THE REGENTS OF THE UNIVERSITY OF CALIFORNIA

OFFICE OF THE CHIEF INVESTMENT OFFICER
1111 Broadway, Suite 2100
Oakland, CA 94607
(510) 987-9600

University of California Office of the Chief Investment Officer of the Regents (“UC Investments”)

Frequently Asked Questions Regarding the Confidentiality, Personal Trading & Material Non-Public Information Policy (the “Policy”)

Updated as of April 2020

This document contains answers to commonly asked questions about the pre-clearance and reporting obligations of covered persons (as defined below) per the Policy. In addition to the guidance provided below, Appendix A of the Policy also contains a list of helpful answers to questions you may have regarding your obligations under the Policy.

Q1: What is the purpose of the Policy?

A: The Policy was adopted by UC Investments to establish a standard of conduct that all covered persons (as defined in the Policy) must follow. The Policy is designed to ensure that all covered persons:

- Conduct UC Investments’ business and personal securities transactions in a manner consistent with the Policy, including avoiding any potential or actual conflicts of interest and any abuse of a covered person’s position of trust and responsibility; and
- Maintain confidentiality of information concerning UC Investments’ investment strategies and recommendations, holdings, and transactions.

Q2: Who is subject to the requirements of the Policy?

A: All **“covered persons,”** meaning a) all UC Investments employees, except unionized employees; b) all secondments working in UC Investments’ office; and c) spouses and dependents of the above referenced covered persons.

Q3: Which accounts are covered by the requirements of the Policy?

A: All **“covered accounts,”** meaning all self-directed brokerage accounts (including retirement accounts) with the capability of trading covered securities.

The following types of covered accounts are exempt from reporting:

- Treasury direct accounts
- Mutual fund only accounts
- 529 plans
- Retirement accounts where mutual funds or commingled funds are the only investment options

- Any account that is managed by a third party ("Managed Account"), provided that a Managed Account Certification is completed on MyComplianceOffice ("MCO") and the third-party manager's signed Managed Account Attestation is attached to the certification.

Q4: Which securities are subject to the requirements of the Policy?

A: All **"covered securities,"** meaning equities (public, private, preferred), bonds (registered and non-registered), private funds (hedge funds, private equity funds, venture capital funds), derivatives, and initial public offerings.

The following types of assets are exempt from pre-clearance and reporting:

- U.S. Treasuries
- Agencies
- Open-end mutual funds
- Exchange-traded funds (ETFs)
- Commercial paper
- Certificate of deposits
- Annuities
- Money market funds
- Cryptocurrencies
- Foreign exchange/currency exchanges
- Covered options
- Exercised options
- Derivatives where the underlying asset is:
    - Exempt from pre-clearance and reporting
    - Indexes
    - Commodities
    - Currencies

Q5: What kind of transactions require pre-clearance?

A: All transactions in covered securities, except the exempt asset types noted above and mandatory corporate actions, are required to be pre-cleared on MCO.

Q6: How can I access my account on MCO?

A: You can access MCO at the following link: https://mco.mycomplianceoffice.com/. Once you arrive at the page, please click on the "Sign In" tab in the top right corner and log in using your login credentials.

Q7: I am a new covered person who is disclosing their holdings of covered securities in the Account Disclosure and Initial Holdings Certification. How can I satisfy my reporting obligations under the Policy?

A: New covered persons can satisfy their reporting obligations regarding covered securities holdings either by manually disclosing all such holdings in the holdings table, or by attaching copies of the most recent brokerage statements of all disclosed covered accounts to the certification form. Following the initial disclosure, UC Investments or a designee will attempt to establish electronic brokerage feeds where possible.

Q8: I recently opened and disclosed a new covered account on MCO. How do I request for my account to be added to the electronic brokerage feed?

A: Once you have disclosed your new covered account by adding it to your list of accounts on MCO, please email CL.UC-OCIOCompliance@duffandphelps.com to request for your account to be added to the electronic brokerage feed. Please include the brokerage firm the account is held at and the last 4 digits of your account number in the email. The Duff & Phelps team will confirm whether your account is eligible to be added to the feed. If the account is eligible for the feed, Duff & Phelps will also provide updates if any further action is required on your end, or once the account has been successfully added to the feed.

Q9: I recently opened a covered account for which establishing an electronic broker feed is not possible or has not yet been established. How can I satisfy my reporting obligations under the Policy?

A: Covered persons must disclose all covered accounts by adding it to their list of accounts on MCO. When completing the quarterly certifications, covered persons must attach brokerage statements for the account for the quarter they are completing the certification for, regardless of whether there were any holdings or transactions in covered securities.

Q10: I recently opened a Managed Account (as defined below). How can I satisfy my reporting obligations under the Policy?

A: “Managed Account” means an account with the capability of trading covered securities that is managed by a third party who is not a covered person.

The Managed Account Attestation must first be completed by a third party that confirms that it has full discretion to act as investment advisor for the account(s) of a covered person. The Managed Account Attestation can be found in the “Documents” tab under “Policies and Procedures” on MCO.

Covered persons must then complete a Managed Account Certification for each Managed Account on MCO. When completing the Managed Account Certification, the third-party manager’s signed Managed Account Attestation must also be attached to the certification to exempt the account from further reporting obligations.

Q11: My spouse has a 401(k) account through his/her previous or current employer. Am I required to disclose this account?

A: If the account is self-directed and has the capability to trade covered securities, then the account should be reported and disclosed. However, if the only investment options available in the account are mutual funds or commingled funds, then the account is exempt from the Policy’s requirements.

Q12: I have no holdings in covered securities or covered accounts to report. What are my compliance obligations?

A: Covered persons must attest as such by completing the Account Disclosure and Initial Holdings Certification in MCO. In addition, covered persons must attest to their full list of covered accounts (or lack thereof) on a quarterly basis by completing the Quarterly Transaction Certification in MCO.

Q13: Who will be able to view my information and data reported through MCO?

A: The data maintained on MCO may be accessed by the compliance manager and authorized users designated by UC Investments, the MCO support team, covered persons' respective brokerage firms, and the Duff & Phelps engagement team. In the event of any breaches or employee non-compliance, this information may be further reviewed by the UC Investments Compliance Committee, consisting of the UCOP Deputy Chief Risk Officer, Chief Investment Officer, Chief Operating Officer, legal team or otherwise, as the compliance managers or their authorized designees determines in their sole discretion, in accordance with University of California policy and internal procedures.

Q14: What safeguards have been put in place to protect my sensitive information?

A: Duff & Phelps is committed to handling covered persons' sensitive information with the utmost care and strict confidentiality, and will limit the review of sensitive information to the least invasive degree of inspection required to provide its services. Duff & Phelps maintains strict controls regarding access to the MCO platform and limits access only to Duff & Phelps team members staffed on the engagement. In addition, Duff & Phelps will not share sensitive information gathered with anyone other than the compliance manager designated by UC Investments, any authorized designees, MCO, and covered persons' respective brokerage firms, as necessary. Should Duff & Phelps maintain any sensitive information, Duff & Phelps personnel shall ensure that all files are saved in a secure password-protected format.

With respect to information security and data privacy, MCO has implemented a variety of security and safety features designed to protect users' sensitive information. For further details regarding MCO's security features and policies, please see MCO's "Technology & Security Overview" presentation, which has been uploaded to the "Documents" tab under "Policies and Procedures" on MCO.

Finally, additional information regarding MCO's Privacy Policy and Duff & Phelps' Data Privacy Overview are outlined in Appendix A and B respectively.

Q15: How is excessive trading defined for the purpose of the Excessive Trading restriction?

A: While there is no value assigned to the maximum number of trades a covered person may conduct in a particular period of time, UC Investments expects covered persons to use their best judgement and trade in a manner that does not bring into question their fiduciary responsibilities, and is not indicative of inappropriate use of company resources or covered persons' time during work hours. Any patterns of frequent trading for a prolonged period of time will be escalated to senior management.

Q16: How are short term profits defined for the purpose of the Short-Term Trading & 30-Day Holding Rule?

A: Covered persons are prohibited from profiting off short-term trades of the same (or equivalent) covered Securities within 30 calendar days. An "equivalent" security means any warrant, convertible security, stock appreciation right, or similar right with an exercise or conversion privilege at a price related to the subject security, or similar securities with a value derived from the value of the subject security. A last-in, first-out methodology will be used for determining compliance with this rule and calculating any short-term profits to be disgorged.

Q17: When does the 30-Day Holding Rule "clock" reset?

A: The "clock" restarts every time a covered person buys a particular security. For example, a covered person may buy 100 shares of company A, and sell all or some of the shares on day 31, provided no additional shares were purchased in the past 30 days. The same covered person may buy more shares of company A at any time after his or her first purchase of 100 shares, but the clock will reset to 30 days after each purchase. For the avoidance of doubt, the 30-Day Holding Rule is based upon calendar days, and not business days.

Q18: What transactions/securities are exempt from the 30-Day Holding Rule?

A: The following transaction/security types are exempt from the 30-Day Holding Rule:

- Transactions effected pursuant to a pre-scheduled automatic investment program;
- Dividends and capital gains
- U.S. Treasuries;
- Agencies;
- Open-end mutual funds;
- Exchange-traded funds (ETFs);
- Commercial paper;
- Certificate of deposits (CDs);
- Annuities;
- Money market funds; and
- Cryptocurrencies.

Please note that some securities may be exempt from the pre-clearance requirements of the Policy but they may not be exempt from the 30-Day Holding Rule.

Q19: How will any short-term profits disgorged be disposed?
A: Covered persons are required to donate any disgorged short-term profits to a charitable organization approved by UC Investments management.

Q20: Are transactions effected prior to the effective date of the 30-Day Holding Rule subject to the rule?
A: Transactions effected prior to the effective date of the 30-Day Holding Rule shall be grandfathered in and are not subject to the rule.

For any further questions regarding OCIO's personal trading policies and procedures, please refer to the Policy or contact CL.UC-OCIOCompliance@duffandphelps.com.

Appendix A

MyComplianceOffice (“MCO”), Privacy Policy
Managed by TerraNua

Table of Contents

1. Introduction

The purpose of this document is to outline a privacy policy for use by TerraNua.

2. Executive Summary

The purpose of this policy is to ensure that all confidential information belonging to customers, staff, and third parties is handled and protected in accordance with the sensitivity of its nature.

3. Privacy Policy for TerraNua

3.1. Purpose

In the course of its business, it is necessary for TerraNua to collect, process, transmit, store, and otherwise handle personal data about individuals. This policy provides the basis for protecting such data while ensuring compliance with legal and regulatory requirements.

This policy should be read and used in conjunction with other related policies such as the TerraNua Information Security Policy.

3.2. Scope

The scope of this policy is to include all personal data which is collected, processed, transmitted, or stored (the term processed will be used throughout the remainder of this policy) by TerraNua, whether for its own purposes or those of its customers. This policy applies to all users within TerraNua. This includes permanent and temporary staff members, independent contractors, subcontractors, staff of partner organizations, or any user of the information processing systems and related services provided by TerraNua.

3.3. TerraNua Company Responsibilities

It is TerraNua's responsibility to ensure that an individual's right to privacy is safeguarded, that personal data is used only as intended, and that precautions preventing misuse are both effective and appropriate. TerraNua recognizes that in the course of its business it is necessary for TerraNua to record, store, process, transmit, and otherwise handle private information about individuals. TerraNua takes these activities seriously and seeks to provide fair, secure, and legal systems for the appropriate handling of this private information. All such activities at TerraNua are additionally intended to be consistent with the requirements of all applicable country, state, and federal privacy law, including (but not limited to) Massachusetts and California privacy laws, European Data Protection Directives, and generally accepted privacy ethics and standard business practices. As such TerraNua will ensure that personal data entrusted to it is:

- Processed fairly and lawfully, having satisfied the requisite conditions for processing
- Obtained for specified business and/or legal purposes and not be processed in a way which is incompatible with the purpose(s) for which it was collected
- Adequate, relevant, and not excessive for the purpose(s) for which it is processed
- Accurate and, where necessary, kept up to date
- Not kept for longer than is necessary to fulfil the purpose(s)

- Processed in accordance with the individuals rights as dictated by relevant legal requirements
- Appropriately protected against unauthorized, inadvertent, or illegal processing and/or disclosure
- Restricted to designated countries in accordance with legal and regulatory requirements

TerraNua will make all reasonable efforts to ensure that all private information maintained by TerraNua is reasonably accurate, timely, relevant, and complete. TerraNua will also make reasonable efforts to ensure that all private information is used only as intended, and that precautions preventing misuse are both effective and appropriate. TerraNua is additionally responsible for establishing appropriate controls to ensure that private information is disclosed only to those who have a legitimate business need, and that all such data is free from a significant risk of undetected alteration.

TerraNua will make all reasonable efforts to ensure that all such information is protected from unauthorized access and disclosure.

3.4. Disclosure of Personal Information

In accordance with certain privacy laws, TerraNua has a duty to disclose any personal information held on its systems, both electronic and paper based, belonging to individuals. Upon written request, TerraNua will disclose to the authorized individual all information held by TerraNua on that individual. Each individual retains the right to make corrections to any incorrect data held on them by TerraNua.

The exception to this policy is where information is being used in pursuit of criminal or civil case, and TerraNua is legally obligated to not reveal such information.

All requests for personal information coming from an individual must be forwarded to TerraNua's Chief Security Officer who will process the request as appropriate.

3.5. Handling of Personal Information

In general, TerraNua will collect, process, store, transmit, and disseminate only that personal information which is necessary for the proper functioning of its business. This information will be retained only for as long as necessary.

The collection of personal information about potential customers and others with whom TerraNua does business is to be expected. However, TerraNua must not collect personal information from individuals without having first obtained their knowledge and consent for the manner in which that personal information will be used.

TerraNua customers will be given an opportunity to inform TerraNua that they do not wish to be contacted via unsolicited direct mail, telemarketing, and related promotions. TerraNua staff must faithfully observe and act on these requests. TerraNua respects the rights of individuals to block data about them from being included in mailing lists or calling lists, block the sale of data about them to third parties, and to have data about them erased from direct marketing lists.

3.5.1. Development Using Private Information

TerraNua will ensure that the development, or acquirement, of all systems which will process personal data will do so in accordance with the requirements of this privacy policy and other related policy. TerraNua will not deploy production data on any non-production environment.

3.5.2. Privacy Impact Analysis

Where possible a Privacy Impact Analysis will be conducted to ensure any systems that are developed or acquired by TerraNua do not impact adversely on the privacy of individuals' personal data entrusted to TerraNua.

3.5.3. Destruction of Private Information

When private information is no longer needed, it must be destroyed securely by shredding or other approved destruction methods. Destruction of private information resident on computer disks and other magnetic media must be accomplished with a secure overwriting process or full disk format.

3.5.4. Removal of Private Information

Private and/or confidential information should not be removed from TerraNua offices. Permission to take such information off-site may be granted by Senior Management in exceptional cases and provided the involved member of staff will use the private and/or confidential information in accordance with the procedures and controls that support this privacy policy.

Third party access to private and/or confidential information should only be granted once a third party non-disclosure agreement has been signed and assurances given to TerraNua by that third party that they will ensure all necessary controls are in place to be consistent with the requirements of this policy and TerraNua's Information Security Policy.

3.5.5. Links between Separate Types of Private Data

Without advance consent from the Chief Security Officer, TerraNua's information systems must not be configured to support new links between private information and other types of information related to the same individual.

3.5.6. Testing With Sanitized Data

All software testing for systems designed to handle private data must be accomplished exclusively with "sanitized" production information. Sanitized information is production information which no longer contains specific details that might be valuable, critical, sensitive, or private. TerraNua will not deploy production data on any non-production environment.

3.5.7. International Data Transfers

Personal Information that TerraNua is entrusted with may from time to time be stored, processed, and transferred between any of the countries where TerraNua operates in order to enable TerraNua to use that personal information in accordance with this policy.

3.5.8. Data Retention

Personal information that TerraNua processes for any purpose or purposes shall not be kept for longer than is necessary.

3.6. Handling Employee Personnel Information

3.6.1. Access to Own Personnel File

TerraNua will provide a copy of an employee’s personnel file upon receipt of a written request. Employees are permitted to both examine and make one copy of the information appearing in their personnel file. If employees object to the accuracy, relevance, or completeness of information appearing in their personnel file they will be given the opportunity to request that TerraNua rectify said information.

3.6.2. Disclosure to Third Parties

TerraNua does not disclose the names, titles, phone numbers, locations, or other contact particulars of its employees unless required for business purposes. Exceptions will be made when such a disclosure is required by law, where the issue is a matter of extreme medical or other life threatening emergency, or when the involved persons have previously consented to the disclosure.

To preserve the privacy of personnel information, the reason for termination of employees must not be disclosed to third parties. Two permissible exceptions are the prior approval of a TerraNua Senior Manager, or if the disclosure is required by law. Separately, every disclosure of private information to third parties must be recorded against the employee’s personnel file.

3.6.3. Private Information from Job Seekers

Private information about a prospective employee may not be gathered unless it is both necessary to make an employment decision and also relevant to the job in question. This policy addresses marital status, family planning objectives, off-hours activities, political affiliations and other personal details.

Appendix B

Duff & Phelps ("D&P"), Privacy Policy

August 6, 2018

Preface

Duff & Phelps, LLC ("D&P"), has developed and implemented a number of policies and procedures to reasonably protect the firm from cyber security risks. Technical, physical and procedural safeguards are in place to deal with a variety of specific threats while frequent monitoring and review help protect the firm from yet to be discovered attack techniques. This overview describes those safeguards and provides excerpts from existing policies.

Management and oversight

D&P has a dedicated team of Information Security Professionals lead by Chief Information Security Officer (CISO), tasked with the development, implementation, and maintenance of the Firm's Cyber Security Program. The CISO reports to D&P's Information Security Steering Committee (DPISSC) which include CIO, COO, CISO and Chief Legal Counsel. The DPISSC is responsible to continually reviews and refines policies and procedures based on changes in the cyber security landscape. This team also receives support from internal and external experts in the cyber security space.

Information Security Program

D&P's mission is to anticipate and serve our customers' critical information needs. One critical need is to protect the confidentiality, availability and integrity of customer data. Another is to ensure that all necessary regulatory requirements for protection and handling of this data are met or exceeded. To answer these needs, D&P has established an Information Security Program that sets a strategy for protecting information assets using controls that are effective and efficient. The program is constantly reviewed and evolves as best practices, threats and risks emerge.

The Information Security Program is a key pillar of the ongoing success of D&P businesses in protecting and maintaining market reputation. The Information Security Program continually evaluates security controls and analyzes emerging threats to maintain the security posture within the organization. The strategy of defense in depth is focused on confidentiality, integrity and availability of client data to build secure solutions that clients can trust.

At its core the D&P Information Security Program consists of the following capabilities:

- Governance, Strategy & Business Alignment
- Policies and Standards
- IT Control Assurance
- Software Assurance
- Assessment and Evaluation
- Vulnerability Management
- Information Security Operations
- Measurements and Metrics
- Risk Management
- Security Incident Response
- Physical Security

Utilizing industry standards and collaborating with business leadership, the Information Security Program is aligned with ongoing business strategy. Success of the Information Security Program is based on effectiveness, efficiency, sustainability, and execution in line with the business strategy.

The governance process defines expectations, grants power and verifies performance of the Information Security Program. The governance process provided a method for effective and efficient decision which is key to the success of the program.

To be successful, the Information Security Program must be aligned with changing business strategies and security threats. Effective communication between business leadership, the governance committee and the Information Security team is vital to maintaining this alignment.

Business alignment is reflected in many aspects of the information security program including communication with potential customers and fulfillment of client requirements. Alignment is also demonstrated through attestation of controls to clients to support business strategy to win the market and be an industry leader.

Training

One of the biggest information security threats to any firm comes from the inside. In some instances, the threat can be due to pure lack of knowledge on how to handle information. All of our staff are required to participate in annual training and awareness programs. They are also required to electronically certify they have read and understand our policy sets, including specific policies for information security and privacy.

Staff are required to certify to the following policies, with certain groups of employees subject to additional policies not listed below:

1. Code of Business Conduct and Ethics
2. Personal Investment Policy
3. Records and Information Management Policy
4. Global Anti-Bribery and Corruption Policy
5. Global Privacy and Information Security Policy
6. Electronic and Telephonic Communications Policy
7. Travel and Expense Policy
8. Country Specific Employee Guide

Business Continuity and Disaster Recovery

Any type of threat to our employees, business, clients or general incidents are handled through our Global Crisis Management process. Our process is simple, direct, and effective. Based on a core platform of Business Continuity, the Global Crisis Management Team (GCMT) provides a centralized command center for any significant event. While typically a Local Crisis Management Team (LCMT) would lead an event, the GCMT has been historically the key driver to ensuring business continuity.

Our BCP local plans are globally distributed to key local contacts in each city. Annual awareness sessions and coordinated information update processes keep the plans fresh. Our GCMT is activated multiple times every year so recurrent testing is not performed. Our Technology Disaster Recovery processes are unit tested to minimize business impact.

To ensure our employees can continue to provide services in and out of our offices, our end-user computing platforms are based on globally standard and secured laptops.

Cyber Security Incident Response

Incidents specifically related to this space are handled through our Cyber Security Response Incident Response Plan. This Plan identifies our Incident Response Taskforce and defines the processes to be followed in the event of a cyber security incident.

Our plan is maintained by our Information Security team and reviewed regularly (annually at a minimum) by industry experts.

End-User Computing Environment

The Firm has global standards for all computing equipment. This ensures consistency for staff productivity, support efficiencies, and most importantly, security. All computers are managed globally through a set of centralized processes that technically enforce a secure environment. Specifically, each end-user computer is managed to the following feature set:

1. Full Disk Encryption. The Firm uses AES encryption with a 256bit key.
2. End-user equipment security. Every end-user computer has an industry leading security application installed and checked by our systems management platform. This provides a centrally managed solution for
    a. Virus and Spyware protection for viruses, malware, and spyware
    b. Real-time threat protection for unknown threats
    c. Network Threat protection for web and network based attacks
3. Centrally managed global directory service with enforced global policies allows specific control of settings and features of all domain attached computers. The policy system allows us to enforce other requirements in our IT Policies and Procedures manual such as:
    a. Inactivity screen lockout
    b. Enforced password complexity
    c. Enforced password expiration
4. End-user system management is further controlled through a global systems management platform. This allows for rapid deployment of software, inventories of applications, and control of running applications.
5. Asset Management processes control our inventory allocation from acquisition through disposal, including provisions for data storage device destruction.

Mobile Devices

All mobile devices are managed through one of our Mobile Device Management (MDM) solutions. No mobile handheld device is allowed to access our internal networks. Only email, calendar and contact information managed via MDM is allowed. The MDM solution also provides for:

1. Mobile security policy enforcement
2. Encryption for corporate data
3. Advanced reporting
4. Selective device wiping
5. Remote lock and remote disable

Core Infrastructure Environment

Datacenter

The Firm's core storage, enterprise applications, and centralized processing systems are all contained within our primary datacenter. This datacenter is a Tier IV datacenter which features:

1. Highly available facility with a TIA Tier IV classification. This is the highest level of classification for 99.995% uptime
2. 24x7x365 armed staff
3. Non-descript building with biometric and physical mantrap entry
4. Fully redundant environmental systems
5. N+1 diesel generators with local fuel contracts
6. Very Early Smoke Detection Apparatus systems (VESDA)
7. Enterprise class redundant storage
8. Redundant and fault tolerant core networking components

The core technical Disaster Recovery facility is geographically separated from the primary center and contained within a D&P managed facility. All client and business services are replicated to the DR center to ensure continuity in the event of a disaster.

Servers

All servers are managed and maintained centrally by our Technology Operations Group. Server health and overall infrastructure performance is monitored through an infrastructure management platform. The management platform provides unified management across on premise, service provider and cloud environments. Our servers are built and hardened using a well-known developed process to ensure consistency and security.

Utilizing the same processes, our virtualized servers are managed the same way a physical server is managed, configured and hardened.

Global Network Environment

Authentication

All user access is controlled through our security directory service. The directory service requires confirmation of the identity of a user before allowing access. The service supports a number of secure Internet-standard protocols and authentication mechanisms used to prove identity upon logon. At D&P we use the Kerberos V5 protocol.

All users have an individual network login account. Before gaining access, users must provide their unique logon name and password. Their logon name is supplied by the company and the password must meet 3 of 4 password complexity requirements. Passwords are forcedly changed every 90 days and must meet the length and complexity requirements. Password lockout occurs on 5 missed attempts. Shared accounts are prohibited.

Remote VPN users must have a D&P owned laptop with an additional hardware certificate installed for authentication.

Private WAN

Our global WAN (Wide Area Network) is centrally managed by our Technology Operations Group with physical staff in the US, UK and Italy. Our WAN is based on a global MPLS (multiprotocol label switching) offering from a top vendor with global presence. All offices are connected through the WAN and there is no network traffic sent over an unencrypted internet pathway.

Internet Access

Internet access is provided by a local provider in each office location. The connection is protected by a centrally managed Palo Alto Networks firewall appliance with appropriate monitoring and reporting. In the event of a local failure, internet traffic can be rerouted through the WAN to our primary datacenter through our Cisco firewalls.

Wireless Access

Centrally managed wireless access points ensure consistent protocols and performance. Utilizing state of the art secure access appliances, we also provide guest access with isolated traffic management.

Remote Access

Only D&P owned and managed equipment may directly access the network remotely. The D&P equipment must have a hardware security certificate installed and must be registered on one of the D&P managed domains. Web based email is available, but optionally disabled for some specific user profiles.

Monitoring and Reporting

We monitor our networks in a variety of ways. All of our monitoring tools provide real-time reporting to our Technology Operations team who responds as appropriate to any threats:

1. Intrusion Detection/Prevention (IDS/IPS) is done through:
    a. Industry standard IPS/IDS on our primary and secondary firewalls.
    b. Industry leading distributed firewall solution for local internet connections.
2. Performance and uptime is monitored via a solution providing fault, availability, performance and deep packet inspection tools.
3. Additional server network monitoring is provided by our infrastructure management platform.
4. Vulnerability scanning, is performed and reviewed on a monthly basis for both internal and external networks. The solution has internal and external devices with vulnerability signatures provided by a third party security vendor.
5. Penetration testing is done annually by an external provider.

Email Communications

All inbound and outbound email communications are run through an external security vendor. This provides an additional prescreen of inbound and outbound messages before they enter or leave our environment. This highly available service features:

1. Accurate and effective email spam and virus filter.
2. Skeptic scanning that attempt to block new and emerging threats.
3. Cloud based with queuing capabilities

Allowed Devices

For any end-user computer to gain access to our network, it must be registered on our multi-domain Active Directory service. Only devices owned and managed by the Firm are allowed access to the internal network. There are no BYOD programs or devices allowed to directly connect to our networks.

Physical Environment

Offices

Where physically possible, we secure all offices with a global security platform managed centrally. This platform provides card swipe access to various entry points around the globe. Secured area access (e.g., network closet) must be specifically granted and all access is recorded in a reporting platform. ID card sharing is prohibited and all staff are issued a unique ID card.

D&P offices in major metropolitan cities are typically Class A buildings with multiple additional layers of security. These buildings may have additional security staff and entry procedures.

Datacenter

Our primary datacenter is a Tier IV facility. This non-descript building is staffed 24x7x365 by armed security personnel. An access control list ensures only approved persons may enter the facility and then are escorted to our section. The datacenter floor is protected by a biometric authentication system with a mantrap cylinder which can only be released by local law enforcement.