing

As fiduciaries, each of us must avoid taking personal advantage of our knowledge of investment activity in client accounts. Although our Code of Ethics sets out a number of specific restrictions on personal investing designed to reflect this principle, no set of rules can anticipate every situation. Each of us must adhere to the spirit, and not just the letter, of our Code in meeting this fiduciary obligation to our clients.

WHICH TYPES OF INVESTMENTS AND RELATED ACTIVITIES ARE PROHIBITED?

Our Code of Ethics prohibits the following personal investments and investment-related activities:

- Purchasing or selling the following:
 - Initial public offerings (IPOs) of any securities
 - Securities of an issuer being bought or sold on behalf of clients until one trading day after such buying or selling is completed or canceled
 - Securities of an issuer that is the subject of a new, changed, or reissued but unchanged action recommendation from a global industry research or fixed income credit analyst until two business days following issuance or reissuance of the recommendation
 - Securities of an issuer that is mentioned at the Morning Meeting or the Early Morning Meeting until two business days following the meeting
 - Securities that are the subject of a firmwide restriction
 - Single-stock futures
 - Options with an expiration date that is within 60 calendar days of the transaction date
 - Securities of broker/dealers (or their affiliates) that the firm has approved for execution of client trades
 - Securities of any securities market or exchange on which the firm trades on behalf of clients
- Purchasing an equity security if your aggregate ownership of the equity security exceeds 0.05% of the total shares outstanding of the issuer
- Taking a profit from any trading activity within a 60 calendar day window
- Using a derivative instrument to circumvent a restriction in the Code of Ethics

Short-term trading

You are prohibited from profiting from the purchase and sale (or sale and purchase) of the same or equivalent securities within 60 calendar days. For example, if you buy shares of stock (or options on such shares) and then sell those shares within 60 days at a profit, an exception will be identified and any gain from the transactions must be surrendered. Gains are calculated based on a last in, first out (LIFO) method for purposes of this restriction. This short-term trading rule does not apply to securities exempt from the Code's preclearance requirements.

WHICH INVESTMENT ACCOUNTS MUST BE REPORTED?

You are required to report any investment account over which you exercise investment discretion or from which any of the following individuals enjoy economic benefits: (i) your spouse, domestic partner, or minor children, and (ii) any other dependents living in your household,

AND

that holds or is capable of holding any of the following *covered investments*:

- Shares of stocks, ADRs, or other equity securities (including any security convertible into equity securities)
- Bonds or notes (other than sovereign government bonds issued by Canada, France, Germany, Italy, Japan, the United Kingdom, or the United States, as well as bankers' acceptances, CDs, commercial paper, and high-quality, short-term debt instruments)
- Interest in a variable annuity product in which the underlying assets are held in a subaccount managed by Wellington Management
- Shares of exchange-traded funds (ETFs)
- Shares of closed-end funds
- Options on securities
- Securities futures
- Interest in private placement securities (other than Wellington Management sponsored products)
- Shares of funds managed by Wellington Management (other than money market funds)

Please see **Appendix A** for a detailed summary of reporting requirements by security type.

For purposes of the Code of Ethics, these investment accounts are referred to as *reportable accounts*. Examples of common account types include brokerage accounts, retirement accounts, employee stock compensation plans, and transfer agent accounts. Reportable accounts also include those from which you or an immediate family member may benefit indirectly, such as a family trust or family partnership, and accounts in which you have a joint ownership interest, such as a joint brokerage account.

Please contact the Code of Ethics Team for guidance if you hold any securities in physical certificate form.

Still not sure? Contact us

If you are not sure if a particular account is required to be reported, contact the Code of Ethics Team by email at **#Code of Ethics Team** or through the Code of Ethics hotline, 617-790-8330 (x68330).

► WEB RESOURCE

Wellington-Managed fund list

An up-to-date list of funds managed by Wellington Management is available through the Code of Ethics System under Documents. Please note that any transactions in Wellington-Managed funds must comply with the funds' rules on short-term trading of fund shares.

Accounts not requiring reporting

You do not need to report the following accounts via the Code of Ethics System since the administrator will provide the Code of Ethics Team with access to relevant holdings and transaction information:

- Accounts maintained within the Wellington Retirement and Pension Plan or similar firm-sponsored retirement or benefit plans identified by the Ethics Committee
- Accounts maintained directly with Wellington Trust Company or other Wellington Management Sponsored Products

Although these accounts do not need to be reported, your investment activities in these accounts must comply with the standards of conduct embodied in our Code of Ethics.

Managed account exemptions

An account from which you or immediate family members could benefit financially, but over which neither you nor they have any investment discretion or influence (a *managed account*), may be exempted from the Code of Ethics' personal investing requirements upon written request and approval. An example of a managed account would be a professionally advised account about which you will not be consulted or have any input on specific transactions placed by the investment manager prior to their execution. To request a managed account exemption, you must complete a Managed Account Letter (available online via the Code of Ethics System) and return it to the Code of Ethics Team.

► WEB RESOURCE

Managed Account Letter

To request a managed account exemption, complete the Managed Account Letter available through the Code of Ethics System under Documents.

WHAT ARE THE REPORTING RESPONSIBILITIES FOR ALL PERSONNEL?

Initial and annual holdings reports

You must disclose all reportable accounts and all covered investments you hold within 10 calendar days after you begin employment at or association with Wellington Management. You will be required to review and update your holdings and securities account information annually thereafter.

For initial holdings reports, holdings information must be current as of a date no more than 45 days prior to the date you became covered by the Code of Ethics.

Please note that you cannot make personal trades until you have filed an initial holdings report via the Code of Ethics System on the Intranet.

Non-volitional transactions include:

Investments made through automatic dividend reinvestment or rebalancing plans and stock purchase plan acquisitions

Transactions that result from corporate actions applicable to all similar security holders (such as splits, tender offers, mergers, and stock dividends)

For subsequent annual reports, holdings information must be current as of a date no more than 45 days prior to the date the report is submitted. *Please note that your annual holdings report must account for both volitional and non-volitional transactions.*

At the time you file your initial and annual reports, you will be asked to confirm that you have read and understood the Code of Ethics and any amendments.

Duplicate statements and trade confirmations

For each of your reportable accounts, you are required to provide duplicate statements and duplicate trade confirmations to Wellington Management. To arrange for the delivery of duplicate statements and trade confirmations, please contact the Code of Ethics Team for the appropriate form. Return the completed form to the Code of Ethics Team, which will submit it to the brokerage firm on your behalf. If the brokerage firm or other firm from which you currently receive statements is not able to send statements and confirmations directly to Wellington Management, you will be required to submit copies promptly after you receive them, unless you receive an exemption from this requirement under the procedures outlined on page 7.

Quarterly transactions reports

You must submit a quarterly transaction report no later than 30 calendar days after quarter-end via the Code of Ethics System on the Intranet, even if you did not make any personal trades during that quarter. In the reports, you must either confirm that you did not make any personal trades (except for those resulting from non-volitional events) or provide information regarding all volitional transactions in covered investments.

► WEB RESOURCE

How to file reports on the Code of Ethics System

Required reports must be filed electronically via the Code of Ethics System. Please see the Code of Ethics System's homepage for more details.

WHAT ARE THE PRECLEARANCE RESPONSIBILITIES FOR ALL PERSONNEL?

Preclearance of publicly traded securities

You must receive clearance before buying or selling stocks, bonds, options, and most other publicly traded securities in any reportable account. A full list of the categories of publicly traded securities requiring preclearance, and of certain exceptions to this requirement, is included in **Appendix A**. Transactions in accounts that are not reportable accounts do not require preclearance or reporting.

Preclearance requests must be submitted online via the Code of Ethics System, which is accessible through the Intranet. If clearance is granted, the approval will be effective for a period of 24 hours. If you preclear a transaction and then place a limit order with your broker, that limit order must either be executed or expire at the end of the 24-hour period. *If you want to execute the order after the 24-hour period expires, you must resubmit your preclearance request.*

If you have questions regarding the preclearance requirements, please refer to the FAQs available on the Code of Ethics System or contact the Code of Ethics Team.

Please note that preclearance approval does not alter your responsibility to ensure that each personal securities transaction complies with the general standards of conduct, the reporting requirements, the restrictions on short-term trading, or the special rules for investment professionals set out in our Code of Ethics.

► WEB RESOURCE

How to file a preclearance request

Preclearance must be obtained using the Code of Ethics System. Once the necessary information is submitted, your preclearance request will be approved or denied within seconds.

Caution on short sales, margin transactions, and options

You may engage in short sales and margin transactions and may purchase or sell options provided you receive preclearance and meet all other applicable requirements under our Code of Ethics (including the additional rules for investment professionals described on page 8). *Please note, however, that these types of transactions can have unintended consequences.* For example, any sale by your broker to cover a margin call or to buy in a short position will be in violation of the Code unless precleared. Likewise, any volitional sale of securities acquired at the expiration of a long call option will be in violation of the Code unless precleared. You are responsible for ensuring any subsequent volitional actions relating to these types of transactions meet the requirements of the Code.

Preclearance of private placement securities

You cannot invest in securities offered to potential investors in a private placement without first obtaining prior approval. Approval may be granted after a review of the facts and circumstances, including whether:

- an investment in the securities is likely to result in future conflicts with client accounts (e.g., upon a future public offering), and
- you are being offered the opportunity due to your employment at or association with Wellington Management.

If you have questions regarding whether an investment would be deemed a *private placement security* under the Code, please refer to the FAQs about private placements available on the Code of Ethics System, or contact the Code of Ethics Team.

To request approval, you must submit a Private Placement Approval Form (available online via the Code of Ethics System) to the Code of Ethics Team. Investments in our own privately offered investment vehicles (our *Sponsored Products*), including collective investment funds and common trust funds maintained by Wellington Trust Company, na, our hedge funds, and our non-US domiciled funds (Wellington Management Portfolios), have been approved under the Code and therefore do not require the submission of a Private Placement Approval Form.

► WEB RESOURCE

Private Placement Approval Form

To request approval for a private placement, complete the Private Placement Approval Form available through the Code of Ethics System under Documents.

WHAT ARE THE ADDITIONAL REQUIREMENTS FOR INVESTMENT PROFESSIONALS?

If you are a portfolio manager, research analyst, or other investment professional who has portfolio management responsibilities for a client account (e.g., designated portfolio manager, backup portfolio manager, investment team member), or who otherwise has direct authority to make decisions to buy or sell securities in a client account (referred to here as an investment professional), you are required to adhere to additional rules and restrictions on your personal securities transactions. However, as no set of rules can anticipate every situation, you must remember to place our clients' interests first whenever you transact in securities that are also held in client accounts you manage.

The following provisions of the code are intended to allow investment professionals to make long-term investments in securities. However, you may not be able to sell personal investments for extended periods of time and therefore should consider the liquidity, tax planning, market, and similar risks associated with making personal investments in securities of an issuer that are or may be held in client accounts.

- **INVESTMENT PROFESSIONAL BLACKOUT PERIODS** — You cannot buy or sell a security for a period of **14 calendar days before or after** any transaction in the same issuer by a client account for which you serve as an investment professional. In addition, You may not sell personal holdings in a security of the same issuer that is held by a client account for which you serve as an investment professional until the **later of** the following periods: (i) **one calendar year** from the date of your last purchase and (ii) **90 calendar days** after all of your client accounts liquidate all holdings of the same issuer.

If you anticipate receiving a cash flow or redemption request in a client portfolio that will result in the purchase or sale of securities that you also hold in your personal account, you should take care to avoid transactions in those securities in your personal account in the days leading up to the client transactions. However, unanticipated cash flows and redemptions in client accounts and unexpected market events do occur from time to time, and a personal trade made in the prior 14 days should never prevent you from buying or selling a security in a client account if the trade would be in the client's best interest. If you find yourself in that situation and need to buy or sell a security in a client account within the 14 calendar days following your personal transaction in a security of the same issuer, you should attempt to notify the Code of Ethics Team (by email at **#Code of Ethics Team** or through the **Code of Ethics hotline, 617-790-8330 [x68330]**) or your local Compliance Officer in advance of placing the trade. If you are unable to reach any of those individuals and the trade is time sensitive, you should proceed with the client trade and notify the Code of Ethics Team promptly after submitting it.

- **SHORT SALES BY AN INVESTMENT PROFESSIONAL** — An investment professional may not personally take a short position in a security of an issuer in which he or she holds a long position in a client account.

Gifts and entertainment

Our guiding principle of “client, firm, self” also governs the receipt of gifts and entertainment from clients, consultants, brokers/dealers, research providers, vendors, companies in which we may invest, and others with whom the firm does business. As fiduciaries to our clients, we must always place our clients’ interests first and cannot allow gifts or entertainment opportunities to influence the actions we take on behalf of our clients. In keeping with this standard, you must follow several specific requirements:

ACCEPTING GIFTS — You may only accept gifts of nominal value, which include logoed items, flower arrangements, gift baskets, and food, as well as other gifts with an approximate value of less than US\$100 or the local equivalent per year from a single source. You may not accept a gift of cash, including a cash equivalent such as a gift card, regardless of the amount. If you receive a gift that violates the Code, you must return the gift or consult with the Chief Compliance Officer to determine appropriate action under the circumstances.

ACCEPTING BUSINESS MEALS — Business meals are permitted provided that neither the cost nor the frequency is excessive and there is a legitimate business purpose. If the host is a broker/dealer or research provider, the host must be reimbursed for the full amount of your proportionate share of the total cost of the meal if the approximate value of the meal is more than US\$100 or the local equivalent.

ACCEPTING ENTERTAINMENT OPPORTUNITIES — The firm recognizes that participation in entertainment opportunities with representatives from organizations with which the firm does business, such as consultants, broker/dealers, research providers, vendors, and companies in which we may invest, can help to further legitimate business interests. However, participation in such entertainment opportunities should be infrequent and is subject to the following conditions:

1. A representative of the hosting organization must be present;
2. The primary purpose of the event must be to discuss business or to build a business relationship;
3. You must receive prior approval from your business manager;
4. If the host is a broker/dealer or research provider, the host must be reimbursed for the full amount of the entertainment opportunity; and
5. For all other entertainment opportunities, the host must be reimbursed for the full face value of any entertainment ticket(s) if:
 - the entertainment opportunity requires a ticket with a face value of more than US\$200 or the local equivalent, or is a high-profile event (e.g., a major sporting event),
 - you wish to accept more than one ticket, or
 - the host has invited numerous Wellington Management representatives.

Business managers must clear their own participation under the circumstances described above with the Chief Compliance Officer or Chair of the Ethics Committee.

Please note that even if you pay for the full face value of a ticket, you may attend the event *only if the host is present*.

LODGING AND AIR TRAVEL — You may not accept a gift of lodging or air travel in connection with any entertainment opportunity. If you participate in an entertainment opportunity for which lodging or air travel is paid for by the host, you must reimburse the host for the equivalent cost, as determined by Wellington Management’s travel manager.

SOLICITING GIFTS, ENTERTAINMENT OPPORTUNITIES, OR CONTRIBUTIONS — In your capacity as an employee of the firm, you may not solicit gifts, entertainment opportunities, or charitable or political contributions for yourself, or on behalf of clients, prospects, or others, from brokers, vendors, clients, or consultants with whom the firm conducts business or from companies in which the firm may invest.

SOURCING ENTERTAINMENT OPPORTUNITIES — You may not request tickets to entertainment events from the firm's Trading department or any other Wellington Management department, or employee, nor from any broker, vendor, company in which we may invest, or other organization with which the firm conducts business.

Outside activities

While the firm recognizes that you may engage in business or charitable activities in your personal time, you must take steps to avoid conflicts of interest between your private interests and our clients' interests. As a result, all significant outside business or charitable activities (e.g., additional employment, consulting work, directorships or officerships) must be approved by your business manager and by the Chief Compliance Officer, General Counsel, or Chair of the Ethics Committee prior to the acceptance of such a position (or if you are new, upon joining the firm). Approval will be granted only if it is determined that the activity does not present a significant conflict of interest. Directorships in public companies (or companies reasonably expected to become public companies) will generally not be authorized, while service with charitable organizations generally will be permitted.

► WEB RESOURCE

Outside Business Activities Approval Form

To request approval to participate in activities outside of Wellington Management, complete the Outside Business Activities Approval Form available through the Code of Ethics System under Documents.

Client confidentiality

Any nonpublic information concerning our clients that you acquire in connection with your employment at the firm is confidential. This includes information regarding actual or contemplated investment decisions, portfolio composition, research recommendations, and client interests. You should not discuss client business, including the existence of a client relationship, with outsiders unless it is a necessary part of your job responsibilities.

How we enforce our Code of Ethics

Legal and Compliance is responsible for monitoring compliance with the Code of Ethics. Members of Legal and Compliance will periodically request certifications and review holdings and transaction reports for potential violations. They may also request additional information or reports.

It is our collective responsibility to uphold the Code of Ethics. In addition to the formal reporting requirements described in this Code of Ethics, you have a responsibility to report any violations of the Code. If you have any doubt as to the appropriateness of any activity, believe that you have violated the Code, or become aware of a violation of the Code by another individual, you should consult the manager of the Code of Ethics Team, Chief Compliance Officer, General Counsel, or Chair of the Ethics Committee.

Potential violations of the Code of Ethics will be investigated and considered by representatives of Legal and Compliance and/or the Ethics Committee. All violations of the Code of Ethics will be reported to the Chief Compliance Officer. Violations are taken seriously and may result in sanctions or other consequences, including:

- a warning
- referral to your business manager and/or senior management
- reversal of a trade or the return of a gift
- disgorgement of profits or of the value of a gift
- a limitation or restriction on personal investing
- termination of employment
- referral to civil or criminal authorities

If you become aware of any potential conflicts of interest that you believe are not addressed by our Code of Ethics or other policies, please contact the Chief Compliance Officer, the General Counsel, or the manager of the Code of Ethics Team.

Exceptions from the Code of Ethics

The Chief Compliance Officer may grant an exception from the Code, including preclearance, other trading restrictions, and certain reporting requirements on a case-by-case basis if it is determined that the proposed conduct involves no opportunity for abuse and does not conflict with client interests. Exceptions are expected to be rare. If you wish to seek an exception, you must submit a written request to the Code of Ethics Team describing the nature of the exception and the reason(s) it is being sought.

Closing

As a firm, we seek excellence in the people we employ, the products and services we offer, the way we meet our ethical and fiduciary responsibilities, and the working environment we create for ourselves. Our Code of Ethics embodies that commitment. Accordingly, each of us must take care that our actions fully meet the high standards of conduct and professional behavior we have adopted. Most importantly, we must all remember “client, firm, self” is our most fundamental guiding principle.

APPENDIX A – PART 1

No Preclearance or Reporting Required:	Preclearance and Reporting of Securities Transactions Required:
Open-end investment funds not managed by Wellington Management ¹	Bonds and notes (other than direct obligations of the US government or the governments of Canada, France, Germany, Italy, Japan, or the United Kingdom, as well as bankers' acceptances, CDs, commercial paper, and high-quality, short-term debt instruments)
Interests in a variable annuity product in which the underlying assets are held in a fund not managed by Wellington Management	Stock (common and preferred) or other equity securities, including any security convertible into equity securities
Direct obligations of the US government (including obligations issued by GNMA and PEFCO) or the governments of Canada, France, Germany, Italy, Japan, or the United Kingdom	Closed-end funds
Cash	ETFs not listed in Appendix A – Part 2
Money market instruments or other short-term debt instruments rated P-1 or P-2, A-1 or A-2, or their equivalents ²	American Depositary Receipts
Bankers' acceptances, CDs, commercial paper	Options on securities (but not their non-volitional exercise or expiration)
Wellington Trust Company Pools	Warrants
Wellington Sponsored Hedge Funds	Rights
Securities futures and options on direct obligations of the US government or the governments of Canada, France, Germany, Italy, Japan, or the United Kingdom, and associated derivatives	Unit investment trusts
Options, forwards, and futures on commodities and foreign exchange, and associated derivatives	Prohibited Investments and Activities:
Transactions in approved managed accounts	Initial public offerings (IPOs) of any securities
Reporting of Securities Transactions Required (no need to preclear and not subject to the 60-day holding period):	Single-stock futures
Open-end investment funds managed by Wellington Management ¹ (other than money market funds)	Options expiring within 60 days of purchase
Interests in a variable annuity or insurance product in which the underlying assets are held in a fund managed by Wellington Management	Securities being bought or sold on behalf of clients until one trading day after such buying or selling is completed or canceled
Futures and options on securities indices	Securities of an issuer that is the subject of a new, changed, or reissued but unchanged action recommendation from a global industry research or fixed income credit analyst until two business days following issuance or reissuance of the recommendation
ETFs listed in Appendix A – Part 2 and derivatives on these securities	Securities of an issuer that is mentioned at the Morning Meeting or the Early Morning Meeting until two business days following the meeting
Gifts of securities to you or a reportable account	Securities on the firmwide restricted list
Gifts of securities from you or a reportable account	Profiting from any short-term (i.e., within 60 days) trading activity
Non-volitional transactions (splits, tender offers, mergers, stock dividends, dividend reinvestments, etc.)	Securities of broker/dealers or their affiliates with which the firm conducts business
	Securities of any securities market or exchange on which the firm trades
	Using a derivative instrument to circumvent the requirements of the Code of Ethics
	Purchasing an equity security if your aggregate ownership of the equity security exceeds 0.05% of the total shares outstanding of the issuer

This appendix is current as of 1 July 2016, and may be amended at the discretion of the Ethics Committee.

¹A list of funds advised or subadvised by Wellington Management ("Wellington-Managed Funds") is available online via the Code of Ethics System. However, you remain responsible for confirming whether any particular investment represents a Wellington-Managed Fund.

²If the instrument is unrated, it must be of equivalent duration and comparable quality.

APPENDIX A – PART 2

ETFs approved for personal trading without preclearance (but requiring reporting)

All regional/country exchange share listings of ETFs listed are also approved

Ticker	Name
United States: Equity	
AAXJ	ISHARES MSCI ALL COUNTRY ASIA
ACWI	ISHARES MSCI ACWI INDEX FUND
BRF	MARKET VECTORS BRAZIL SMALL-CA
DIA	SPDR DJIA TRUST ETF
DVY	ISHARES DOW JONES SELECT DIVID
ECH	ISHARES MSCI CHILE INVESTABLE
EEB	GUGGENHEIM BRIC ETF
EEM	ISHARES MSCI EMERGING MARKETS
EFA	ISHARES MSCI EAFE INDEX FUND
EFV	ISHARES MSCI EAFE VALUE INDEX
EPI	WISDOMTREE INDIA EARNINGS FUND
EPP	ISHARES MSCI PAC EX-JAPAN FUND
EWA	ISHARES MSCI AUSTRALIA INDEX FUND
EWC	ISHARES MSCI CANADA INDEX FUND
EWG	ISHARES MSCI GERMANY INDEX FUND
EWI	ISHARES MSCI HONG KONG IDX FUND
EWJ	ISHARES MSCI JAPAN IDX FUND
EWM	ISHARES MSCI MALAYSIA IDX FUND
EWS	ISHARES MSCI SINGAPORE INDEX FUND
EWT	ISHARES MSCI TAIWAN INDEX FUND
EWU	ISHARES MSCI UK INDEX FUND
EWY	ISHARES MSCI SOUTH KOREA INDEX
EZU	ISHARES MSCI EMU INDEX FUND
FXI	ISHARES FTSE CHINA 25 INDEX
GDX	MARKET VECTORS GOLD MINERS
GDXJ	MARKET VECTORS JUNIOR GOLD MIN
IBB	ISHARES BIOTECH INDEX FUND
ICF	ISHARES COHEN & STEERS REALTY
IEV	ISHARES S&P EUROPE 350 INX FUND
IGE	ISHARES S&P GSSI NAT RES INDEX
IJH	ISHARES S&P MIDCAP 400 IDX FUND
IJJ	ISHARES S&P MIDCAP 400/VALUE
IJK	ISHARES SP MCAP 400/BARRA GTH
IJR	ISHARES SP SMALLCAP 600 IDX FUND
IJS	ISHARES S&P SMALLCAP 600/BARRA
IJT	ISHARES SP SMCAP 600/BARRA GTH
ILF	ISHARES S&P LATIN AMER 40 INDEX
INP	IPATH MSCI INDIA INDEX ETN
IOO	ISHARES S&P GLOBAL 100 INDEX FUND
IVE	ISHARES SP 500/BARRA VALUE
IVV	ISHARES S&P 500 INDEX FUND
IVW	ISHARES S&P 500/BARRA GRTH INDEX
IWB	ISHARES RUSSELL 1000 INDEX
IWD	ISHARES RUSSELL 1000 VALUE INDEX
IWF	ISHARES RUSSELL 1000 GROWTH
IWM	ISHARES RUSSELL 2000 INDEX
IWN	ISHARES RUSSELL 2000 VALUE
IWO	ISHARES RUSSELL 2000 GROWTH
IWP	ISHARES RUSSELL MIDCAP GROWTH
IWR	ISHARES RUSSELL MIDCAP INDEX FUND
IWS	ISHARES RUSSELL MIDCAP VALUE I
IWV	ISHARES RUSSELL 3000 INDEX
IXC	ISHARES S&P GLOBAL ENERGY SECT
IYR	ISHARES DOW JONES US RE INDEX
IYW	ISHARES DJ US TECH SECTOR INDEX
MDY	SPDR S&P MIDCAP 400 ETF TRUST
MOO	MARKET VECTORS-AGRI
OEF	ISHARES S&P 100 INDEX FUND
PBW	POWERSHARES WILDERHILL CLEAN E
PFF	ISHARES S&P US PREFERRED STOCK
PGX	POWERSHARES PREFERRED PORTFOLI
PHO	POWERSHARES GLOBAL WATER PORTF
QID	PROSHARES ULTRASHORT QQQ
QLD	PROSHARES ULTRA QQQ
QQQ	POWERSHARES QQQTRUST
RSP	RYDEX S&P EQUAL WEIGHT
RSX	MARKET VECTORS RUSSIA ETF
RWM	PROSHARES SHORT RUSS
RWR	SPDR DOW JONES REIT ETF

Ticker	Name
RWX	SPDR DJ INTL REAL ESTATE
SCZ	ISHARES MSCI EAFE SMALL CAP INDEX
SDS	PROSHARES ULTRASHORT S&P500
SDY	SPDR DIVIDEND ETF
SH	PROSHARES SHORT S&P500
SKF	PROSHARES ULTRASHORT FINANCIAL
SPY	SPDR S&P 500 ETF TRUST
SRS	PROSHARES ULTRASHORT REAL ESTATE
SSO	PROSHARES ULTRA S&P500
TWM	PROSHARES ULTRASHORT RUSS2000
UWM	PROSHARES ULTRA RUSSELL
UYG	PROSHARES ULTRA FINANCIALS
VB	VANGUARD SMALL-CAP VIPERS
VBK	VANGUARD SMALL-CAP GROWTH VIPE
VBR	VANGUARD SMALL-CAP VALUE VIPER
VEA	VANGUARD MSCI EAFE ETF
VEU	VANGUARD FTSE ALL-WORLD EX-US
VGK	VANGUARD MSCI EURO ETF
VIG	VANGUARD DIVIDEND APPRECIATION
VNQ	VANGUARD REIT VIPERS
VO	VANGUARD MID-CAP VIPERS
VPL	VANGUARD S&P PACIFIC ETF
VTI	VANGUARD TOTAL STOCK MARKET
VTV	VANGUARD VALUE VIPERS
VUG	VANGUARD GROWTH VIPERS
VV	VANGUARD LARGE-CAP VIPERS
VWO	VANGUARD MSCI EM MAR
VXX	IPATH S&P 500 VIX
XLB	MATERIALS SEL SECTOR SPDR FUND
XLE	ENERGY SELECT SECTOR SPDR FUND
XLF	FINANCIAL SEL SECTOR SPDR FUND
XLI	INDUSTRIAL SELECT SECTOR SPDR
XLK	TECHNOLOGY SELECT SECTOR SPDR
XLP	CONSUMER STAPLES SELECT SPDR
XLU	UTILITIES SELECT SECTOR SPDR
XLV	HEALTH CARE SELECT SECTOR SPDR
XLY	CONSUMER DISCRETIONARY SPDR
XME	SPDR S&P METALS & MINING ETF
XOP	SPDR S&P OIL & GAS EXPL AND PROD
United States: Fixed Income	
AGG	ISHARES BARCLAYS AGGREGATE
BIV	VANGUARD INTERMEDIATE-TERM BON
BND	VANGUARD TOTAL BOND MARKET
BOND	PIMCO TOTAL RETURN BOND ETF
BSV	VANGUARD SHORT-TERM BOND ETF
BWX	SPDR BARCLAYS INT TREA BND ETF
BZF	WISDOMTREE DREYFUS BRAZILIAN REAL FUND
CYB	WISDOMTREE DREYFUS CHINESE YUA
ELD	WISDOMTREE EMERGING MARKETS LO
EMB	JPM EMERGING MARKETS BOND ETF
HYG	ISHARES IBOX \$ HIGH YIELD COR
IEF	ISHARES BARCLAYS 7-10 YEAR
IEI	ISHARES BARCLAYS 3-7 YEAR TREAS
JNK	SPDR BARCLAYS HIGH YIELD BOND
LQD	ISHARES IBOX INVESTMENT GRADE
MBB	ISHARES MBS BOND FUND
MUB	ISHARES S&P NATIONAL MUNICIPAL
PCY	POWERSHARES EM MAR SOV DE PT
PST	PROSHARES ULTRASHORT LEH 7
SHY	ISHARES BARCLAYS 1-3 YEAR TREA
TBF	PROSHARES SHORT 20+ TREASURY
TBT	PROSHARES ULTRASHORT LEHMAN
TIP	ISHARES BARCLAYS TIPS BOND FUND
TLT	ISHARES BARCLAYS 20+ YEAR TREAS
VCSH	VANGUARD SHORT-TERM CORPORATE
United States: Commodity Trusts and ETNs	
AMJ	JPMORGAN ALERIAN MLP INDEX ETN
CORN	CORN ETF
COW	IPATH DJ-UBS LIVESTOCK SUBINDX
DBA	POWERSHARES DB AGRICULTURE FUND
DBB	POWERSHARES DB BASE METALS FUND

Ticker	Name
DBC	DB COMMODITY INDEX TRACKING FUND
DBE	POWERSHARES DB ENERGY FUND
DBO	POWERSHARES DB OIL FUND
DBP	POWERSHARES DB PRECIOUS METALS
DGZ	POWERSHARES DB GOLD SHORT ETN
DJP	IPATH DJ-UBS COMMODITY
DNO	UNITED STATES SHORT OIL FUND L
GAZ	IPATH DJ-UBS NAT GAS SUBINDEX
GLD	SPDR GOLD SHARES
GLL	PROSHARES ULTRASHORT GOLD
GSG	ISHARES S&P GSCI COMMODITY INDEX
JJA	IPATH DJ-UBS AGRICULTURE SUBINDEX
JJC	IPATH DJ-UBS COPPER SUBINDEX
JJE	IPATH DJ-UBS ENERGY SUBINDEX
JJG	IPATH DJ-UBS GRAINS SUBINDEX
JJM	IPATH DJ-UBS INDUSTRIAL METALS
JJN	IPATH DJ-UBS NICKEL SUBINDEX
JJS	IPATH DJ-UBS SOFTS SUBINDEX
JJU	IPATH DJ-UBS ALUMINUM SUBINDEX
SGG	IPATH DJ-UBS SUGAR SUBINDEX TR
SLV	ISHARES SILVER TRUST
UCO	PROSHARES ULTRA DJ-UBS CRUDE
UGA	UNITED STATES GASOLINE FUND LP
UGL	PROSHARES ULTRA GOLD
UHN	UNITED STATES HEATING OIL LP
UNG	UNITED STATES NATL GAS FUND LP
USO	UNITED STATES OIL FUND LP
ZSL	PROSHARES ULTRASHORT SILVER
United States: Currency Trusts	
DBV	POWERSHARES DB G10 CURRENCY HA
EUO	PROSHARES ULTRASHORT EURO
FXA	CURRENCYSHARES AUD TRUST
FXB	CURRENCYSHARES GBP STERL TRUST
FXC	CURRENCYSHARES CAD
FXE	CURRENCYSHARES EURO TRUST
FXF	CURRENCYSHARES SWISS FRANC
FXM	CURRENCYSHARES MEXICAN PESO
FXS	CURRENCYSHARES SWEDISH KRONA
FXU	CURRENCYSHARES JPY TRUST
UDN	POWERSHARES DB US DOLLAR IND
UUP	POWERSHARES DB US DOL IND BU
YCS	PROSHARES ULTRASHORT YEN
Australia: Equity	
STW.AX	SPDR S&P/ASX 200 FUND
England: Equity	
EUN LN	ISHARES STOXX EUROPE 50
IEEM LN	ISHARES MSCI EMERGING MARKETS
FXC LN	ISHARES FTSE CHINA25
IJPN LN	ISHARES MSCI JAPAN FUND
ISF LN	ISHARES PLC- ISHARES FTSE 100
IUSA LN	ISHARES S&P 500 INDEX FUND
IWRD LN	ISHARES MSCI WORLD
England: Fixed Income	
IEBC LN	ISHARES BARCLAYS CAPITAL EURO
Hong Kong: Equity	
2800 HK	TRACKER FD OF HONG KONG
2823 HK	ISHARES FTSE/ XINHUA A50 CHINA
2827 HK	BOCI-PRUDENTIAL – W.I.S.E. - C
2828 HK	HANG SENG INVESTMENT INDEX FUND
2833 HK	HANG SENG INVESTMENT INDEX FUND
Hong Kong: Fixed Income	
2821 HK	ABF PAN ASIA BOND INDEX FUND
Japan: Equity	
1305 JP	DAIWA ETF – TOPIX
1306 JP	NOMURA ETF – TOPIX
1308 JP	NIKKEI ETF – TOPIX
1320 JP	DAIWA ETF – NIKKEI 225
1321 JP	NOMURA ETF – NIKKEI 225
1330 JP	NIKKEI ETF – 225

This appendix is current as of 23 June 2014, and may be amended at the discretion of the Ethics Committee.

Memorandum

Wellington Management Company LLP

To: All Employees

From: Andrés E. Saldaña

Re: Policy on Property and Confidential Information

Date: 14 April 2016

Policy

All Property of Wellington Management Company LLP (including its affiliates, "Wellington Management") that Employees access or use during their employment at Wellington Management, is and shall remain the sole and exclusive property of Wellington Management.

Employees shall neither have nor acquire any rights to any Intellectual Property or other Property of Wellington Management during their employment with Wellington Management or thereafter.

Employees may not use or disclose any Confidential Information of Wellington Management, except as required for the proper performance of their duties at Wellington Management. Employees should take all reasonable steps to preserve the confidential and secret nature of Confidential Information.

Except as required for the proper performance of their duties at Wellington Management, Employees may not copy or transmit any Confidential Information or remove from Wellington Management's premises any media containing Confidential Information.

Notwithstanding the foregoing, Employees may report violations of law or regulation to any of Wellington Management's regulators. Employees do not need Wellington Management's prior authorization to make any such report or disclosures. Further, Employees are not required to notify Wellington Management after they make any such report or disclosures.

Definitions

Employees include all full time and temporary employees and consultants.

Property of Wellington Management includes property of any kind, for example documents, files, archives, computer software and hardware, facilities and equipment. Property also includes Intellectual Property and Confidential Information of Wellington Management.

Intellectual Property means any trade secrets, service marks, works of authorship and inventions, for example:

- Quant models and in-house databases
- PMW, FI-PMT and WIRE
- The trade allocation algorithm
- The Wellington Management brand
- Portfolio holdings and transactions executed for clients

-
- Confidential Information about the business of Wellington Management

Intellectual Property also includes any discoveries and processes developed or reduced to practice by Employees or Partners of Wellington Management, that relate in any way to our business or services, or that result from any work performed for Wellington Management.

Confidential Information means any information of Wellington Management that is not generally known. *Confidential Information* includes any information about our clients or vendors, for example:

- Portfolio holdings and transactions executed for clients
- Information about Wellington Management's business relationships, including the identity of business partners as well as their personnel, business plans and financial information

Confidential Information also includes any information about the business of Wellington Management, for example:

- Our investment mandates, products and services, including investment guidelines and fees
- Information systems, methods and software
- Business manuals, policies and procedures
- Business, marketing or strategic plans
- Financial results, statements or projections
- Personnel records

Termination of
Employment

When Employees leave the firm, they should return all Property of Wellington Management. For that purpose, Wellington Management may search the departing Employee's desk, files and work area for any Property in the employee's possession or control.

Departing Employees should return all notes, documents, records and media containing Intellectual Property or Confidential Information of the firm. Wellington Management will assist the Employee with this process as needed.

Memorandum

TO: All Personnel
FROM: David Eikenberry and Scott Lopez
RE: Error Resolution Council – Annual Update
DATE: 29 January 2015

BACKGROUND

The Error Resolution Council (ERC) is responsible for reviewing, overseeing and ensuring the resolution of errors that arise in the management of client portfolios. The members of the ERC come from many disciplines across the firm and meet regularly to discuss policy issues relating to errors.

Current members of the ERC are: David Eikenberry (Co-Chair), Scott Lopez (Co-Chair), Katie McKeown (Vice Chair), Cindy Clarke, Sandhya Douglas, Beth Evitts, Craig Gainey, Ray Helfer, Ian Link, Nancy Morris, Stephen Mortimer, Charlie Mulhern, Erin Murphy, Steve Muson, Susan Pozer, Tim Smith, Ed Steinborn, Justin Stephan, Graham Stone, and Matt Strzepka. Jill Kacich serves as Secretary.

ERRORS

Our experience suggests that most errors can be avoided by following procedures, reducing haste and questioning incomplete or unclear information or instructions. Errors are unpredictable in nature and may occur in all areas of the firm. Importantly, asking direct questions when something doesn't seem right can often be critical in identifying and/or avoiding potential errors.

The resolution of errors requires a prompt and well-reasoned response, which often incorporates considerations that may not be immediately evident to those closest to the incident. The ERC process increases the likelihood that all relevant resources are made available to assist in the resolution process and that we ultimately come to an appropriate solution. Our clients value our approach to the resolution of errors and look to the ERC process as assurance that we are fulfilling our fiduciary duties.

REQUIRED ACTION

Any employee who identifies an error or potential error affecting a client's portfolio, regardless of the potential financial impact, should immediately inform his or her Line Manager as well as the ERC Support Team or a member of the ERC directly before any action is taken to correct the error.

CONTACTING THE ERC

ERC Contact information is included on the firm's intranet site [here](#). The ERC support team members are: Jason Kirby (x63102), Marines Piney (x46125), David Rouse (x68223), Jill Kacich (x67236) and Lauren Greeley (x67627). The ERC hotline number is x68002. In addition, for non-urgent matters, incidents can be reported to #ERC Support.

Information Security
Mobile Devices
Standard Policy

Revision: 1.4
September 17, 2008

Standards Statement	Mobile devices are used to gain access to WMC systems, networks, and proprietary information and can be easily moved within or outside WMC facilities. This document defines standards for mobile devices and is in direct support of the WMC Information Security Policy.
Scope	This document applies to all personnel, contractors, and temporary employees of Wellington Management Company, LLP (WMC) and its affiliates.
Responsibilities	<p>Information Security Team must:</p> <ul style="list-style-type: none">• Maintain all standards documents• Grant approval for any mobile device not included in this standard• Document any exceptions to the standard <p>Employees, including contractors and temporary staff must:</p> <ul style="list-style-type: none">• Read and abide by all security policies and standards• Report any observed violations from this standard to their Wellington manager• Maintain control and possession of mobile devices issued by WMC, or purchased or leased by the individual in those instances where access to WMC information resources is enabled• Report the lost or theft of a mobile device immediately to the Solutions Center <p>Managers should:</p> <ul style="list-style-type: none">• Understand and enforce this standard• Ensure their employees and consultants read and adhere to the standard• Report any violation of this standard to WMC Information Security at ext (7)2444
Standards	<p>Mobile Devices are defined as devices that are easily portable and are used to connect to WMC information resources. These include, but are not limited to, laptops, smart phones, and handheld devices (e.g., Blackberry devices). This standard addresses the minimum security requirements for usage of these types of devices.</p> <ul style="list-style-type: none"><input type="checkbox"/> Mobile devices must employ appropriate encryption technology to protect all data resident on the device. The minimum levels of encryption required can be reviewed in the <i>WMC Encryption Standard</i>.<input type="checkbox"/> Mobile devices may only connect to the WMC computing infrastructure using a WMC-provided gateway technology with a minimum of 128-bit, triple DES encryption. An example of a gateway technology would be the NeoVPN, Outlook Web Access (OWA), or Blackberry Enterprise Server.<input type="checkbox"/> Mobile devices must employ an automated password lockout function.<input type="checkbox"/> Mobile devices must appear on the approved list of devices supported by WMC Information Services. The list is defined and updated by the Enterprise

Information Security Mobile Devices Standard

Revision: 1.3
January 10, 2007

Technologies Engineering Group and can be obtained by contacting the Solutions Center.

- ☐ All hand-held devices must have a format option for remote deletion of all WMC proprietary data if lost or stolen.

Wellington Management Company, LLP

Information Security Policy

Summary

The misuse of confidential information has the potential to cause harm to our clients, the markets in which we trade, and the reputation of our firm.

Wellington Management Company, LLP (“Wellington Management” or the “Company”) has a fiduciary duty to treat confidential information with care. This Information Security Policy document describes our obligations in this area. The Information Security Standards documentation provides further guidance and best practice reminders on related topics.

Policy Statement

Wellington Management prohibits any unauthorized access, disclosure, duplication, modification, diversion, destruction, theft, or other misuse of Confidential Information (defined below).

Any individual who violates this, or related information security policies, standards, or procedures for the protection of Confidential Information may be subject to disciplinary action up to and including termination of employment.

Standards Documentation

The Information Technology (IT) group will develop, maintain and monitor a set of Standards to support this Policy in light of the changing needs of the business and the evolution of the technical landscape. The Standards Documentation is published and maintained on the Wellington Management intranet at

<http://wmcintranet.wellmanage.com/infosec/Information%20Security%20Standards/>

Business units and IT are expected to incorporate procedures into their operational practices for the protection of Confidential Information in support of this policy and the Information Security Standards.

Scope and Accountability

This policy applies to all Wellington Management partners, employees, contractors, consultants, and temporary staff (collectively “Personnel”) who have access to Wellington Management information.

This policy applies to all computer systems and data communication systems owned, leased, operated, and/or accessed by Wellington Management Personnel for business purposes, and any Wellington Management data resident on those systems, or printed in hard copy, including data housed in cloud storage and personal media devices such as iPads, Blackberries and smart phones.

All Personnel are responsible for familiarizing themselves with and complying with all firm policies, procedures, and standards dealing with information security. Some Wellington Management offices may have additional policies, procedures, or standards as dictated by local government regulations. Personnel in these locations should familiarize themselves with Information Security Policy any local regulations and treat those as an addendum to the standard Wellington Management Information Security Policy.

Definitions

Confidential Information

- Information or data related to the firm's investments (e.g., investment decisions and processes, holdings, transactions, pool data), models, trading, and counterparties, client identifiable information such as account numbers, client names, unique identifiers, information regarding Wellington Management's Partners and Employees, or any other information designated by the firm as Confidential Information.

Data Owner

- The individual or group responsible for determining whether particular information should be considered Confidential Information. At Wellington Management, the Data Owner typically refers to a business unit.

Data Handling

Wellington Management's Confidential Information should be accessed and used only by those people who have a legitimate business need for such information.

**Computers, Laptops,
and Mobile Devices**

All Personnel must take reasonable steps to protect and secure all Wellington Management equipment and data.

**Release of Information
to Third Parties**

Unless it has specifically been designated as public or disclosure has been properly approved by the appropriate line manager, all Wellington Management's Confidential Information must be protected from disclosure to third parties (i.e., non-Wellington Management Personnel).

Wellington Management

Required Information Security Practices and Restrictions for Contingent Workers

1.0 Overview

All consultants and temporary employees (collectively “Contingent Workers”) working for Wellington Management are required at all times to follow the Required Information Security Practices and Restrictions outlined in this document and the supporting Reference Guide. After a review of the document you will be required to sign the Acceptance and Agreement form, attached hereto, acknowledging you fully understand and will adhere to the Required Information Security Practices and Restrictions.

This document provides a summary of the required practices, types of information at Wellington Management and twelve required security practices and restrictions.

2.0 Summary of Required Information Security Practices and Restrictions

As a Contingent Worker working for Wellington Management you are required to protect the firm’s information, the quality and value of the firm’s services for its client’s and the firm’s reputation. This includes but is not limited to: 1) following all firm information security policies, standards, and guidelines, 2) properly managing the security of any account credentials, 3) ensuring that information you will have access to is protected from unauthorized disclosure, 4) maintaining the confidentiality of Wellington Management’s client and vendor relationships, and 5) promptly reporting any suspected information security incidents to Wellington Management.

Protecting Wellington Management Information

You may have access to Wellington Management data, proprietary business plans, applications, source code and many other forms of internal Wellington Management information. Disclosure of Wellington Management information in any form may potentially risk the firm’s business operations, reputation and/or client’s confidentiality. You are **required** to keep all Wellington Management information on Wellington Management managed systems at all times, especially any firm confidential, client confidential or non-public confidential information as defined in the next section. To protect Wellington Management’s information you should always follow the required information security practices below:

- Do not copy, forward, or otherwise transfer Wellington Management information to Non-Wellington Management managed devices
- Only use your Wellington provided email account for Wellington Management business.
- Do not email to external addresses from your Wellington Management account without pre-approval from your Wellington manager
- Do not use external file sharing services to share or communicate Wellington Management information
- Do not use external developer collaboration services to share or communicate Wellington source code, test scripts, or any other work product.

Wellington Management

Required Information Security Practices and Restrictions for Contingent Workers

- Do not print Wellington Management documents except in the firm's offices or company offices restricted to Wellington Management use only, and never remove any printed materials from those restricted locations

Maintaining the Security of Your Account Credentials and Your Mobile Devices

Wellington Management has provided you access to accounts with a user name and password, and/or other authentication credentials. These accounts are to be used for accessing Wellington Management's applications, systems, data, and for remote access where approved. You are responsible to maintain the security of the account credentials at all time.

Wellington Management may permit you to receive email and other communications on a personal or firm-provided mobile device. Should you be provided such mobile access you are **required** to:

- Only access Wellington information on the device using the applications and processes provided by Wellington and in compliance with security guidelines.
- Maintain the security of your mobile device by keeping current on all application and mobile device security updates.
- Not bypass the vendor provided security (e.g. jailbreak) on the device
- Never expose or share your Wellington Management login credentials with anyone

Maintain the Confidentiality of Wellington Management's Client Relationship with Your Company

Wellington Management is a non-referenceable client of your company and no aspect of your company's relationship with the firm shall be discussed or shared. Wellington Management also prohibits posting, seeking or providing recommendations or referrals from current or former Contingent Workers, Wellington Management employees, customers or service providers. Follow the practices below to maintain Wellington Management's confidentiality:

- Do not discuss your role at Wellington Management with third parties
- Do not post Wellington Management information to career sites
- Do not post information about your role at Wellington Management, or Wellington Management-specific information of any kind, to social media

Reporting Information Security Incidents

You are required to immediately report Information Security incidents to enable Wellington Management to assess any incident and limit any impact to the firm if a security issue has occurred. Additional information on how to report an incident is available in the *Contingent Workers Required Security Practices and Restrictions - Reference Guide*.

Wellington Management
Required Information Security Practices and Restrictions for Contingent Workers

4.0 Required Information Security Practices and Restrictions – Reference Guide

#	Required Security Practice	Contingent Worker Restrictions	Examples of Restricted Actions	Exceptions
1	<p>Do Not Store Wellington Management Information on Non-Wellington Management Devices</p> <p>Non-Wellington Management Devices are your personal smart phone, laptop, tablet, or desktop computer</p>	<p>Storing of Wellington Management information to a Non-Wellington Management device is strictly prohibited.</p> <ul style="list-style-type: none"> Storing Wellington Management information, including your Wellington Management notes, emails, Skype chat comments, Wellington Management documents, on a Non-Wellington Management device Restriction includes your home computer, your tablet, your mobile phone This restriction especially restricts storing of Wellington Management Firm & Client Confidential information, Non-Public Personal Confidential information and Wellington Management Public information 	<p>“I had to join a conference call and I needed to view a document during the call. I saved the Wellington attachment to my mobile phone for the call.”</p>	<p>Storing and accessing information using Wellington provided applications, with mobile devices enrolled in Wellington Airwatch (Apple) or Good (Android)</p>
2	<p>Do Not Email to External Addresses from Wellington Management</p>	<p>Emailing to any external email address in any form, including any Wellington Management information in any form is prohibited unless specifically approved by your Wellington manager.</p> <ul style="list-style-type: none"> Emailing Wellington Management information externally to clients, vendors, business contacts, family, friends, and your own personal account without a pre-approved exception. Forwarding Wellington Management email or calendar events to your consulting company’s calendar, personal calendar, or personal email. 	<p>“I email copies of my Wellington team’s project documents so I can update them from home and have them ready for the next day”</p> <p>“I had some error log files the vendor needed to fix a critical issue; I emailed them to the tech support contact without getting pre-approval from my Wellington manager.”</p>	<p>Email to outside parties must be directly related to your Wellington responsibilities and approved by your Wellington manager.</p>

Wellington Management
Required Information Security Practices and Restrictions for Contingent Workers

#	Required Security Practice	Contingent Worker Restrictions	Examples of Restricted Actions	Exceptions
			"I like to keep two copies of my meetings, one on my Wellington calendar and one on my personal calendar."	
3	Do Not Use External File Sharing Services to Post Wellington Management Information	Posting Wellington Management information in any form to external file sharing services is strictly prohibited. <ul style="list-style-type: none"> Posting of your Wellington Management notes, emails, Skype chat comments, Wellington Management documents to your personal OneNote, DropBox, or other non-Wellington Management file sharing Service Exposing or mishandling of Wellington Confidential Information <ul style="list-style-type: none"> Sharing Wellington Confidential Information with outside parties such as product vendors Printing Wellington Confidential Information and leaving documents unattended Printing Wellington Confidential Information and not properly destroying the documents 	<p>"I use Evernote every day and found it easier to keep my Wellington work notes with my personal notes"</p> <p>"I was in a rush to test bug fixes and I needed production data. I made a copy of production with personnel information to the test environment"</p>	None
4	Do Not Use External Developer Collaboration Services	Posting Wellington Management Development Information in any form to external developer collaboration services is strictly prohibited. <ul style="list-style-type: none"> Posting of any development information including source code, specification documents, test documents, test data 	"I use GitHub to save a backup copy of my Wellington source code to my GitHub repo. I like to get comments from the community on my project"	None
5	Do Not Print Wellington Management Documents except in Wellington Management Offices or Company Offices Restricted to	Printing and removing Wellington Management documents is strictly prohibited <ul style="list-style-type: none"> Printing your Wellington Management notes, emails, Skype chat comments, documents in any location not provided for in the exceptions 	<p>"I print Wellington documents at home to review and make changes, then bring them back into the office."</p> <p>"I print Wellington documents and take</p>	Printing in a Wellington Management Office or Consultant Office that is physically is restricted to Wellington management use

Wellington Management
Required Information Security Practices and Restrictions for Contingent Workers

#	Required Security Practice	Contingent Worker Restrictions	Examples of Restricted Actions	Exceptions
	Wellington Management Use Only, and never allow printed documents to leave the approved restricted areas.	<ul style="list-style-type: none"> Removing printed documents from areas permitted in the exceptions 	them with me over the weekend to work on when I have spare time.”	only
6	Do Not Violate Wellington Management Proprietary Information and Copyright Protections	Sharing Wellington Management documents or information with an outside company is strictly prohibited <ul style="list-style-type: none"> Sharing of Wellington Management’s documents, source code, design, art work with another client or third party client 	“I took some of the code and a Web Page layout I developed for Wellington, removed any Wellington markings and showed my work to another client.”	None
7	Never Expose Your Wellington Management Login Credentials	Shared use or improper handling of your Wellington Management login credentials is strictly prohibited <ul style="list-style-type: none"> Writing down, storing in a file or file sharing application your Wellington Management User ID Password, or other credentials Using the same password for both your Wellington Management and personal accounts Sharing your Wellington Management password with anyone at any time 	<p>“I have to change my password often for Wellington so I put it in my mobile phone notes.”</p> <p>“I am going on vacation and I asked a co-worker on my team to check production processes. It was easier to just share my password then setup their account for access.”</p>	None
8	Never Put Your Mobile Devices You Use to Access Wellington Management at Risk	Exposing your mobile devices to potential theft or compromise is strictly prohibited <ul style="list-style-type: none"> Storing Wellington Management information, including your Wellington notes, emails, Skype chat comments, Wellington documents, on your mobile device is prohibited Storing Wellington Management information on any mobile device at any time with the exception Leaving your mobile devices unattended or in an unsecure location 	<p>“I am traveling to the US over a long flight and wanted to work on a Wellington deliverable on the way. I emailed the document to my personal account and saved it”</p> <p>“I have not enabled encryption on my laptop I use to access Wellington since I only use MyPC for access”</p>	Storing Files from Your Mobile Device to Wellington Management OneNote or Wellington Management File Share.

Wellington Management
Required Information Security Practices and Restrictions for Contingent Workers

#	Required Security Practice	Contingent Worker Restrictions	Examples of Restricted Actions	Exceptions
		<ul style="list-style-type: none"> Not taking steps to fully encrypt your Laptop or keeping your Anti-Virus software up to date 		
9	Do Not Discuss your role with Wellington Management with an Outside Party	<p>Discussing your work with Wellington Management or sharing any Wellington Management information with an outside party is strictly prohibited.</p> <ul style="list-style-type: none"> Discussing Wellington Management with vendors, professional colleagues, job placement specialists, friends, or family members Discussing Wellington Management with any of your company's other consultants who are not assigned to Wellington Management. 	<p>"I was at an industry event and I mentioned that I work for Wellington as a consultant"</p> <p>"At lunch in our common area, I shared with my colleagues who work for other clients that I worked a long weekend on a major software upgrade to the Wellington trading system."</p>	None
10	Do Not Post Any Wellington Management Information on Career Sites or Social Media Sites	<p>Including Wellington Management on your resume as your full time employer or posting Wellington Management on career or job search sites is strictly prohibited.</p> <ul style="list-style-type: none"> Adding "Wellington" to your resume as full time employer instead of using "Consultant at" or "Major Financial Services Firm" Posting any information about Wellington Management on career sites such as LinkedIn, or job search sites such as Career Builder <p>Posting Wellington Management's name or any reference to Wellington Management on social media is strictly prohibited</p> <ul style="list-style-type: none"> Posting any reference to Wellington Management on social media sites such as Facebook, Twitter 	<p>"I recently updated my resume and highlighted Wellington specifically and posted my resume to several job search sites"</p> <p>"I like to keep my LinkedIn profile up to date, so I posted my recent java development projects and referred to Wellington in my job experience on LinkedIn."</p>	None
11	Always Report Information Security Incidents	<p>Delaying or failing to report an information security incident is strictly prohibited.</p> <p>Report any Information Security incident to Wellington Management by contacting the solutions center: US +1-617-790-8400 or 6-8400</p>	<p>"I may have accidentally emailed Wellington trade data to an external email address. I didn't report it because the data was over month old"</p> <p>"I lost the Smartphone I use to access</p>	None

Wellington Management
Required Information Security Practices and Restrictions for Contingent Workers

#	Required Security Practice	Contingent Worker Restrictions	Examples of Restricted Actions	Exceptions
		<p>Global Office Access Lines: Beijing: +86-10-6622-7698 Frankfurt: +49-69-67-77-61-570 Hong Kong: +852-2846-8380 London: +44-20-7126-6666 Luxembourg: +352 2848 27098 Singapore: +65-6428-0299 Sydney: +61-2-8233-6498 Tokyo: +813-5533-0333 Zurich: +41 4326 81298</p> <p>Information Security Incidents Include:</p> <ul style="list-style-type: none"> ○ Lost/stolen mobile device ○ Disclosure of confidential data ○ Suspicious computer or account activity <p>Report Physical Security or Life-Safety issues on Wellington Premises to Global Security at +1-617-289-HELP (4357), or 6-4357:</p> <ul style="list-style-type: none"> ○ Suspicious person on Wellington premises ○ Suspicious postal mail or package ○ Suspicious phone call 	<p>my Wellington email, but I didn't report it because I just use it for email."</p>	

Wellington Management
Policies and Required Information Security Practices and Restrictions for
Contingent Workers
~Signature Page~

Acceptance and Agreement

By signing this Document, you, the Contingent Worker, verify that you have read all of the required Consultant Policies and Information Security Practices and Restrictions for Contingent Workers and that you understand, and agree to each of the policies, practices and restrictions herein.

Name (Print Name)

_____/_____/_____

Date

Signature