University of California
Office of the Chief Investment Officer of the Regents ("UC Investments") POLICY – UC Investments Code of Ethics

Issued by: Chief Operating Officer
Issue date: March 27, 2017
Last Updated: September 26, 2024
Effective Date: October 1, 2024

I. Purpose

UC Investments has adopted this policy to establish the standard of business conduct that all covered persons (as defined in Appendix A below) must follow. This policy aligns with the University of California's Standards of Ethical Conduct[1] that all UC employees are subject to. In accordance with ethical standards, the policy incorporates the following general principles:

- Conduct UC Investments business and personal securities transactions in a manner consistent with the policy, which includes avoiding any actual or potential conflicts of interest and any abuse of a covered person's position of trust and responsibility.
- Maintain confidentiality of information concerning investment strategies and recommendations, holdings and transactions.
- Do not trade or recommend others to trade while in receipt of material non-public information.

II. Scope

This policy applies to all UC Investments staff, including full-time, part-time and contract employees, except union employees. At the discretion of the chief operating officer or his/her designee, consultants and other non-employees also may be required to adhere to this policy as a condition of their association with UC Investments. Such employees, consultants and other non-employees are collectively referred to as "covered persons" throughout this policy (see Appendix A for a definition of covered persons). Covered persons must read this policy in its entirety and will be asked to complete an acknowledgment at least annually, or whenever material policy changes take place.

III. Confidentiality

UC Investments produces, maintains and possesses confidential and proprietary information that covered persons must hold in **strict confidence.** This information may include, without limitation,

governing and operative documents, investment strategies and positions, investment updates, research analysis, legal advice. Covered persons may not use any confidential or proprietary information for their own benefit or enrichment. Likewise, they may not disclose confidential or proprietary information to anyone outside UC Investments, except in connection with the business of UC Investments in a manner consistent with UC Investments' policies or as required by applicable regulation, law or legal process. Failure to maintain the confidentiality of this information may have serious detrimental consequences to UC Investments as well as the covered person(s) who breached the confidentiality.

Please note that these confidentiality obligations are in addition to, and do not limit, any other confidentiality requirements set by the University of California Office of the President.

IV. Material Non-Public Information

This section of the policy describes the processes for handling material non-public information ("MNPI") and how to prevent covered persons from carrying out personal trading activities that conflict with the interests of UC Investments or otherwise might breach U.S. securities regulations and federal laws.

Occasionally, covered persons may come across confidential information or MNPI as part of his or her role with UC Investments. Covered persons are reminded that breaching regulations concerning MNPI can negatively affect the University's business reputation and can have real, personal consequences, including criminal penalties.

UC Investments policy equates MNPI acquired by any covered person while acting in his/her professional capacity or within the scope of his/her employment with UC Investments as belonging to UC Investments itself. In view of this policy, it is essential that covered persons not seek to obtain information that may be MNPI without the prior approval of the chief operating officer or his/her designee.

In the event that covered persons find themselves in possession of MNPI, they should notify UC Investments' compliance team ("compliance team") immediately. Covered persons must be aware that even where there is no expectation of confidentiality, a person may become an insider upon receiving MNPI. Whether the tip made to the covered persons makes him or her a "tipee" depends on whether the corporate insider expects to benefit personally, either directly or indirectly, from the disclosure. This benefit is not limited to a present or future monetary gain; it could be a reputational benefit or an expectation of a quid pro quo from the recipient by a gift of the information. Covered persons may also become insiders or tipees if they obtain MNPI by happenstance, at social gatherings, by overhearing conversations, etc.

Covered persons who are uncertain whether information they possess is material and non-public should consult the compliance team.

Covered persons are specifically prohibited from:

- Trading in securities on UC Investments restricted list
- Trading in the securities of an issuer while in possession of MNPI
- Trading ahead of orders placed on behalf of UC Investments
- Engaging in transmitting MNPI from an insider

What is Public Information?

Public information consists of information generally available in the public domain, including press releases, reports and financial statements filed with the SEC or foreign market equivalent regulatory agency (such as prospectuses, proxy statements, 10 Ks, 10 Qs and 8 Ks) and information published in media sources, such as Bloomberg, Reuters, CNBC, television and internet news, newspapers, periodicals, journals, and industry publications.

What is Non-Public Information?

For the purposes of this policy, any information that does not generally meet the above criteria for public information is considered non-public information. Non-public information is

information unavailable to the investing public. It may be provided to UC Investments, the University, or UC Investments' covered persons by an external source with the expectation that such information will be kept confidential and used solely for the business purposes for which it was conveyed. Typically, such information is provided to covered persons directly by a company or its agent pursuant to the terms of a confidentiality or nondisclosure agreement. Less frequently, covered persons may receive non-public information from other market professionals. Non-public Information may or may not be material. Non-public information is a broad category that includes:

- All information that a company provides pursuant to the terms of a nondisclosure or confidentiality agreement
- All other information about a company that is not publicly available, such as tips received directly or indirectly from a third party and information learned outside of the scope of one's employment or consulting relationship with UC Investments.

Once non-public information has been effectively distributed to the investing public, it is no longer classified as non-public. However, for the classification to change, the distribution of non-public information must occur through commonly recognized channels of distribution designed to reach the securities marketplace. Such instances include disclosure in a national business and financial wire service (e.g., Dow Jones or Reuters); a national news service (e.g., AP or UPI); a national newspaper (e.g. The Wall Street Journal or the New York Times); a publicly disseminated disclosure document (e.g., a proxy statement or prospectus); etc. The circulation of rumors does not meet the requisite public disclosure, even if the rumors are accurate, widespread and reported in the media. In addition, the information must not only be publicly disclosed, but there must be adequate time for the public to receive and process the information.

What is Material Information?

Material Information generally means any information (i) that is likely to affect the market price of a security, (ii) that a reasonable investor would be substantially likely to consider important in making his or her investment decisions, or (iii) that, when publicly disclosed, would be expected

to significantly alter the total mix of information in the marketplace about the security. Generally, this is information whose disclosure will have a substantial effect on the price of a company's securities. No simple test exists to determine whether information is material; assessments of materiality is a complex legal matter that continues to evolve and involves highly fact-specific inquiries.

Material information often relates to an issuer or a company's financial results and operations, including, for example, changes to dividend policies, earnings results, changes in previously released earnings estimates, significant merger or acquisition proposals, agreements, major litigation, liquidity problems, extraordinary management changes, declarations of stock splits and combinations, public or private offerings, changes of debt ratings, the development of new products, services or contracts, curtailment of any portion of the business's operations, as well as information obtained from an issuer or company in advance of a private offering for which UC Investments has entered into a confidentiality agreement.

Material information also may relate to the market activity of an issuer or company's securities. For instance, information about a significant order to purchase or sell securities may, in some cases, be deemed to be material. Pre-publication information regarding reports to be published in the financial press also may be material. Similarly, advance notice of an investment bank's intent to upgrade, downgrade or make other commentary regarding an issuer or company would be considered material.

Additionally, political intelligence, such as information learned from current or former government officials or government employees (whether domestic or foreign) could be deemed material. For example, this could cover, but not be limited to, confidential information about the results of non-public government hearings or regulatory decisions could be deemed material. Other scenarios related to political intelligence may also be deemed material information (and also non-public). For example, (i) non-public information provided by a congressperson or congressional staffer obtained from an executive branch department or agency (e.g., Treasury, FRB, FDA, FTC, etc.) regarding a matter under consideration by such department or agency; (ii)

information provided by a congressperson learned during the course of committee meetings that has not become public; or non-public information provided by a foreign government official or a representative of the office of a foreign government official.

It is important to note that, if there is a dispute about whether information is material, the courts will determine what is material after the fact, with the benefit of hindsight. As such, err on the side of caution when considering whether information is material or not. Should a covered person come across information that may be deemed material, he or she should assume the information is material and direct any questions regarding the materiality of information to the chief operating officer, or his/her designee.

Confidentiality versus MNPI

It is important that covered persons understand the difference between confidential information versus information that is deemed to be material non-public. Covered persons routinely have access to confidential information of UC Investments. Covered persons are generally permitted to share confidential UC Investments related information with one another but are strictly prohibited from sharing externally. As it pertains to MNPI, if a covered person receives MNPI they are not permitted to share this information with anyone both within UC Investments as well as externally, with the exception of the required escalation to the compliance team. As previously noted, when MNPI is received the compliance team will promptly add the respective issuer to the restricted list which is communicated to all covered persons. Covered persons are prohibited from sharing the restricted list externally. Please note, although information at UC Investments may be deemed confidential it generally is not considered to be MNPI.

Communications with Public Companies

Contacts with public companies represent an important part of the UC Investments' research efforts. UC Investments may make investment decisions based upon conclusions reached through discussions with such contacts and analysis of publicly available information.

When speaking to officers, directors, employees or agents (including lawyers, accountants and consultants) of a public company, employees must ensure that such person understands that you are not seeking any MNPI.

Contacts with Unaffiliated Advisers and Buy-Side Firms

When speaking to unaffiliated advisors and buy-side firms, covered persons must safeguard the confidentiality of UC Investments information, including definitive information about portfolio holdings, pending orders, and investment recommendations whose effect may not yet be reflected in the marketplace.

Securities on the Restricted List May Not Be Traded

UC Investments maintains a restricted list that includes issuers on which UC Investments possesses, or expects to come into possession of, MNPI. Some securities may be added as a result of regulatory requirements, for example, OFAC sanctions. Specific securities may also be added to prevent covered persons from potentially front running UC Investments' trades.

UC Investments trading desk will be restricted from trading in the portfolios any securities of issuers that are on the restricted list due to MNPI or regulatory reasons.

Covered persons will be restricted from trading in any security, including derivative securities, of issuers on the restricted list nor disclose the name of any issuer on the restricted list to anyone outside of UC Investments unless explicit permission is received from the chief operating officer or his/her designee.

See section X below for additional information on the types of securities that are restricted from personal trading.

Restricted Securities

The following securities are restricted from personal trading:

- Securities of issuers on which UC Investments office has MNPI. It is the responsibility of each covered person to notify UC Investments compliance team when he or she comes in contact with MNPI.

- Securities of publicly traded private equity firms whose funds are held in accounts managed by the private equity, absolute return, real assets, and real estate teams. This restriction does not apply to accounts managed by external managers. It is the responsibility of the private equity, absolute return, real assets, and real estate teams to notify compliance of such publicly traded private equity firms.
- Public equity securities that are held in accounts managed by the private equity, absolute return, or real assets teams. These may be securities that were initially bought as private securities but have since gone public. This restriction does not apply to public equities that are held in accounts managed by external managers. It is the responsibility of private equity, absolute return, and real assets teams to notify compliance of private holdings that are about to go public.
- Securities of public companies that are involved in the deals that the private equity, absolute return, real estate, and real assets teams are working on, or received MNPI on during the diligence process. To the extent that these teams are aware of any public company's involvement in a deal, they will notify UC Investments' compliance team.

Maintenance of the Restricted List

The compliance team, under supervision by the chief operating officer, is responsible for maintaining the restricted list. A company will be placed on the restricted list either at the time the chief operating officer or his/her designee approves a proposed election to receive MNPI or when the compliance team is notified by a covered person that he or she has come into the possession of MNPI.

In general, a company will be removed from the restricted list when:

- All MNPI possessed by covered persons becomes publicly available; or
- Projections, financial ratios, financial statements or other information possessed by covered persons becomes stale.

Any request to have a company removed from the restricted list must be directed to the compliance team. While the compliance team makes the final determination to remove a

company from the restricted list, it is the responsibility of relevant covered persons to monitor and promptly alert the compliance team as to the likely events that would justify removal. Some guiding factors for removing names from the restricted list include:

- If information is widely disseminated, then take the name off the next business day;
- Other situations – if the investment team has exited a deal after receiving MNPI, but prior to the deal getting finalized, the names can be taken off in 180 days (two quarters).

Exceptions

Any request for an exception from the restrictions discussed above must be directed to the compliance team. In appropriate circumstances, exceptions may be granted after consultation with senior management of UC Investments.

Trading on MNPI is Prohibited

It is unlawful to buy or sell securities based on, or while in possession of, MNPI, including information obtained through one's work at UC Investments. It makes no difference whether the undisclosed material information reflects positively or negatively on an issue. Covered persons must not trade in any accounts (including any UC Investments managed accounts or personal accounts) or advise others to effect transactions while in possession of MNPI. This prohibition applies regardless of whether the security is on the restricted list. Under U.S. federal law, these legal requirements are pursuant to Sections 10(b) and 21A of the Securities Exchange Act and regulations promulgated thereunder.

If there is any uncertainty about the possession of MNPI, covered persons are encouraged to speak to the chief operating officer or the compliance team before trading to avoid any breaches. Each covered person is personally responsible for complying with securities laws even in the situation where internal advice is obtained.

While in possession of MNPI, covered persons must safeguard the information in accordance with the terms of this policy and not intentionally or inadvertently communicate it to any person (including family members and friends).

Prohibition on Front-Running and Scalping

This policy prohibits personal trading based on the knowledge of proposed trading activity in a UC Investments account. This type of trading activity, referred to as front-running or scalping, could also violate securities regulations.

Front-running occurs when an individual with knowledge of UC Investments' trading intentions knowingly makes a trade in the same direction as UC Investments just before UC Investments makes its trade. This includes buying a security just before UC Investments buys that security (in the expectation that the price may rise based on such purchase) or selling a security just before UC Investments sells a security (in the expectation that it will lead to a drop in price). Front-running restrictions also prohibits covered persons from conducting speculative trading, for example, trading options, based on the knowledge of UC Investments' trading intentions.

Scalping is making a trade in the opposite direction just after UC Investments' trade. In other words, scalping is buying a security after UC Investments' stops selling, or selling a security after UC Investments stops buying.

Covered persons must conduct themselves in such a manner that all investments for the account of UC Investments take priority in all respects over investments owned by the employee, the employee's family, or any acquaintance. As a general reminder, any covered person who knows of a pending buy or sell recommendation or decision must not buy or sell the securities involved or encourage another person to buy or sell the securities before UC Investments takes action.

Tipping is Prohibited

Tipping refers to the transmission of MNPI from an insider (tipper) to another person (tipee) who may then buy or sell the securities. Tipping, whether done intentionally or not, is against the law. If a covered person receives MNPI about an issuer from any person this should be promptly

reported to the compliance team. The covered person should not trade in securities of such issuer, either for his/her own account or for UC Investments' account. MNPI need not come from a person known to be an insider to be covered by this policy.

Safeguarding of Non-Public Information

Access to Documents and Technology

You must safeguard and store documents containing non-public information in locked file cabinets or other secure locations when they are not in use. Documents containing non-public information should not be placed in office areas where unauthorized persons may have access and should not be left exposed on desks, printers, fax machines, copiers, or in work rooms or other locations that are not secure. Databases and other sources that contain non-public information and are accessible by computer or other technological means should be password protected or otherwise secure from access by unauthorized persons.

Discussions and Electronic Communications

Discussions relating to non-public information should be conducted with care and discretion. You should not discuss non-public information in public places such as hallways, elevators, taxis, airplanes, airports, subways, trains, restaurants, or open spaces within your household, etc. Speakerphones should not be used in circumstances where non-public information may be overheard. Mobile phones may not be secure; therefore, please use them with care. Also, use email and other electronic communications with care and in compliance with policies on use of electronic communications. When performing duties for UC Investments, you may only use UC Investments authorized email and instant messaging systems. Text messages are also prohibited to conduct substantive communication.

Physical Separation

UC Investments is physically separated from other parts of the University. Covered persons must act in a manner that is consistent with these physical barriers to restrict information flow and efforts should be undertaken to prevent inadvertent or improper access to non-public

information. The restrictions of this paragraph do not apply to any individuals designated by the chief operating officer or his/her designee as "above the wall" or to individuals brought "over the wall" on a temporary basis. One may be designated "above the wall" if, among other reasons, that individual is charged with risk management, legal or general oversight responsibilities and does not direct, effect, or recommend securities transactions. An individual may be temporarily brought over the wall by prior request to the chief operating officer or his/her designee. The request should identify the person to be brought over the wall, the reason for the request and the time period applicable. The chief operating officer or his/her designee will consider and approve, modify or deny the request, based on analysis of the risk to the University of granting the request. No wall crossing should occur prior to obtaining approval. Any person who is above the wall or brought over the will is subject to this policy.

V. Reporting

It is the responsibility of each covered person to immediately notify the chief operating officer or his/her designee if he/she has come into possession of MNPI or has reason to believe that they or another covered person has obtained or disclosed non-public information in a manner not permitted by law, these guidelines or another applicable UC Investments policy or procedure. In such circumstances, the covered person must not use or further disclose such information.

If there or any questions about possession of MNPI, you should promptly consult with the chief operating officer or his/her designee.

VI. Criminal and Civil Penalties

The seriousness of personal trading on MNPI is reflected in the penalties that it may carry, which are personal to the covered person. Penalties may range from disgorgement of profits to temporary revocation of personal trading privileges. If trading on MNPI is found to be a willful violation of the SEC's insider trading rules, the covered person may be penalized millions of dollars or imprisoned for many years, regardless of whether or not the covered person or any tipper

benefit from the violation. The SEC pursues a "zero tolerance" policy, and aggressively pursues "ordinary investors" such as spouses, cousins and friends of insiders.

The SEC also has the authority to seek a civil monetary penalty of up to three times the amount of profit gained or loss avoided as a result of an individual's illegal trading on MNPI. From the amounts imposed on violators as a penalty, the SEC is authorized to pay a cash bounty of up to 10% to persons who provided the information leading to the imposition of that penalty. In addition to the civil penalty, the SEC may seek other relief such as an injunction against future violations and disgorgement of profits resulting from illegal trading. Finally, private parties may bring actions against any person purchasing or selling a security while in the possession of MNPI. "Profit gained" or "loss avoided" is defined as the difference between the purchase or sale price of the security and its value as measured by the trading information.

In addition to the risk of civil and criminal penalties described above, covered persons who violate this policy may be subject to disciplinary action by the University, which may include termination of employment or its service provider relationship with the University.

VII. Pre-clearance of Transactions in Covered Securities

Refer to **Appendix A – Preclearance and Disclosure Requirements FAQs.**

VIII. Prudent Trading

All covered persons are expected to adhere to the highest ethical standards and must actively work to avoid actual or potential conflicts of interests that serve their own self-interests and not the best interests of UC Investments.

Personal trading should not conflict with the securities traded by UC Investments directly, or indirectly through an external manager, or in any way compromise the interests of UC Investments. Covered persons are prohibited from trading securities that are currently being discussed internally or with external managers, or are part of the transactions that are going

through due diligence. This restriction may apply even if such securities are not on the restricted list.

Covered persons are encouraged to seek clarification about potential conflicts of interest. If you have questions about a particular situation or become aware of a conflict, or potential conflict, you should bring it to the attention of the compliance team.

IX. Excessive Trading

While frequent personal trading may not, in and of itself, raise issues under applicable securities laws and regulations, a high volume of personal trading can be time consuming and can increase the risk of actual conflicts or appearance of conflicts that can lead to potential headline risks for UC Investments.

Covered persons must always conduct their personal trading activities lawfully, properly and responsibly, and are encouraged to adopt long-term investment strategies that are consistent with their financial resources and objectives. We discourage high levels of personal trading activity as well as short-term trading strategies, and covered persons are cautioned that such strategies may inherently carry a higher risk of regulatory and other potential scrutiny.

Excessive or inappropriate trading of any security during working hours will not be tolerated and will be escalated to management and Human Resources. Reasons for this include:

- Interferes with job performance or work functions
- Constitutes a misuse of company resources for personal gain
- Gives rise to conflicts or perceived conflicts
- Compromises the fiduciary duty that we owe to our stakeholders and clients

The excessive trading restriction does not apply to:

- U.S. Treasuries
- Agencies

- Open-end and closed-end mutual funds
- Exchange-traded funds (ETFs), including options on ETFs
- Commercial paper
- Certificate of deposits
- Annuities
- Money market funds
- Cryptocurrencies
- Automatic transactions taking place on pre-determined timeframe

X. Short-Term Trading & 30-Day Holding Rule

Any profits recognized from short-term personal trades must be disgorged in order to minimize the appearance of a conflict of interest. For purposes of disgorgement, profit recognition is based upon the difference between the most recent purchase and sale prices for the most recent transactions. Accordingly, profit recognition for disgorgement purposes may differ from the capital gains calculations for tax purposes. The disposition of any disgorged profits will be at the discretion of UC Investments Management and Compliance Committee, and the employee will be responsible for any tax and related costs.

30-Day Holding Rule

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. Thus, for example, the rule prohibits profiting from short sales of a covered security within 30 days of the purchase of the underlying security. The rule permits, however, profiting from an option transaction within 30 days of the purchase or sale of an underlying security provided the expiration date of the option is at least 30 days after the option transaction. The rule applies regardless of the employees' other holdings of the same security or

whether the employee has split his or her holdings into tax lots. A last-in, first-out methodology will be used for determining compliance with this rule and for disgorgement calculation purposes. In effect, the 30-day holding rule "clock" restarts each time the employee trades in that security. However, securities transactions that are effected pursuant to an automatic investment plan are not considered for determining compliance with this rule and for disgorgement calculation purposes. Automatic reinvestment would not be in scope with the spirit of this rule.

The closing of a position (including exercise) in an option or contract on any security (other than those covered securities exempt from this rule) will result in a 30-day holding rule violation if the position was opened within the 30-day window and the closing transaction results in a gain. Multiple positions will not be netted to determine an overall gain or loss in options on the same underlying security expiring on the same day.

Profiting in violation of the 30-day holding rule will result in the disgorgement of any profit received with the proceeds donated to a charitable organization approved by UC Investments management. Repeated profits in violation of the rule may result in other actions deemed appropriate by the UC Investments compliance team and management.

The 30-day holding period rule does not apply to:

- U.S. Treasuries
- Agencies
- Open-end and closed-end mutual funds
- Exchange-traded funds (ETFs), including options on ETFs
- Commercial paper
- Certificate of deposits
- Annuities
- Money market funds
- Cryptocurrencies
- Automatic transactions taking place on pre-determined timeframe

* Note that some securities may be exempt from pre-clearance requirements but they may not be exempt from the 30-day holding requirements.

Derivative Transaction Restrictions

Transactions in derivatives, including options, are prohibited unless the expiration of the instrument is at least 30 days after the transaction. The policy will prohibit opening a position in the front-month contracts unless the contract expires 30 days or more after execution of the transaction.

Questions about this rule should be directed to the UC Investments compliance team or to your supervisor.

XI. Certifications

Covered persons will be asked to complete various certifications:

Initial Disclosure:

Within 30 calendar days after becoming a covered person, such person shall report on the MyComplianceOffice ("MCO") platform all of his/her covered accounts as well as covered securities held in these accounts (see Appendix A for definitions of covered accounts and securities as well as initial disclosures).

Ongoing Disclosure:

On a quarterly basis, covered persons will be required to update their personal accounts and holdings disclosures in MCO as needed. They will also be asked to acknowledge their compliance with the disclosure requirements of this policy (see Appendix A for more information on ongoing disclosure requirements).

Quarterly Transaction Certification

Covered persons will certify all transactions in covered securities and covered accounts within 30 calendar days after quarter-end. This certification will be completed in MCO. For accounts that are set up with electronic feeds, the system will automatically display all trades from the previous quarter; however, for accounts that do not receive electronic feeds, covered persons will need to upload statements that display all trading activity from the previous quarter.

If covered persons open new brokerage accounts, they must disclose those accounts in MCO prior to trading any covered securities.

UC Investments Code of Ethics Acknowledgment and IPS Acknowledgment

Covered persons must read this policy in its entirety and will be asked to complete an acknowledgment at least annually, or whenever the policy incorporates material changes.

Additionally, employees will be asked to acknowledge that they understand their teams' responsibilities with respect to the guidelines listed in the IPS. They will also be asked to acknowledge that they have processes in place to ensure compliance with the IPS guidelines that pertain to their teams.

XII. Responsibility for Policy

The establishment and review of this policy and the oversight of its implementation by management is the responsibility of the chief operating officer or his/her designee, who will also be responsible for the administration, interpretation, and application of this policy.

XIII. Compliance Committee Reviews

The UC Investments Compliance Committee will meet on a periodic basis to review Covered Persons' violations of the Policy and will take appropriate steps as needed.

The Compliance Committee currently consists of the following members:

- Chief operating officer (UC Investments)
- UC Investments Director, investment transactions & operations (UC Investments)
- Director, investment risk management (UC Investments)
- Deputy chief risk officer (UCOP)
- HR business partner (UCOP)
- Manager, investment compliance & operational risk (UC Investments)

XIV. Operational Risk

A. BYOD (Bring Your Own Device) Policy

The purpose of this policy is to provide acceptable BYOD guidelines for UC employees. This standard aims to balance the benefits of increased flexibility and productivity with the need to safeguard sensitive organizational information and maintain a secure computing environment. BYOD allows access to UCOP/Investments systems with a personally owned mobile phone, tablet, laptop, or computer, is allowable provided that the device complies with this standard and related policies.

This policy applies to all covered employees who use their personal devices (e.g., mobile phones, tablets, laptops, and desktop computers) to access, store, or process UCOP/Investments institutional information (i.e., data) and/or access UCOP/Investments IT resources (e.g., systems, networks).

Eligibility

To be eligible to participate in the BYOD program, and individual must meet the following criteria:

- Receive approval from IO Director/Managing Director, Investment Transaction Services or Chief Operating Officer. Approval is subject to review and may be revoked at any time.
- Receive approval from IO Director/Managing Director, Investment Transaction Services or Chief Operating Officer. Approval is subject to review and may be revoked at any time.
- Enable device password-protection on phone/tablet devices.

- Keep device operating system and applications updated with the latest security patches no further than 30 days from release.
- Report all lost or stolen devices that may contain or allow access to UC institutional information or IT resources immediately to the UCOP IT Service Desk.

Prior to departing UCOP, all UC data and software must be removed from BYOD device. This includes but is not limited to UCOP saved passwords, UCOP system information (e.g., network diagrams, manuals, configuration guides), UCOP applications, UCOP network settings, UCOP institutional information and UCOP security tools.

Non-compliance with this standard may result in disciplinary action, up to and including termination of employment or contract. Computing devices found to be non-compliant to these standards and without an exception on file are subject to being disconnected from the UCOP network and prohibited from connecting to UCOP resources.

Requests for an exception to this standard may be made by contacting Jimmy Castro (jimmy.castro@ucop.edu)

B. Travel Policy (High-Risk Countries)

The Department of homeland security (DHS) and The US Department of State has issued a warning regarding Chinese government cyber actors who continue to target key critical infrastructure sectors in the United States, including healthcare and public health, financial services, the defense industrial base, government facilities, and communications. Employees should reconsider travel to Mainland China due to the subjective enforcement of local laws, including in relation to exit bans, and the risk of wrongful detentions and potential confiscation of hardware and data.

Employees travelling outside of the United States to high-risk countries are required to request a loaner laptop from UCOP IT and utilize the UC VPN when conducting UC business. If an employee is unable to come to the office for a loaner laptop, then the employee must uninstall the Box folder and utilize the UC VPN while overseas.

Procedure

- To request a loaner laptop, please initiate your request directly through Jimmy Castro (jimmy.castro@ucop.edu) or reach out to the IT Service Desk (servicedesk@ucop.edu).
- Travelers are responsible for transferring all data from the loaner laptop to their own computer or storage device before returning the loaner laptop. Any data left on the loaner laptop may be wiped and may not be retrievable. UCOP IT is not responsible for lost data.
- Loaner Laptops may be borrowed for up to two weeks. Exceptions may be made on a case-by-case basis, subject to availability. It is advised to reserve equipment at least two weeks before departure and to pick up the equipment a few days early incase any additional software needs to be installed.

C. Artificial Intelligence(AI) Policy

This Policy is geared solely towards legal concerns with respect to generative AI tools, including ChatGPT, Microsoft Copilot, Bing Chat, Google Bard, Snap's MyAI and other up and coming AI tools. Such AI tools generate responses based on user prompts or user data, as well as data scraped from public websites. They fine-tune themselves to understand and interpret user inquiries, then generate relevant responses. Tools such as ChatGPT are versatile, able to write computer programs, compose music and essays, play games, and simulate chat rooms. They also have several known limitations, including uneven factual accuracy and bias.

The use of such AI-enabled tools raises legal, compliance, and ethical questions to consider[2], and we offer the following guardrails for use of these tools. As always, check with your local legal counsel and privacy and security officials for specific questions regarding your location's use of generative AI tools.

1. Confidential Information of UC and Third Parties, Privileged Information, and Personal Information

Unless specific precautions are taken, any content that is provided to generative AI tools can be

[2] For discussion of some of these ethical considerations by UC, refer to UC's Presidential Working Group on Artificial Intelligence, Responsible Artificial Intelligence Recommendations to Guide the University of California's Artificial Intelligence Strategy (October 2021).

saved and reused by the company offering the tool (e.g., OpenAI for ChatGPT) and their affiliates. Therefore, unless Units enter into properly negotiated agreements with these companies, Units are prohibited from providing any information that could be construed as confidential information of UC, or confidential information of a third party. Such disclosure could cause UC to be in violation of contractual requirements.

Confidential information of UC or of third parties, including information that may be protected by a privilege, such as attorney-client privileged information, or psychotherapist-patient information, also may not be provided to generative AI tools. UC employees do not have the authority to disclose attorney-client privileged information of the University.

Similarly, Units are prohibited from providing these generative AI companies and tools with personal information, including but not limited to the financial or medical information of UC's employees, students, and patients. Such disclosure (even if the data is de-identified) could run afoul of underlying laws protecting the data, including but not limited to, the Health Insurance Portability and Accountability Act (HIPAA), the California Constitutional of Medical Information Act (CMIA), and the California Information Practices Act (IPA). Not only would sharing this information be a privacy violation, but this data could also be exposed by a data breach. Indeed, in March 2023, a bug leaked ChatGPT users' "first and last name, email address, payment address, the last four digits (only) of a credit card number, and credit card expiration date". https://openai.com/blog/march-20-chatgpt-outage. Breaches such as these could subject UC to reporting obligations and penalties under state and federal breach notification statutes

2. Output Generated by Generative AI Tools

Output generated by generative AI tools, including chatbots, may not always be correct, and could also infringe on the intellectual property rights of others. If UC has no direct contract with a generative AI tool provider, there is no obligation for them to defend or indemnify the University in claims brought by third parties. Some AI companies have also recognized that their tool sometimes exhibits biased behavior. See more about the limitations of ChatGPT here.

3. Free-to-Use Generative AI Terms

Generative AI services have terms of use and/or privacy policies that should be reviewed, as they may automatically apply if the service is used. Acceptance of such terms as written could expose UC to unacceptable and costly risks, including, but not limited to, liability for third-party acts or omissions, privacy law violations, and liability for infringement. Work with local procurement officers prior to finalizing any transactions to include agreement terms that comply with UC policies.

For example, if you use ChatGPT, you are automatically deemed to have agreed to its Terms of Use and Privacy Policy, which are subject to change. These terms currently include:

- Restrictions on use and distribution of ChatGPT content;
- The right for OpenAI to use content provided to it to help develop and improve its Services;
- An obligation to defend, indemnify, and hold OpenAI and its affiliates and personnel harmless from and against all claims "arising or relating to your use of the Services." Note that this violates Standing Order 100.4(dd)(9), which could subject UC to third-party claims.
- A limitation of OpenAI's liability, with aggregate liability not exceeding the greater of the amount paid to use ChatGPT, or $100; and
- Unless this form is completed, within 30 days of using ChatGPT any dispute with OpenAI over the use of ChatGPT is subject to final and binding arbitration. The arbitration terms are here.

4. Location Risk Assessments and Review

Whether for internal UC business, education, research, or other purposes, the use of free-to-use and paid AI products should undergo location-based risk assessments by information security, with participation from legal counsel and privacy officers. Procurement offices should also review and negotiate problematic terms such as insurance, indemnification, and limitations of liability

with appropriate input from risk, privacy, security, and other units. Given the potential use of these products to access regulated data (e.g., scanning student essays or other FERPA-protected records for plagiarism, or parsing patient health information to facilitate access to care and improve outcomes), such contracts must include an Appendix Data Security, and, where PHI is involved, an Appendix - Business Associate Agreement. Contact UC Legal when engaging vendors who provide AI-based products so that we can help assess privacy and data security implications. Locations should also conduct an equity or nondiscrimination assessment of the tools to be used, in consideration of recent enforcement action at both the federal and state level related to AI bias.

XV. Covered Person Violations

UC Investments adheres to the following procedures to remediate identified covered persons' violations of the policy:

1st Violation: The UC Investments compliance team will have a discussion with the covered person and his/her manager regarding the violation. A memo of reprimand will be issued to the covered person and included in his or her employee file.

2nd Violation: The covered person may be subject to corrective action as mentioned in UCOP's Personnel Policies for Staff Members ("PPSM") – 62[3], also referred to as PPSM-62, which may include a financial impact or termination of employment as per PPSM-64[4]. Any non-compliance or violation of law may also result in civil and criminal penalties.

UC Investment Compliance Reporting: UC Investments' quarterly compliance reporting will include the listing of all covered persons' violations of the policy.

[3] https://policy.ucop.edu/doc/4010411/PPSM-62
[4] https://policy.ucop.edu/doc/4010413/PPSM-64

Appendix A – Preclearance and Disclosure Requirements FAQs

UC Investments Code of Ethics	
Who is considered a "covered person"?	• All UC Investments employees, except unionized employees • Certain secondments, contractors, and consultants working in UC Investments office that have access to MNPI as determined by Compliance.[i] Documentation will be maintained as to why certain secondments are not considered "Covered Persons" • Spouses and dependents of the above covered persons
Which accounts are considered "covered accounts" and require disclosure?	Self-directed brokerage accounts (including retirement accounts) with the capability of trading covered securities. The following accounts are exempt from reporting: • Treasury direct accounts • Mutual fund only accounts • 529 plans • Retirements accounts where mutual funds or commingled funds are the only investment options • Any account that is managed by a third party, 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.
Which securities are considered "covered securities" and are subject to pre-clearance and reporting?	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 assets are exempt from preclearance and reporting: • U.S. Treasuries • Agencies • Open-end and closed-end mutual funds • Exchange-traded funds (ETFs) • Commercial paper

	• Certificate of deposits
	• Annuities
	• Money market funds
	• Cryptocurrencies
	• Foreign exchange/currency exchanges
	• Automatic transactions taking place on pre-determined timeframe
	• Covered options
	• Exercised options
	• Derivatives where the underlying asset is:
	  ○ Exempt from pre-clearance and reporting
	  ○ Indexes
	  ○ Commodities
	  ○ Currencies

How does the pre-clearance process work?	All transactions in covered securities, except mandatory corporate actions, are required to be pre-cleared in MCO. Covered persons' spouses and family members who are subject to the pre-clearance policy should ask the covered person to submit pre-clearance requests in MCO on their behalf. In certain cases, where pre-clearance cannot be obtained in MCO, covered persons may send an email to UC Investments compliance team to get manual pre-clearance. MCO will reconcile all pre-clearance requests against the firm-wide restricted list. The employee will receive an automated approval as long as the requested security is not on the restricted list. The latest version of the restricted list can be found in MCO, or it may be requested from the compliance team via email. Requests to transact corporate bonds, term loans, or other securities that may be traded by UC Investments' internal trading desk will require manual approval from the compliance team. An approval or denial of the request will be provided via MCO following the completion of the review. Requests to pre-clear private equity securities will also require manual approval form the compliance team. Refer to MCO desktop procedures for step-by-step procedures in submitting pre-clearance requests. Pre-clearance approval will be effective for two business days (the day on which approval is granted, if approved during market hours, and one additional business day). Pre-clearance approvals for private investments are exempt from the two business day effective period. Covered persons should complete the transaction as soon as practicable after receiving pre-clearance approval. Pre-clearance approvals for limit orders are also exempt from the two business day rule mentioned above, however, covered persons must comply with the following: • On the MCO pre-clearance form, indicate that the trade is a limit order by clicking "Yes" under the limit order field • Include the limit price in the comments field of the pre-clearance form

	• If covered persons wish to change the limit price at which they want to trade, new pre-clearance form must be submitted
	• Include other terms of the limit order in the comments field of the pre-clearance form. For example:
	  o Day Trade
	  o GTC (Good Till Cancel)
	  o Fill or Kill
	  o Immediate or cancel
	  o On the Open
	  o On the Close
	
	• The GTC date must not exceed 90 days from the date of pre-clearance. Covered persons will need to enter new limit order and pre-clearance form after 90 days
	• The limit trade will typically execute once the limit price is met and some brokers may split lots whch will still count as one transaction for compliance purposes
	• Covered persons may not engage in excessive use of such orders, and
	• The trade(s) may not present any other concerns/risks

What are the disclosure requirements for newly opened covered accounts?	Covered persons must disclose new covered accounts in MCO prior to trading any covered securities in the account.

How does the certification process work?	1. Disclosure of Covered Accounts and holdings
	  a. Covered persons will be given 30 calendar days from quarter-end to submit required information to compliance and/or designated third-party compliance support staff.
	  b. Any newly opened covered accounts must be disclosed in MCO prior to trading any covered securities in the account.
	  c. For newly hired covered persons, required information must be submitted no later than 30 calendar days after joining UC Investments.
	2. Quarterly Transaction reporting
	  a. Employees must certify all transactions in covered securities within 30 calendar days after quarter-end.
	
	To the extent possible, all covered accounts will be set up on MCO to establish direct electronic feeds with brokers or custodians. Employees are required to upload brokerage statements for covered accounts for which electronic feeds cannot be established when completing their quarterly transaction certifications.
	
	Refer to MCO desktop procedures for step-by-step procedures in completing required reporting and certification.

Automated platform	MyComplianceOffice (MCO) is an automated compliance platform that will support the policy's pre-clearance and reporting requirements. Each UC Investments employee will be assigned web-based access to the platform.
Managed Account	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. In order to exempt a managed account from further reporting, a signed managed account attestation must 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 must also be attached to the completed managed account certification on MCO.
Restricted Securities	Compliance maintains a list of restricted securities. Issuers may be added to the list because UC Investments possesses or expects to come into possession of material non-public information (MNPI). Specific securities may also be added to prevent potential front running. In addition to the firm-wide restricted securities, certain investment team members may be subject to additional restrictions due to discussion of specific securities with external managers. This customized restricted list is reviewed by Legal and maintained by the compliance team. The latest Restricted list will also be saved in MCO.
Post-Trade Surveillance	The compliance team and/or designated third party compliance support staff will be performing periodic surveillance and analysis of trading activities. Please prepare to provide additional information or explanation upon request.

[i] Compliance will determine which secondments, contractors, and consultants will be defined as "Covered Persons" subject to this policy based upon discussions with immediate supervisors and the type of work the individual will be conducting and what access the individual may have to MNPI.