Acceptable Use Policy Acknowledgement

Instructions: Please read the following KPMG policy and sign below to acknowledge your receipt and understanding of the policy. Please print and retain a copy for your files.

Acceptable Use Policy

The Acceptable Use Policy (AUP) describes policy requirements all resources are to follow when accessing or using KPMG Information Technology Resources. Please read and acknowledge the latest Acceptable Use Policy (pages 2-21) and reference the FAQs (pages 22-24).

I acknowledge that I have fully read, understand, and affirm my agreement to comply with the Acceptable Use Policy.

Ajinkya Nimbhorkar
Print Name

Signature

Date

KPMG

Acceptable use policy

Confidential

For all KPMG LLP partners, employees, contractor personnel and other authorized third parties who access or use KPMG IT Resources

July 2024

kpmg.com

Contents

1. Introduction 2
2. Guiding principles 2
3. Ownership of KPMG IT Resources 3
4. Intended Use of IT Resources 4
   4.2 Use of unapproved third-party equipment or services 4
5. Protecting KPMG Technology Assets and Media 5
   5.1 Use of removable media – Encryption and other controls 5
   5.2 Protecting KPMG IT Resources 6
   5.3 Physically securing KPMG IT Resources 6
6. Technology Solutions use 7
   6.1 Approved Technology Solutions 7
   6.2 Prohibited Technology Solutions 8
   6.3 Use of software 9
7. Access to KPMG IT Resources 9
   7.1 Passwords and other credentials 9
   7.2 Third-party access to KPMG IT Resources 9
8. Electronic communications requirements and useof communications tools 9
   8.1 Electronic communication requirements 10
   8.2 Approved software for electronic communication 10
   8.3 Use of the internet 11
   8.4 Appropriate use of the KPMG intranet or portal sites 12
   8.5 Email and other electronic communication tools 12
   8.6 Wireless technologies, including Bluetooth 13
9. Client-related requests 13
   9.1 Controls for connecting KPMG IT Resources to client networks 13
   9.2 Approved activity using client networks 13
   9.3 Client-related software requests 14
   9.4 Responding to client inquiries 14
10. Information and Cybersecurity Incident reporting 14
   10.1 Reporting Information and Cybersecurity Incidents 14
11. Monitoring and enforcement 16
12. Retired partner and expatriate access toKPMG IT Resources 16

1. Introduction

In this Acceptable Use Policy (AUP), KPMG LLP[1] ("KPMG"), the U.S. member firm of KPMG International, describes the policy requirements all KPMG partners, employees, contractor personnel, and other authorized third parties (collectively "KPMG Personnel") are required to follow when accessing or using KPMG Information Technology Resources ("KPMG IT Resources") or engaging in firm business-related electronic communications regardless of whether KPMG IT Resources are used. This AUP also applies to retired partners and expatriates. KPMG IT Resources are defined as IT equipment, devices, computer systems, appliances, scripts, bots, email, internet, fax, phone, voice mail, infrastructure, and Technology Solutions owned, issued, and/or managed by KPMG. A "Technology Solution" is defined as software and services, including internet and cloud services, cloud environments and open-source software, whether developed by KPMG or licensed from a third party (including KPMG International or its member firms).

As members of an accounting and professional services firm, KPMG Personnel must protect Confidential Information, as set forth in **RMM Chapter 15 – Confidentiality, Privacy, and Information Protection**, in accordance with applicable legal requirements and professional standards. Our work with Confidential Information is highly integrated with our KPMG IT Resources and is a key part of our information protection program. Thus, any use of KPMG IT Resources or firm business-related electronic communications must be in compliance with applicable firm policies, including, but not limited to, this AUP, the **Code of Conduct**, **U.S. Risk Management Manual**, and Talent and Culture (T&C) policies. Failure to comply with these policies may result in serious professional, legal or brand consequences.

KPMG reserves the right to deploy changes to IT policy that may impact use at any time and without prior notification.

2. Guiding principles

The use of KPMG IT Resources is governed by the following guiding principles:

2.1.1 Users of KPMG IT Resources must comply with applicable laws, professional standards, contractual requirements, and related KPMG policies and training requirements.

2.1.2 KPMG Personnel accessing the internet while using KPMG IT Resources must not access, download, or disseminate any illegal materials.

2.1.3 KPMG Personnel must, in accordance with relevant policies, take reasonable steps to protect KPMG IT Resources and client information, which may also include personal information covered by privacy laws, that are in their possession or under their control against theft/loss, misuse, damage and destruction. These responsibilities apply equally whether on KPMG premises, in transit, or working at other locations (e.g., at a client site or at home)

2.1.4 KPMG Personnel may not bypass or circumvent information security controls.

2.1.5 KPMG Personnel must have prior authorization before making representations or expressing opinions about KPMG IT Resources that could be construed to be those of KPMG.

2.1.6 In their dealings with others at KPMG, its clients or third parties, KPMG Personnel are prohibited from impersonating any other person, either in person or by using any technology or electronic means.

[1] Including KPMG US Tax Services (London), LLP (USTSL), a Delaware limited liability partnership, and KPMG US Tax Services (Hong Kong) LLC (HTO), a Delaware limited liability corporation, each a sublicensee of KPMG LLP.

2.1.7 KPMG IT Resources are provided to KPMG Personnel for firm business purposes. In this context, something is for “firm business purposes" if it 1) is for the purpose of soliciting business, executing an engagement, or otherwise discusses, relates to, or refers to an engagement or potential engagement, or 2)discusses, relates to, or refers to the operation of the firm, including but not limited to the operation of Business Process Group (BPG) functions.

2.1.8 During litigation, internal investigations, or government, regulatory or administrative inquiries or examinations, the Firm may ask you to provide information (including documents, communications, statements or testimony) or to meet with investigators, our outside counsel, or other parties. The Firm expects its personnel to be candid and cooperative and provide truthful, accurate and complete information in connection with any such request. A failure to cooperate in these circumstances may result in discipline, up to and including the termination of youremployment.

2.1.9 All electronic communications for firm business purposes, as defined above, including those containing Confidential Information, must be made using KPMG-approved electronic communication tools.

KPMG will investigate any violations of this AUP and take disciplinary action, up to and including separation from the firm, as appropriate.

For help, guidance, or clarification on this AUP, please contact the **Policy Office.**

3. Ownership of KPMG IT Resources

3.1.1 Unless explicitly agreed to the contrary and appropriately documented (e.g., in a contract), such KPMG IT Resources remain the property of KPMG. As such, KPMG reserves the right to monitor and review the use of KPMG IT Resources, whether owned or managed (e.g., mobile device management tools installed on personal phones). KPMG Personnel must recognize that KPMG may exercise this right at any time without prior notice. Personal devices or other third-party equipment that may be used to access firm-sponsored Virtual Desktop Infrastructure (VDI) are not considered KPMG IT Resources; however, VDI as a Technology Solution provisioned to KPMG Personnel is considered a KPMG IT Resource.

3.1.2 Upon the termination of partnership/employment (or of a contract), KPMG IT Resources in the possession of or under the control of the affected individual must be promptly returned to KPMG.

3.1.3 Generally, data backed up for business continuity or operational and disaster recovery purposes is to be used for recovery only in the event of a system problem (e.g., systems become inoperable), natural disaster or similar event. Data cannot be recovered for purposes other than business continuity or operational and disaster recovery without prior approvals from the Office of General Counsel (OGC) and Risk Management.

3.1.4 Any transfer of the ownership of **KPMG IT resources** to a third party shall be reviewed by the Risk Management Technology, Data and Operations, the Office of General Counsel (OGC), Enterprise Security Services (ESS), and escalated through established protocols when appropriate. Certain circumstances will also require approval from the associated functional National Managing Partner or delegate. The transfer of IT resources, by license or sale, also needs to be appropriately documented in a written agreement. Also see **RMM 15.4.1- Use and Protection of KPMG IP** .

4. Intended Use of IT Resources

KPMG IT Resources are provided to KPMG Personnel for firm business purposes and shall be used in a manner that complies with applicable laws, professional standards, contractual requirements, and related KPMG policies and limits exposure to information security risk.

4.1.1 KPMG IT Resources are intended for firm business purposes,. Accordingly, the expectation is that KPMG IT Resources are not used for personal activities (e.g., using KPMG email to send or receive personal emails, downloading or using personal software, storing personal files).

4.1.2 KPMG is not responsible for and does not warrant the confidentiality, integrity, or availability of personal files on KPMG IT Resources.

4.1.3 KPMG scans IT Resources and may restrict access to web sites, uninstall personal applications, and remove personal files.

4.1.4 KPMG reserves the right to deploy changes to KPMG IT Resources at any time and without prior notification.

4.1.5 KPMG is not responsible for providing technical support for matters unrelated to KPMG business purposes.

4.2 Use of unapproved third-party equipment or services

KPMG Personnel are only permitted to use **approved** Technology Solutions for firm business purposes. Use of unapproved KPMG IT Resources for firm business purposes is a violation of multiple firm policies and is strictly prohibited. KPMG Personnel who violate this policy by communicating about firm business using unapproved communication methods ("Off-Channel Communications") may become subject to legal obligations to preserve, collect and produce such Off-Channel Communications to regulators, civil litigants and other parties.

KPMG Personnel are also only permitted to use firm-**approved** Technology Solutions on personal mobile devices (e.g., phones and tablets) and **approved** mobile applications to transmit firm-related email and access email contacts, calendar, and work-related documents. The use of texts on a personal device for firm business purposes is prohibited, even if the personal device is enrolled with the firm's Mobility Access Program (MAP).[2] The use of personal email (e.g., a personal Gmail account) and chat/instant message platforms not managed by KPMG (including but not limited to WhatsApp, SnapChat, iMessage, Facebook Messenger, LinkedIn), is prohibited, unless an exception is specifically granted by Risk Management – Technology, Data and Operations (TDO) and the Office of General Counsel (OGC) for LinkedIn. For more information on the use of personal mobile devices, contact the Digital Desk at 1-800-KPMG-HELP. If calling from outside of the United States, please use the direct number to the Digital Desk at 201-505- 6600.

In keeping with this policy, KPMG Personnel are prohibited from purchasing any KPMG IT Resources, including cloud-based services or tools, using a corporate card, personal card, or any other unapproved method.

4.2.1 Third party services must not be used to handle or process KPMG or client information, without explicit approval. Approval requirements and processes are determined by respective functions. Third- party equipment or services may include mobile devices, portable storage media and internet tools and services such as:

[2] KPMG Personnel, such as those working in KPMG Corporate Finance LLC, who are issued firm-owned mobile devices that back up texts to a server may use such text messages for firm business. This does not apply to the vast majority of firm professionals.

- Third-party cloud hosting environments, such as Amazon Web Services, Azure and Google Cloud Platform
- Services or tools located in the cloud, such as Dropbox
- Personal email
- Services such as Siri, Google Translate or Babel Fish
- Unapproved Technology Solutions
- External Generative AI services

4.2.2 KPMG Personnel may not attach any unapproved devices to the KPMG network, with the exception of the KPMG Guest network. The connection of any unapproved device not covered by an existing mobile program or firm-sponsored VDI requires the prior permission of ESS and Risk Management.

4.2.3 KPMG Personnel must consult with **ESS** to identify third-party equipment or services approved for firm business purposes. KPMG reserves the right to perform a "remote wipe" of any mobile device used for firm business purposes and is not responsible for the loss of any personal data stored on the device.

4.2.4 KPMG Personnel must adhere to firm policy on the recording of audio and video communications. KPMG's policy on recording audio and video communications is set forth in the **Recording of Audio and Video Communications** policy statement.

5. Protecting KPMG Technology Assets and Media

5.1 Use of removable media – Encryption and other controls

5.1.1 The firm prohibits the use of removable media (e.g., USBs, CD/DVD, etc.).

5.1.2 Portable electronic devices, including firm endpoints (e.g., laptops, desktops) and mobile devices (e.g., mobile phones, tablets) must be encrypted using firm-approved encryption.

5.1.3 Established encryption measures must not be circumvented or interfered with, except in cases where prior ESS approval has been granted and, in the case of CCI, client consent has been obtained.

5.1.4 Engagement teams must identify any additional client- or industry-specific encryption or security provisions contained in the engagement letter, contract, or Information Protection Plan (IPP). Engagement teams determine if the use of removable media is permitted under the governing engagement letter, contract or IPP.

5.1.5 If clients are using removable media to provide information to engagement teams, they are encouraged to encrypt the information. If clients provide information on unencrypted removable media, teams must immediately transfer the information to secure media (e.g., KPMG laptop or encrypted media), place the unencrypted removable media in a secure location and return the unencrypted removable media to the client as soon as possible.

5.1.6 When removable media is stored with final engagement documentation that is retained in accordance with firm policy, encryption is usually not used, as the removable media is adequately protected within the systems used for these purposes and must be accessible to authorized reviewers. Please refer to the **Removable Media Guide** and **Records Management Enterprise Standard.**

5.2 Protecting KPMG IT Resources

5.2.1 KPMG IT Resources must not be left unattended in any public place at anytime.

5.2.2 Except in rare circumstances, KPMG IT Resources must not be left unattended in any vehicle. In these circumstances, KPMG IT Resources must be stored in a secure section and placed out of sight (e.g., in the trunk of a car, if available). This should be done at the point of origin and not at the destination. Under no circumstances should KPMG IT Resources be left overnight in a vehicle.

5.2.3 KPMG Personnel are required to maintain a "clear desk." This means that when you leave your desk (at a remote location or in an office setting) for an extended period (a half day or longer or overnight), all documents, files, media and portable computing equipment must be cleared and secured in locked drawers or cabinets.

5.2.4 KPMG Personnel must always be aware of the whereabouts of their assigned KPMG IT Resources, whether they are in a KPMG workplace, home office, client site, ortraveling.

5.2.5 KPMG IT Resources, such as laptops, must not be checked as baggage unless mandated by airport security officials. When placed in an overhead compartment (on a plane or train), said compartment containing the KPMG IT Resource should be within sight.

5.2.6 KPMG Personnel must use a privacy filter (or integrated privacy screen capabilities) when using a laptop or other equipment in public places or in circumstances where others might observe the screen.

5.2.7 KPMG Personnel shall follow the firmwide IT shipping procedure when **shipping IT Resources** outside of the United States. Although they are not foreign jurisdictions, this also applies to Puerto Rico and the United States Virgin Islands.

5.2.8 When traveling for both personal and firm business purposes to, through, or within countries defined by Enterprise Security Services as high risk, KPMG Personnel are prohibited from traveling with KPMG IT Resources. This restriction includes any personal mobile device enrolled in the firm's MAP. The list of high-risk countries is updated as necessary by Enterprise Security Services and is available **here** KPMG provides loaner equipment for approved business travel to high-risk countries. Requests for a loaner laptop for personal travel to a high-risk country will be approved if the request complies with the firm's Remote International Worker – Personal Requests policy, found **here.**

For more information, contact the Digital Desk at 1-800-KPMG-HELP. If calling from outside of the United States, please use the direct number to the Digital Desk at 201-505-6600.

5.2.9 KPMG personnel are prohibited from taking KPMG IT Resources to **jurisdictions** **subject to comprehensive sanctions and jurisdictions determined by the Economic Sanctions & Export Control Officer to be subject to strict export controls.** This restriction includes any personal devices enrolled in KPMG's MAP unless MAP software has been removed from the device prior to travel in accordance with firm procedures. Requests for loaner laptops will not be accepted or approved.

5.3 Physically securing KPMG IT Resources

5.3.1 KPMG Personnel are required to keep documents, files, media, and KPMG IT Resourcessecured.

5.3.2 KPMG Personnel must physically secure KPMG-issued computers when in a KPMG workplace, home office, client site, or traveling.

5.3.3 KPMG Personnel must store portable electronic devices out of sight and physically secure such resources before leaving them unattended in a KPMG workplace, home office, or client site, or when

traveling.

Note: It is not appropriate to store KPMG IT Resources in a locked room if anyone else has access to the room.

5.3.4 To protect KPMG IT Resources from unauthorized physical access, KPMG Personnel must display identification badges at all times when working in KPMG workplaces. KPMG Personnel are required to challenge and report individuals not displaying a proper firm identification badge. Lost identification badges should be reported immediately to the Digital Desk at 1-800-KPMG-HELP. If calling from outside of the United States, please use the direct number to the Digital Desk at 201-505-6600.

6. Technology Solutions use

6.1 Approved Technology Solutions

Only KPMG-approved Technology Solutions may be used for firm business purposes in accordance with usage requirements, user guides, and license agreements, as applicable. Technology Solutions must comply with the firm's **Use of Software** requirements. Bots and Robotic Process Automation (RPA) must comply with the firm's **Bot and RPA requirements** .

6.1.1 KPMG-issued computers come with an approved suite of licensed and KPMG proprietary Technology Solutions. KPMG Personnel using KPMG IT Resources are responsible for complying with applicable laws, regulations and license terms that accompany such Technology Solutions, including restrictions on copying or modifying the Technology Solutions or associated documentation.

6.1.2 Approved Technology Solutions and associated documentation may be copied only if it is specifically permitted by the license agreement and with the support of the authorized IT teams. Any Technology Solutions that have been duplicated in violation of a licensing agreement or KPMG policy may not be installed or used. If unauthorized duplication or use of Technology Solutions appears to have occurred, notify the Digital Desk at 1-800-KPMG-HELP. If calling from outside of the United States, please use the direct number to the Digital Desk at 201-505-6600.

6.1.3 Approved Technology Solutions include:

— Technology Solutions, including cloud services, which are approved via the firm standard approval processes for installation and use on a KPMG IT Resource and deployed by KPMG

— Technology Solutions not deployed by KPMG that will be used for firm business purposes, which have been approved via the firm standard approval processes, and do not appear on the **Prohibited Technologies List** .

— KPMG Personnel using KPMG IT Resources with Technology Solutions that were not deployed by KPMG, but have been specifically approved for firm business purposes must also comply with the following:

- Technology Solutions requested and/or provided by clients to carry out services in accordance with engagement contracts must be discontinued and promptly removed at the conclusion of the engagement or when the Technology Solutions are no longer needed to provide services and the affected KPMG IT Resources must be restored to a standard KPMG configuration
- KPMG Personnel using nonstandard Technology Solutions are responsible for obtaining the appropriate licenses for its installation and use and complying with the terms and conditions of the licensing agreement, including any terms regarding copying of the Technology Solutions

6.1.4 All cloud services and subscriptions, including multi-tenancy hosting services that process or store KPMG or **Confidential Information** , must follow firm process and procedures for maintaining cloud

systems inventory, except for:

- Subscriptions utilizing One Platform or purchased through One Platform
- Existing solutions that have completed a formal security riskassessment
- O365 subscriptions managed by ITS Global
- Microsoft Developer Network subscription/licenses

6.1.5 To initiate a review of a new Technology Solution, KPMG Personnel must consult with **ESS.**

6.2 Prohibited Technology Solutions

6.2.1 Technology Solutions prohibited by KPMG must not be installed on KPMG IT Resources. The **Prohibited Technologies Policy** is maintained within the **IT Policy Library** . KPMG Personnel must check the **Prohibited Technologies Policy** prior to requesting, installing and using Technology Solutions on a KPMG workstation. Also see section 6.1.3.

6.2.2 Any Technology Solution included on the **Prohibited Technologies Policy** , or subsequentlyadded to this list, must be promptly removed from KPMG IT Resources.

6.2.3 KPMG must comply with federal restrictions on the use of telecom and other equipment and services by certain companies. Purchase and use of telecommunication equipment or services produced by the following Chinese firms: Huawei Investment & Holding Co., ZTE Corporation, Hytera Communications Corporation Limited, Hangzhou Hikvision Digital Technology Co., and Zhejiang Dahua Technology Co. and any subsidiaries to these firms are prohibited (“Prohibited Equipment or Services”).

These restrictions stem from KPMG’s status as a federal government contractor and are applicable under federal law. These restrictions prohibit KPMG from the delivery or any other use of the Prohibited Equipment and Services and apply not only to KPMG’s federal government engagements, but the firm as a whole, including commercial engagements with non-governmental clients.

Personnel may not:

- Use Prohibited Equipment and Services to access firm-sponsored VDI
- Use subcontractors or other third parties that use Prohibited Equipment and Services or otherwise employ the named Chinese firms or their subsidiaries in connection with their provision of services to KPMG
- Procure Prohibited Equipment or Services directly

Failure to comply may result in a range of penalties levied against KPMG, up to and including debarment from engaging in future contracting activity with the federal government.

6.2.4 KPMG Personnel who are (a)client-facing; (b)charge time directly to a federal client contract or subcontract; and (c)have a personal device which is used in performance of that work in any way (e.g., cell phone calls about Federal clients, KPMG email, etc.), must not have TikTok and other products from its parent company (ByteDance) installed on their personal device enrolledin the Mobility Access Program (MAP). Failure to comply may result in personal financial, legal, or disciplinary ramifications with respect to your employment. Details may be found in the Government TikTok Ban FAQ.

6.2.5 KPMG Personnel should contact the Digital Desk at 1-800-KPMG-HELP for any questions regarding the use of Technology Solutions on KPMG IT Resources. If calling from outside of the United States, please use the direct number to the Digital Desk

at 201-505-6600.

6.3 Use of software

6.3.1 KPMG Personnel must not change or disable any configuration or settings, including, but not limited to, collaboration tools or security-related software that is part of the standard configuration provided by the firm.

6.3.2 The installation of software must follow firm policies and procedures to reduce the likelihood of legal, compliance, and cyber-oriented risks.

6.3.3 The deliberate introduction of any software designed to cause damage to KPMG IT Resources (e.g., viruses, malware) is prohibited.

7. Access to KPMG IT Resources

7.1 Passwords and other credentials

KPMG Personnel access KPMG IT Resources using unique personal credentials. These credentials must be protected and not shared with others.

7.1.1 KPMG Personnel must protect login credentials and the associated passwords, PINs, tokens, and other access devices from disclosure to others and from loss. KPMG Personnel are not allowed to share passwords; if there is suspicion that the password has been compromised, it must be changed immediately, and promptly reported to the Digital Desk at 1-800-KPMG-HELP (1-800-576-4435) or 201-505-6600 if calling from outside of the United States.

7.1.2 Do not use your KPMG login credentials (user ID and password) or a KPMG email address for any other systems, including personal accounts.

7.1.3 KPMG Personnel are personally accountable for activity that occurs using their assigned credentials.

7.1.4 When selecting passwords, KPMG Personnel must create a complex password that meets the minimum requirements as outlined within the **Password** policy statement.

7.1.5 A password-protected screen saver must be activated whenever a KPMG computer is left unattended.

7.1.6 Remote access to KPMG IT Resources is only permitted through KPMG-approved methods.

7.2 Third-party access to KPMG IT Resources

7.2.1 Access to KPMG IT Resources and information assets by third parties is limited by the written authorization provided by appropriately authorized KPMG Personnel and is limited to the duration of the engagement/project. Where client information is accessed, consider if client permission is required.

8. Electronic communications requirements and use of communications tools

All electronic communication must comply with the firm's legal, professional, and quality standards, including communication tools viewed as informal (e.g., instant message, chat rooms, social media groups). This policy protects client and KPMG confidentiality, privacy and personal information and facilitates the proper

retention, protection and use of **Confidential Information** .

Electronic communication without effective controls over development presents a significant risk to KPMG and to the KPMG network. The firm and its personnel must comply with applicable laws, professional standards, contractual requirements, and related KPMG policies and training requirements, including laws and regulations regarding the retention of engagement documentation to address the compliance and risk aspects of data retention across all media.

8.1 Electronic communication requirements

8.1.1 Posting, downloading, or otherwise transmitting messages or information that contain obscene, profane, threatening, harassing (racially, sexually, or otherwise), defamatory, or otherwise offensive language or images are strictly prohibited. Other restrictions include forwarding or circulating electronic communications unrelated to firm business, sending unsolicited commercial, political or religious messaging, and promoting spamming activities.

8.1.2 When communicating electronically, KPMG Personnel must carefully choose the form of communication that is the most suitable and professional for the topic, recipient, or subject matter at hand. KPMG Personnel must be aware that all electronic communications, including those transmitted via third-party cloud applications or personal mobile devices, may become public and reviewed by others and must, therefore, compose all communications accordingly. See **10.5.3 Policy: Engagement Communications within the U.S. Risk Management Manual**

8.1.3 Business-related electronic communication in any form may be treated as records subject to the firm's **Records Management Enterprise Standard** . Formal correspondence that is being sent electronically must comply with the firm's requirements for use of **Email and other electronic communication tools**.

8.2 Approved software for electronic communication

8.2.1 Only KPMG-approved electronic communication tools may be used to conduct firm business. All communication tools will be evaluated, at a minimum, for their ability to:

- Achieve compliance with the duty to maintain the confidentialityof client information
- Conform to data privacy laws and regulations
- Meet KPMG quality and security requirements
- Comply with KPMG's Records Management Enterprise Standard and preservation policies

8.2.2 KPMG Personnel must not use personal email or any personal electronic communication accounts (including texts on a personal device or chat/instant message platforms not managed by KPMG such as WhatsApp, SnapChat, iMessage, Facebook Messenger, LinkedIn, unless an exception is specifically granted by Risk Management-TDO and the OGC for the latter) for firm business purposes. The firm's Talent & Culture professionals are authorized to communicate by text and personal email for limited purposes with firm personnel regarding human resource matters (e.g., in connection with firm disaster/emergency protocols, where necessary to contact firm personnel regarding other exigent human resource matters). In addition to being subject to sanctions, KPMG Personnel who violate this policy by communicating about firm business using unapproved communication methods ("Off-Channel Communications") may become subject to legal obligations to preserve, collect and produce such Off-Channel Communications to regulators, civil litigants and other parties.

8.2.3 KPMG Personnel must understand and remain aware of our professional obligations and firm policies related to confidentiality, retention, and preservation. Confidential or proprietary firm information must only be included in communications with authorized individuals, and only the

amount of **Confidential Information** necessary to achieve our firm business purposes must be shared. KPMG Personnel are required to maintain the confidentiality of client and former client information, as well as information of non-clients that is known to be confidential. Refer to **RMM Chapter 15 – Confidentiality, Privacy, and Information Protection** for additional detail on maintaining confidentiality.

8.2.4 In all electronic communication, the sender must be clearly identified and not bemisrepresented. When an electronic communication is sent on behalf of another, the originator of the communication must be clearly indicated, e.g. “This message is sent on behalf of [name].” In addition, if electronic communications are forwarded or re-sent, their content must not be changed, unless specifically indicated.

8.2.5 KPMG Personnel must remain aware that electronic communications may be forwarded to or intercepted, printed or stored by persons other than the intended recipients. KPMG personnel must remain aware that email and other forms of electronic communication are frequently requested, received, and reviewed by third parties.

8.2.6 KPMG Personnel must use reasonable efforts to verify the accuracy of recipients of electronic communications and avoid sending communications to unintended recipients. Where an electronic communication is known to have been sent to an unintended recipient, contact the Digital Desk for assistance at 1-800-KPMG-HELP.

8.2.7 As directed by the OGC, electronic communication with the OGC or outside counsel must be labeled “Attorney-Client Communication/Privileged and Confidential/Do Not Forward”.

8.3 Use of the internet

8.3.1 When accessing the internet or posting information on the internet using KPMG IT Resources, KPMG Personnel must comply with applicable laws, professional standards, contractual requirements, and related KPMG policies (including the KPMG Code of Conduct, the U.S. Social Media Policy, and other applicable firm policies) and training requirements.

8.3.2 KPMG Personnel may not access the internet using KPMG IT Resources for unapproved or inappropriate uses. Inappropriate use of the Internet, other than when meeting business requirements, is defined as deliberately accessing for the purpose of viewing and/or interacting with:

- Pornographic websites
- Gambling websites
- Websites containing details of or encouraging illegal activities
- Other websites or material that is abusive, sexist, pornographic, racist, offensive, or degrading, or categories of websites that include material that may damage KPMG’s reputation
- Other categories of websites that may present a risk because of a knownthreat

8.3.3 The retrieval of executable files from untrustworthy sources is prohibited. Such action can lead to the introduction of viruses or pirated, unlicensed programs.

8.3.4 DO NOT upload, download, or transmit games, unlicensed software, or offensivematerials.

8.3.5 Even where a particular use of the internet is not expressly prohibited by policy, KPMG Personnel must consider the potential impact to the firm prior to accessing thecontent.

8.3.6 Posting Confidential Information to both personal and professional networks is strictly prohibited. This includes invite-only websites and private forums (e.g., Fishbowl).

8.3.7 The above requirement (8.3.3) does not apply where such access is required in connection with a client engagement, which must be approved in advance by ESS and Risk Management.

8.4 Appropriate use of the KPMG intranet or portal sites

KPMG Personnel accessing KPMG's internal IT Resources (including SaaS resources) must comply with the following:

8.4.1 Comply with all applicable laws, professional standards, contractual requirements, and related KPMG policies and training requirements related to the confidentiality and security of information, personal privacy of other individuals, independence, and professional conduct.

8.4.2 Use KPMG's Intranet Services and the Intellectual Capital contained within for firm business purposes only (e.g., to improve their job knowledge, access business and technical information or other information relevant to their job function).

8.4.3 Protect the Intellectual Capital within KPMG's Intranet Services from loss, misuse, modifications, manipulation, or dissemination to anyone outside of KPMG without proper approval.

8.4.4 Review the accuracy and applicability of content before using it since content on the intranet may not be current, complete, or relevant for the specific situation or reflect competitive practices.

8.4.5 Ensure that copyrighted materials are not reproduced or distributed without proper permission; this includes knowledge KPMG purchased from third parties that is under copyright and/or a license agreement.

8.4.6 Observe any disclaimers or privacy statements displayed when accessing KPMG Intranet Services.

8.5 Email and other electronic communication tools

Only KPMG-approved communication tools may be used for firm business-related communication. The following are examples of communication tools that are not approved for firm business-related communication: texts on a personal device, chat/instant message platforms not managed by KPMG (e.g., WhatsApp, SnapChat) and personal email (e.g., a personal Gmail account). In addition to being subject to sanctions, KPMG Personnel who violate this policy will be required to cooperate with the OGC in the event it needs to preserve, collect, or produce Off-Channel Communications.

8.5.1 Use of the auto address-complete feature in email may result in inadvertently selecting an unintended recipient. KPMG Personnel must take particular care to verify the accuracy of addressees' names and other recipient information before sending any communication.

8.5.2 The KPMG-approved disclaimer and confidentiality notice that is automatically included in outgoing KPMG emails must not be deleted in any work-related email.

8.5.3 KPMG Personnel must not intercept or assist in intercepting any electronic communication processed through the KPMG IT network except as necessary to comply with applicable laws or regulations, to respond to requests from a government authority, or as permitted under firm policy.

8.5.4 KPMG Personnel must verify that email links, files, and other data received through media or email are from legitimate and trusted sources before clicking on or opening them.

8.6 Wireless technologies, including Bluetooth

8.6.1 KPMG Personnel using wireless technologies, including Bluetooth, should consider the following:

- Devices should not be paired in public places in order to not increase the chances of the device paring with different/unknown devices.
- Random connection requests or uninitiated paring requests from other devices should not be accepted in order to prevent the attacker from gaining full access to your device.
- Devices should be checked to ensure that they are set to “non-discoverable” or “hidden” mode when not pairing in order to decrease the exposure to any malicious users scanning for devices with Bluetooth, Airdrop, etc.

9. Client-related requests

9.1 Controls for connecting KPMG IT Resources to client networks

9.1.1 While providing client services, KPMG Personnel may need to connect their KPMG-issued IT Resource or other equipment to a client’s network. KPMG IT Resources (not including VDI on personally owned devices) may only connect to client IT networks when the following requirements have been met:

- Permission of the client in writing (e.g., in the engagement letter)
- Authorization of the engagement or lead partner
- Implementation of any additional information technology controls as defined via the client in writing

Accessing the client’s Guest Wi-Fi does not require written approval.

Additional restrictions may be required for higher-risk services (e.g. cyber penetration testing).

The Engagement Technology Services (ETS) team can assist with meeting these requirements by assessing the business needs, determining what standard technology options are available, and working with appropriate IT teams, including information security, risk, engineering, and architecture. Contact the Digital Desk at 1-800-KPMG-HELP to engage with ETS. If calling from outside of the United States, please use the direct number to the Digital Desk at 201-505-6600.

9.1.2 KPMG computers connected to client IT networks must connect to a KPMG IT network only via approved connections (e.g., KPMG Virtual Private Network [VPN]). For any other type of connection to the KPMG network while connected to a client IT network, client engagement teams need to contact the Digital Desk. The Digital Desk will assign ETS to work with engagement teams on the appropriate solution.

9.2 Approved activity using client networks

9.2.1 KPMG Personnel may only access a client network in accordance with client contractual agreements.

9.2.2 Client networks may only be accessed using individually assigned credentials issued by the client. In no circumstances should KPMG Personnel share credentials with others unless directed to do so by the client in writing.

9.2.3 No client materials may be accessed, downloaded, transmitted, or stored other than as explicitly agreed to with the client in writing.

9.3 Client-related software requests

There may be times when teams are asked to use client-licensed technology for an engagement. Use of technology solutions as directed and provided by a client is permissible under the following conditions:

9.3.1 Requests to use and/or install unapproved software must be submitted for approval in accordance with RMM US 14.4 New and Modified Products and Solutions. An Exception Request to use and/or install software on the Prohibited Technologies list must be submitted through CORE. Unapproved or Prohibited software must not be used until approved or an exception is granted.

9.3.2 Written requests from the client, along with confirmation from the engagement lead that the proper terms and conditions are documented with the client, must be documented in the engagement workpapers.

9.3.3 The risks associated with the request should be identified and the decision made as to how these risks will be mitigated. This should be documented in the engagement letter and understood by both KPMG and the client.

9.4 Responding to client inquiries

9.4.1 KPMG Personnel must direct any client inquiries regarding KPMG's IT security policies and practices, such as questionnaires, to the ESS team by initiating a **Client Security Inquiry (CSI) request** . Alternatively, KPMG Personnel can open CSI requests online at **CORE** by searching for "CSI" or by calling the Digital Desk at 1-800-KPMG-HELP and selecting option 1 followed by option 3. An ESS representative will contact the requestor to gather any necessary additional information and establish a timeline to respond to the client. If calling from outside of the United States, please use the direct number to the Digital Desk at 201-505-6600.

9.4.2 Client engagement teams must confer with ESS before discussing with the client the expected timeline or the extent of detail that may be provided in the response.

10. Information and Cybersecurity Incident reporting

10.1 Reporting Information and Cybersecurity Incidents

10.1.1 KPMG Personnel must promptly report potential Incidents (defined below), whether suspected or confirmed, to the Digital Desk at 1-800-KPMG-HELP. If calling from outside of the United States, please use the direct number to the Digital Desk at 201-505-6600.

10.1.2 There are two types of incidents for the purposes of this policy: Information Incidents and Cybersecurity Incidents (collectively, "Incidents").

- An "Information Incident" is defined as:

(i) the firm's known or reasonably suspected (a) loss, theft, or destruction of, (b) unauthorized transfer, disclosure, use, or modification, or (c) unauthorized access to any

CCI, FCI, and/or non-public Third Party Content (TPC) in any event whether intentional or unintentional; or

(ii) the firm's receipt of any:

(a) Personally Identifiable Information (PII), Protected Health Information(PHI), CCI-Export Controlled Information, and/or CCI-Federal Contract Information as defined in **RMM Chapter 15 – Confidentiality, Privacy, and Information Protection** and/or

(b) Material non-public information (MNPI) of any party (e.g., a non-public draft of an SEC filing; non-public information regarding a proposed merger, acquisition, or other strategic transaction),

if such receipt is unauthorized or the information is not reasonably needed for the firm's provision of services to a client or for other legitimate firm business purposes, including the firm's receipt of such information due to the intentional or unintentional transfer, disclosure, use, or modification of the information by a client and/or third party.

The information may be in hard copy or electronic form. An Information Incident may include, but is not limited to, the loss or theft of any equipment or device containing CCI or FCI, the emailing of CCI or FCI to a personal or unauthorized email address, the unauthorized uploading of CCI or FCI to a third-party cloud hosting environment or service, a misdirected email containing CCI or FCI, or a party's qualifying "spill-in" of information pursuant to clause (ii) above.

- A "Cybersecurity Incident" is defined as a malicious activity or a violation or imminent threat[3] of violation of firm IT security policies or AUP with respect to the confidentiality, integrity, or availability of KPMG IT Resources. A Cybersecurity Incident may include, but is not limited to, social engineering, denial of service, exploits of vulnerabilities, introduction of malware or any activity that may affect the confidentiality, availability or integrity of KPMG IT Resources or **Confidential Information** as set forth in **RMM Chapter 15 – Confidentiality, Privacy, and Information Protection** .
- An Information Incident may also constitute a Cybersecurity Incident and vice versa. An Information Incident or a Cybersecurity Incident may constitute a Major Incident (as defined below).
- A "Major Incident" is defined as an Information Incident or Cybersecurity Incident in which the potential impact of the Incident on our clients or the firm is major. The classification of "major" is attributed based upon the Incident's potential impact (e.g., the number of clients or personnel affected, the ability of KPMG to continue to operate, brand reputation, media coverage) and is ultimately determined by the Incident Response Team (IRT), a cross-functional group with representatives from ESS, Risk Management, and the OGC, in consultation with firm leadership.

10.1.3 KPMG Personnel must comply promptly with any requests by the firm's IRT regarding the incident and cooperate fully in the investigation and resolution of the incident.

Additional detail on the firm's Incident Management policy and procedures can be found by clicking the following **link** .

[3] An "imminent threat of violation" refers to a situation in which an individual has a factual basis for believing that a specific violation is about to occur. For example, a threat to KPMG is posted on the internet or there is awareness of new malware that is rapidly spreading across the internet.

11. Monitoring and enforcement

11.1.1 Access to KPMG's IT Resources is subject to review and restriction by KPMG at any time and without notice, subject to and in accordance with applicable laws, professional standards, contractual requirements, and related KPMG policies.

11.1.2 KPMG also reserves the right to monitor activities performed with KPMG IT Resources, whether use is at KPMG workplaces or outside of KPMG workplaces, such as at a client site. Monitoring includes, but is not limited to, using physical or electronic searches or security or related surveillance equipment, to the extent permitted by applicable law. As such, KPMG Personnel have no expectation of privacy in any such communications or information when using any KPMG IT Resources or when in KPMG's workplaces.

11.1.3 KPMG reserves the right to monitor and remove any Technology Solutions, files, or information on any KPMG IT Resource as considered necessary to obtain ongoing compliance with KPMG policies, applicable laws, professional standards, and contractual requirements. Such review may be conducted by, and at the behest of, KPMG and third parties authorized by KPMG. KPMG Personnel are required to cooperate fully in any such activity.

11.1.4 KPMG reserves the right to collect, inspect, and/or image personal devices in accordance with firm procedures, to the extent certain data contained therein is deemed necessary for the purpose of litigation, investigations, and/or complying with regulatory obligations. To the extent legally permissible, KPMG shall (i) document the purpose for processing data extracted from Personnel's personal devices and (ii) provide the impacted Personnel with information regarding the processing, retention and deletion of the data.

11.1.5 Personnel who fail to comply with section 11.1.4 are subject to the firm's **disciplinary process** , which may include separation from the firm and/or termination of a contract.

12. Retired partner and expatriate access to KPMG IT Resources

12.1.1 If a retired partner requires access to the KPMG network for 30 or less days after their date of retirement, Partner Services (Talent and Culture) approval is required, and the retired partner must be in good standing before they can gain access to the KPMG network. This excludes circumstances when a retired partner is returning to the firm as an employee.

12.1.2 Retired partners transitioning to a contingent worker are required to return existing KPMG IT Resources before the transition; however, if the retiring partner requests the retention of data, approval from the OGC's Electronic Data Discovery must be obtained prior to the transition. Once approval has been obtained, the data from the existing KPMG IT Resources is migrated to new KPMG IT Resources and the hard drives from the original KPMG IT Resources are provided to the OGC for preservation.

12.1.3 Retired partners that return to the firm as a contingent worker must adhere to the requirements outlined in the **Third Party Decision Framework** .

12.1.4 Expatriates are required to return existing KPMG IT Resources to the local Digital Nexus representative prior to going on rotation.

12.1.5 Expatriates who require the use of KPMG U.S. configured KPMG IT Resources when joining another member firm must return existing KPMG IT Resources to the local Digital Nexus representative. New KPMG IT Resources will be issued by the member firm.

Document review and approval

Revision history[4]			
Version	**Author**	**Date**	**Key Revisions**
5.3	Risk Management – Policy Office	March 2023	— Added clarification that personnel must comply with investigations into business-related communications on personal devices — Added clarification regardingoff-channel communications — MAP software must be removed from personal devices prior to personaltravel to high-risk countries — Corrected URLs as needed — Addition of content from US – RMM Chapter 17 around ownership of IT resources
5.4	Risk Management – Policy Office	September 2023	— The definition of "firm business purposes" has been added — Clarified language around shipment ofIT Resources — Clarified language around travel to high-risk countries with IT Resources — Updated monitoring and enforcement language for IT Resources and personal devices
5.5	Risk Management – Policy Office	July 2024	— Clarified that use of personal email is prohibited unless a specific exemption has been granted — Clarified language around the use of third-party equipment and services — Updated Third party services to include external generative AI — Clarified language around client-related software requests

This document has been reviewed by:		
Version	**Reviewer**	**Date reviewed**
5.3	IT policy review board members, Office of General Counsel (OGC)	March 2023
5.3	Robyn Brown (Senior Director, Risk Management – Policy Office)	March 2023
5.3	Allison Kasson (Partner, Risk Management – Policy Office)	March 2023

5.4	IT policy review board members, Office of General Counsel (OGC)	September 2023
5.4	Alicia Fortunato (Director, Risk Management – Policy Office)	September 2023
5.4	Allison Kasson (Partner, Risk Management – Policy Office)	September 2023
5.5	Allison Kasson (Partner, Risk Management – Policy Office)	July 2024

This document has been approved by:		
Version	**Name**	**Date reviewed**
5.3	Allison Kasson (Partner, Risk Management – Policy Office)	March 2023
5.4	Allison Kasson (Partner, Risk Management – Policy Office)	September 2023
5.5	Allison Kasson (Partner, Risk Management – Policy Office)	July 2024

[4] The full revision, review and approval history is maintained by the Policy Office and is available for review upon request.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.
kpmg.com/socialmedia

What you need to know aboutusing personal devices for firm business purposes

Using your personal mobile device to conduct firm business is convenient and efficient – but can pose risks that you should be aware of.

Learn how to properly use your personal device for firm business purposes.

1. Can I use my personal device to conduct firm business?

Yes, KPMG Personnel may use their personal devices to communicate for firm business purposes as long as the device is enrolled in the Mobility Access Program (MAP) and the communication is made using approved Technology Solutions. Examples of approved Technology Solutions include Microsoft Outlook, Microsoft Teams, Sharepoint, and other tools available through the Company Portal.

Using chat/instant message platforms and personal email (e.g., a personal Gmail account) not managed by KPMG to communicate for firm business purposes is prohibited, even if the personal device is enrolled in the MAP. Examples of prohibited messaging platforms include WhatsApp, SnapChat, iMessage, and Facebook Messenger. These are considered "off-channel communications." While LinkedIn is permitted for personal networking purposes, it may only be used for firm business purposes if an exception is specifically granted by Risk Management – Technology, Data and Operations (TDO) and OGC.

2. What are considered firm business purposes?

Something is for "firm business purposes" if it 1) is for the purpose of soliciting business, executing an engagement, or otherwise discusses, relates to, or refers to an engagement or potential engagement, or 2)discusses, relates to, or refers to the operation of the firm, including but not limited to the operation of Business Process Group (BPG) functions. Posts that are promoted on the **KPMG Social Share** social media enablement platform that allows KPMG partners and professionals to share appropriate content through their own social media networks may be shared to a personal LinkedIn profile in accordance with the U.S. Social Media Policy.

3. Does being enrolled in Mobility Access Program (MAP) mean I can use any application on my phone for firm business purposes?

Professionals should be aware that while your personal device may be enrolled in MAP, only firm-approved Technology Solutions available through the Company Portal can be used for firm business purposes on personal devices. Applications that were either pre-installed on your personal device or installed by you outside of the firm's technology provisioning process should not be used for firm business purposes.

4. What am I allowed to use on my personal device to conduct firm business?

Only firm-approved Technology Solutions available through the Company Portal may be used on a personal device for firm business purposes. Examples of off-channel communications on a personal device like an iPhone or Android (whether enrolled in the MAP or not) would be messages sent or received for business purposes through the native Messages app, Facebook Messenger, WhatsApp, etc.

In short, don't send any firm business-related correspondence using Technology Solutions not approved or provisioned by the firm.

5. Is the firm allowed to send me announcements and firmwide message to my personal messaging app?

Yes. Firm and practice leadership may need to reach you for important matters like technology outages, office closings, National Check-In requests, and other important firm announcements. Such communications and announcements are permitted to be sent to your personal messaging app, such as iMessage, and personal email.

6. Can I text my coworker about lunch plans or let them know I'm running late?

It depends. As a professional, you are expected to exercise sound judgment and discretion in all communications with KPMG Personnel and clients. Assuming the off-channel communications do not include content relating to firm business purposes as described above, including client engagements, or other Confidential Information, then casual messages that are not material to the conduct of firm business are permitted.

7. Will my personal device be subject to inspection if I use unapproved Technology Solutions or off-channel communications?

Yes. If communications using unapproved Technology Solutions or off-channel communication methods are deemed necessary for the purpose of litigation, internal investigations, or government, regulatory or administrative inquiries or examinations, the firm reserves the right to collect, inspect, and/or image your personal device in accordance with documented firm procedures.

8. What if someone else sends something related to firm business to my personal iMessaging app or personal email?

Should you receive a communication regarding firm business via an unapproved Technology Solution, you should tell the sender to contact you through approved communications channels, or you may respond using an approved Technology Solution.

9. What is the process if my personal device is requested for investigation?

In the event that your personal device needs to be accessed and/or inspected, you will be notified by a representative from the OGC with instructions on how to comply. This notification will include relevant details, including appropriate information regarding the investigations process.

10. How is the firm protecting my personal data if I'm asked to provide my personal device?

In the event the firm needs to collect, inspect, or image your personal device, all contents of the device will be imaged and stored on an encrypted drive with controlled access. In accordance with firm procedures, only relevant data will be identified and used. The contents of the drive will be deleted once there is no longer a legal obligation to preserve it.

Virtual Desktop Infrastructure (VDI) User Notice and Acknowledgement

Please review the information below carefully.

KPMG offers the option to use a “virtual desktop infrastructure,” or VDI, to remotely access KPMG applications during your assignment. VDI environments can be provisioned more quickly so that you can be set up and billable in a short time period (subject to the start date and other terms of your assignment). You can access the VDI from PC or Mac computers.

By submitting your confirmed response, you acknowledge the following terms and conditions below, which govern your use of VDI:

- You may use the VDI only in connection with your assignment, and all use must be in accordance with the terms of the agreement(s) governing your services to KPMG. These may include, but are not limited to:
  - your agreement to follow the KPMG Acceptable Use Policy provided as part of the onboarding process; and
  - other instructions from your engagement manager regarding document preservation, export controls, or other topics.
- Access to the VDI does not constitute authorization to process any data subject to NIST compliance or to store any data on your machine.
- The VDI should not be accessed from a KPMG client site on any device that has not been issued to you by KPMG unless specifically authorized by KPMG in writing.

Non-compliance may result in the termination of your contract and other ramifications. For any additional questions please contact our US-FM HR SC CW Support <us-hrsccwsupport@KPMG.com> mailbox.

If you do not or cannot confirm the above, please respond to our US-FM HR SC CW Support <us-hrsccwsupport@KPMG.com> mailbox and request cancellation of the VDI provisioning request.

I acknowledge that I have fully read, understand, and affirm my agreement to comply with the Policy.

Ajinkya Nimbhorkar
Print Name

Signature

Date

Sexual and Other Harassment Policy Acknowledgement

Instructions: Please read the following KPMG policy and sign below to acknowledge your receipt and understanding of the policy. Please print and retain a copy for your files.

Sexual and Other Harassment Policy for KPMG Contingent Workers

It is KPMG's policy to maintain a work environment that is free of sexual or other unlawful harassment of its contingent workers, whether by employees, partners, other contingent workers, clients, customers, vendors, or anyone else who conducts business with the firm.

Examples of Sexual and Other Harassment include:

- Unwelcome or unwanted sexual advances, including patting, brushing up against, hugging, cornering, kissing, or any other offensive sexually oriented conduct.
- Requests or demands for sexual favors, including subtle or blatant expectations, pressures, or requests.
- Verbal abuse, teasing or joking that is sexually oriented and may be considered offensive by another person.
- Physical, verbal, or nonverbal behavior that harasses or interferes with a contingent worker's work performance or creates or contributes to an intimidating, hostile, or offensive work environment. This includes slurs, off-color jokes, threats, or posters, cartoons, e-mails, or drawings that are insulting, degrading or that ridicule one based on his or her protected status.

Procedure for Reporting a Complaint

For the firm to effectively implement this policy, all individuals are expected to report behavior that they believe may violate this policy. Cooperation in preventing this type of conduct is essential. Any contingent worker who believes that he or she has been subjected to inappropriate sexual or other behavior that they believe is harassing is encouraged to tell the offender that his or her behavior is offensive and should be stopped. If such a direct approach does not work or is impractical under the circumstances, or if any contingent worker has reason to believe that another contingent worker or any employee of the firm has been subjected to or has engaged in behavior that may violate this policy, the contingent worker is expected to inform by contacting the Ethics and Compliance Hotline at (877)-576-4033 or EthicsPoint - KPMG LLP and to state the specifics of the allegations.

KPMG will investigate any complaint or report of inappropriate behavior. All reports are handled confidentially, although we may need to disclose facts as required by law, or to fully investigate and address concerns.

Anyone who violates our policies, regardless of title or tenure, may be subject to discipline, up to and including termination of assignment or employment and partner separation

Sexual and Other Harassment Policy Acknowledgement

Preventing Retaliation

KPMG prohibits retaliation against anyone who, in good faith, reports a concern or participates in an investigation, even if the allegation is not substantiated. Every contingent worker is encouraged to come forward without fear of retaliation. Any contingent worker who believes that he or she has been or may be subjected to retaliation should direct those complaints to the Ethics & Compliance Hotline (877)-576-4033 or EthicsPoint - KPMG LLP .

I acknowledge that I have fully read, understand, and affirm my agreement to comply with the Sexual and Other Harassment Policy for KPMG Contingent Workers.

Ajinkya Nimbhorkar
Print Name

Signature

Date

Firm Personnel Data Privacy Notice

KPMG LLP[1] (“**KPMG**”) is dedicated to protecting the confidentiality and privacy of information entrusted to it, including Personal Information (also known as “personal data,” “Personally Identifiable Information,” or “PII”). This Firm Personnel Data Privacy Notice (“**Data Privacy Notice**”) aims to give Firm Personnel (as defined below) information on how their Personal Information (as defined below) is collected, processed, used, and retained by KPMG. For the purposes of this Data Privacy Notice: (i) “**Firm Personnel**” includes current and former partners, principals, employees, directors, officers, interns, and Third Party Personnel[1] of KPMG; and (ii) “**Personal Information**” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Firm Personnel, or a particular household that Firm Personnel is a member of. Please review this Data Privacy Notice to learn about how we collect, use, share, and protect Firm Personnel’s Personal Information.

Collection and Use of Personal Information

KPMG’s collection of Personal Information from and about Firm Personnel is necessary in order for KPMG to fulfill its legal, professional, and contractual obligations, and for the performance of current and former partnership or employment relationships, as applicable. Therefore, the failure by any Firm Personnel to provide Personal Information, in whole or in part, could prevent KPMG from fulfilling some or all of its obligations regarding the partnership or employment relationship, or as may be required under contract, applicable law, or our professional standards, including, but not limited to, obligations related to auditor independence rules, payroll, social security contribution, tax, and insurance.

KPMG may process the following types of Personal Information, including Sensitive Personal Information (as defined below), for the purposes set out in this Data Privacy Notice, and subject to and in accordance with applicable law:

- *Identifiers*, which may include: your name, address, e-mail address, phone number, and other contact details; usernames and passwords; social security number and national identity number, driver’s license number, passport number, or other government-issued identification number;
- *Commercial and financial information, which may include: your bank account information and other information relating to your financial institution; credit applications, credit checks, and information from credit reporting agencies; and brokerage account information;*
- *Professional or employment-related information, which may include: information regarding your current and previous employers; job title and responsibilities; assets; income; and/or other information related to your work history and/or prospective employment; compensation, bonus or incentive information and social security premiums (including amounts paid, the frequency and currency of payments); benefits information (e.g., car allowance, health insurance, pension contributions) (including amounts paid, the frequency and currency of payments); records of your work history (including internal and external work history, references, and civil and criminal background checks); participation on corporate boards or advisory councils; records of your performance (including evaluations and ratings, grievances, and disciplinary records); information relating to absences from work; general organizational data (such as your department, work location, job title, and seniority);*
- *Education information, which may include: academic records, degrees, and educational history;*
- *Biometric information, which may include: signatures; fingerprints; facial scans, voice recognition information, genetic information, and/or other similar biometric identifiers;*
- *Information relating to Internet activity or other electronic network, application, and systems activity, which may include: cookie identifiers, clear gifs, browser type, Internet service provider (ISP), Internet Protocol (IP) addresses, media access control (MAC) addresses, referring/exit pages, operating system, date/time stamp, clickstream data, device platform, device version, and/or other device*

Firm Personnel Data Privacy Notice

characteristics including your choice of settings such as Wi-Fi, Bluetooth, and Global Positioning System (GPS) data; usage data; and other, similar Personal Information collected for monitoring purposes, or other purposes pursuant to any KPMG policy, in relation to your interaction with KPMG's networks, applications, and systems, including badge swipes to KPMG's workplaces, hoteling, training, messaging and calendaring, mobile device management, and remote access;

- *Geolocation data, which may include GPS data, locational information based upon your IP address, cell network data, and/or other similar locational data;*
- *Audio, electronic, or visual information, which may include records of calls to or from our service or support centers; and/or audio or video information recorded for surveillance or training purposes, during meetings (virtual or in person), or at firm events/town halls;*
- *Information not listed above and related to characteristics protected under applicable state or federal law, which may include gender, race and ethnicity, nationality, marital status, disability, military service or veteran status, and/or date of birth;*
- *Inferences about you, which may include preferences and characteristics and other information we may infer from other Personal Information we have collected;*
- *Other Personal Information not listed above and defined in applicable law(s), which may include insurance policy number; bank account number, credit card number, debit card number, and other financial information; and health or medical information and health insurance information; and*
- *Other information voluntarily disclosed by you to us, or collected or generated by KPMG in connection with your partnership or employment relationship or the related activities in which you participate on account of your relationship with KPMG.*

KPMG may process Sensitive Personal Information (as defined below) if and to the extent such processing is: (i) necessary for compliance with applicable law; (ii) specifically authorized or required by law; or (iii) of Sensitive Personal Information that is voluntarily shared by any Firm Personnel with KPMG. What constitutes Sensitive Personal Information may vary by law, but for the purposes of this Data Privacy Notice, "Sensitive Personal Information" is Personal Information is that may reveal an individual's person's race, ethnicity, political beliefs, trade union membership, religious or similar beliefs, physical or mental health, biometrics, precise geolocation, sexual orientation or criminal record.

We may create de-identified or anonymized data from Personal Information by removing data components that make the data personally identifiable to you, or through obfuscation or other means. Our use of de-identified or anonymized data is not subject to this Data Privacy Notice

Collection and Use of Personal Information of Family Members of Firm Personnel

KPMG may also collect certain information from or regarding the spouses, partners, dependents, and other household members of Firm Personnel, excluding Third Party Personnel ("Family Members"), such as emergency contact details and contact information and information in connection with the administration of health, medical, or other employment benefits. In addition, to comply with federal law, regulations, and professional standards, KPMG is required to collect certain information from or regarding Family Members of Firm Personnel, including certain financial information, such as brokerage account information, and certain Personal Information that we require to fulfill our obligations under applicable professional standards and laws, including, without limitation, auditor independence rules. KPMG's collection and processing of Personal Information of Family Members of Firm Personnel is subject to KPMG's external Privacy Statement .

Firm Personnel Data Privacy Notice

Purposes of Processing Personal Information

- Personal Information may be processed by KPMG for the purposes set out below:
- Managing the recruitment, onboarding, and retention of Firm Personnel;
- Administering human resource functions, including performance reviews and appraisals, personal time off, including, without limitation, sickness leave, training, internal directories and organizational charts, internal communications, professional development and continuing education tracking, social and cultural activities directly implemented by KPMG and dealing with disciplinary action, termination, and retirement of Firm Personnel;
- Planning and staffing client engagements, including, without limitation, providing resumes and descriptions of work experience and qualifications to clients and potential clients;
- Administering payroll, or partner drawing accounts and partner statements, the reimbursement of expenses, the payment of remuneration and other benefits of Firm Personnel, such as bonuses, car allowances, the booking of a flight or hotel room, loans, pensions, health insurance, life insurance, travel insurance, death-in-service benefits, and disability plans;
- Communicating with Firm Personnel and emergency contacts;
- Authorizing, granting, and administering access to or use of any KPMG IT Resources (including firm-issued laptops, firm-managed personal devices, and e-mail accounts), workplaces (including offices and facilities), and firm records;
- Health, safety, and wellness of our workplace and workforce;
- Investigating and resolving complaints, grievances, or misconduct;
- Preparing for and acting in relation to inquiries, investigations, or proceedings by governmental, administrative, judicial, or regulatory authorities or third parties, including civil litigation;
- Audit purposes and complying with policy, procedures, laws, regulations, and professional standards, including performing checks for auditor independence purposes;
- Monitoring Firm Personnel pursuant to our policies and applicable law, including those policies set forth in the Policy Center and the Acceptable Use Policy;
- Improving the delivery or quality of services or technology for KPMG and its clients (through the use of artificial intelligence, machine learning, internal analytics, and benchmarking related to those services or technology);
- Alumni updates and post-employment engagement; and
- Any other purposes relating to the above.

Sharing and Transfer of Personal Information

We do not share Personal Information with unaffiliated third parties, except as stated in this Data Privacy Notice, including as necessary for our legitimate professional and business needs, to carry out your requests, to market our services, and/or as required or permitted by law or professional standards, or otherwise with your consent.

In some instances, KPMG may share Personal Information about you with various third-party service providers working on our behalf, or to help fulfill your requests. These third parties include, for example, providers of administrative, identity management, website hosting, data analysis, data back-up, and security management services. Third parties receiving Personal Information from KPMG are obligated to protect Personal Information in accordance with their contractual obligations and data protection legislation applicable to their provision of services.

Firm Personnel Data Privacy Notice

Our service providers also may use aggregated, deidentified or anonymized data for improving the delivery or quality of services or technology, among other lawful uses and for research and development. As set forth above, de-identified or anonymized data does not identify you individually but rather helps to identify trends in preferences and behaviors of Firm Personnel at an aggregate level.

KPMG may disclose Personal Information to address or respond to requests of, or guidance provided by, government entities, bodies, or agencies, law enforcement agencies, or other entities or organizations, such as public health agencies, authorized by, or otherwise acting or operating pursuant to the lawful direction or authority of, an international, federal, state, or local governmental body, including to meet national security or law enforcement requirements and for health and safety purposes. We may also disclose Personal Information where disclosure is required by applicable laws, court orders, government regulations, or other legal process, or where we believe disclosure is necessary or appropriate to protect the rights or safety of KPMG, Firm Personnel, or other third parties.

In the event that the ownership of KPMG or an affiliate or their assets changes as the result of a merger, acquisition, or sale of assets, information owned or controlled by KPMG may be transferred to another company. Information may also be shared in connection with the consideration, negotiation, or completion of a corporate transaction in which we are acquired by or merged with another company, or we sell, liquidate, assign or transfer all or a portion of our assets. If any such transaction occurs, the purchaser will be entitled to use and disclose the Personal Information collected by KPMG in the same manner that we are able to, and the purchaser will assume the rights and obligations regarding Personal Information as described in this Data Privacy Notice.

KPMG may also need to disclose certain Personal Information in connection with audits and/or to investigate or respond to a complaint or security threat.

KPMG neither sells Firm Personnel's Personal Information to any third parties nor shares Firm Personnel's Personal Information with any third parties for cross-context behavioral advertising.

Further, Personal Information may be disclosed to the extent necessary for the purposes described in this Notice to the following recipients:

- Departments within KPMG, including, Talent & Culture, Finance & Accounting, Digital Nexus, Risk Management, and Legal, Regulatory & Compliance, among others;
- Financial institutions, pension plan institutions, insurance companies, consultants, and professional advisors;
- Other service providers, such as payroll administrators, benefits providers and administrators, and information technology systems providers involved in the provision of services to KPMG and/or Firm Personnel;
- Independent public accountants and auditors, authorized representatives of internal control functions, such as audit, legal, and/or firm-wide security;
- KPMG International or other member firms affiliated with KPMG International; and
- Applicable tax authorities

Firm Personnel Data Privacy Notice

Cross-Border Collection and Transfer

We may collect Personal Information from or about you if you are in a jurisdiction other than the U.S. for purposes of your employment or relationship with KPMG. Similarly, if you are in the U.S., we may transfer outside of the U.S. the Personal Information we collect from or about you. Regardless of where you are located, we may transfer certain Personal Information across geographical borders to KPMG International, other member firms affiliated with KPMG International or to various third-party providers working on our behalf, or we may receive Personal Information in the U.S. or elsewhere transferred from KPMG International, another member firm affiliated with KPMG International or an unaffiliated third party. KPMG may also store Personal Information in a jurisdiction other than where you are based, and such jurisdiction may not provide the same level of protection for your Personal Information as your home country. By providing your Personal Information to KPMG, you understand that your Personal Information may be collected, transferred and/or stored in a jurisdiction other than your home country. Each member firm affiliated with KPMG International is required to safeguard Personal Information in accordance with its contractual obligations and data protection legislation applicable to its provision of services. Your Personal Information will only be transferred if appropriate or suitable safeguards are in place

Data Privacy Framework

The following provisions in this section apply only to Firm Personnel who are residents of European Economic Area member countries and the United Kingdom.

KPMG complies with the EU-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. Data Privacy Framework as set forth by the U.S. Department of Commerce. KPMG has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles ("EU-U.S. DPF Principles") with regards to the processing of Personal Information received from the European Union in reliance on the EU-U.S. If there is any conflict between the terms in this Data Privacy Notice and the EU-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework ("DPF") program, and to view our certification page, please visit https://www.dataprivacyframework.gov .

For more details, please review the KPMG LLP Data Privacy Framework Policy , which applies to Personal Information transferred from member countries of the European Economic Area and the United Kingdom (including Gibraltar), pursuant to the DPF.

The Federal Trade Commission has jurisdiction over KPMG's compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. In compliance with the DPF, KPMG commits to resolve EU-U.S. DPF Principles-related complaints about our collection and use of your Personal Information. EEA or UK individuals with inquires or complaints regarding our handling of Firm Personnel's Personal Information received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, should first contact Talent & Culture by e-mailing us-hrprivacy@kpmg.com. Third Party Personnel may address questions by first contacting the Contingent Workforce Center of Excellence at us-hrsccwsupport@kpmg.com.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, KPMG commits to refer unresolved complaints concerning our handling of Personal Information received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF to the BBB NATIONAL PROGRAMS, an independent, alternative dispute resolution provider based in the U.S. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit www.bbbprograms.org/dpf-complaints information or to file a complaint. The services of BBB NATIONAL PROGRAMS are provided at no cost to you.

Firm Personnel Data Privacy Notice

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, KPMG further commits to cooperate and comply (respectively) with the advice of the panel established by the EU data protection authorities ("**DPAs**"), the UK Information Commissioner's Office (**"ICO**"), and the Gibraltar Regulatory Authority ("**GRA**"), with regard to unresolved complaints concerning our handling of Firm Personnel's Personal Information received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF in the context of the employment relationship. If your DPF complaint cannot be resolved through the above channels, under certain conditions, you may be able to invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See https://www.dataprivacyframework.gov/s/a for further information.

Rights of Firm Personnel

It is the responsibility of all Firm Personnel to provide the Talent and Culture Department with accurate Personal Information. If you have provided Personal Information to KPMG, under most circumstances, subject to applicable law, you have the right to reasonable access to that Personal Information to correct any inaccuracies. You can also make a request to update or remove Personal Information about you, and we will make all reasonable and practical efforts to comply with your request, so long as it is consistent with applicable law and professional standards.

Furthermore, the firm will retain Personal Information subject to any record retention requirements set forth in the Enterprise Retention Schedule and the U.S. Risk Management Manual. Your Personal Information may also be subject to preservation requirements and in accordance with the firm's Preservation Guidelines.

To make a Data Privacy Request, please contact us by:

- Submitting a Data Privacy Request through our webform; or
- E-mailing us-privacy@kpmg.com

In addition, you may make corrections to certain Personal Information that you provide to the firm via Self Service Connection.

Rights of Firm Personnel Residing in California

The California Consumer Privacy Act, as amended and including its regulations, ("**CCPA**"), grants rights to Firm Personnel, who are California residents, with regard to their Personal Information. If you are a California resident, the following explains your CCPA rights and our Personal Information practices as applicable.

For purposes of the CCPA, "Personal Information", "Sensitive Personal Information", and other terms below have the meaning defined in the CCPA.

Our Personal Information collection practices, including during the preceding 12 months, are identified above.

If you are a California resident, you have the right to request the following:

- The categories of Personal Information we collected about you in the last 12 months;
- The categories of sources from which that Personal Information was collected in the last 12 months;
- Our business or commercial purpose for collecting or selling or sharing (as such terms are defined under the CCPA) that Personal Information in the last 12 months;
- The categories of third parties with whom we shared that Personal Information in the last 12 months;

Firm Personnel Data Privacy Notice

- The categories of that Personal Information we sold or shared for cross-context behavioral advertising in the last 12 months;
- The categories of third parties to whom we sold that Personal Information in the last 12 months;
- The categories of Personal Information we disclosed for a business purpose in the last 12 months;
- The categories of third parties to whom we disclosed that Personal Information for a business purpose in the last 12 months;
- The specific pieces of your Personal Information we collected in the last 12 months;
- The correction of Personal Information that we maintain about you,
- The deletion of Personal Information that we have collected from you;
- To limit or restrict the use of your Sensitive Personal Information; and
- To opt-out (or opt-in for children under 16) to the sale or sharing of your Personal Information.

To exercise any of your rights, please contact us by:

- Submitting a Data Privacy Request through our webform; or
- E-mailing us-privacy@kpmg.com

In addition, you may make corrections to certain Personal Information that you provide to the firm via Self Service Connection.

We will respond to authorized and verified requests as soon as practicable and as required by law, including any reason for denying or restricting a request. The above rights are subject to various exclusions and exceptions under firm policies and applicable laws (including professional standards), and under certain circumstances we may be unable to fulfill your request. The firm will retain Personal Information subject to any record retention requirements set forth in the Enterprise Retention Schedule and the U.S. Risk Management Manual. Your Personal Information may also be subject to preservation requirements and in accordance with the firm's Preservation Guidelines.

You may authorize someone to exercise the above rights on your behalf. If we have collected information about your Family Members, including minor children, you may exercise the above rights on behalf of your Family Members.

Note, KPMG neither sells Firm Personnel's Personal Information to any third parties nor shares Firm Personnel's Personal Information with any third parties for cross-context behavioral advertising

KPMGConnect Alumni Portal

Current and former partners, principals, and employees may enroll in the firm's alumni community portal, available at https://kpmgconnect.us.kpmg.com ("**KPMGConnect**"). KPMGConnect is a voluntary social platform to connect firm professionals. This Data Privacy Notice applies to the collection and processing of Personal Information on KPMGConnect, in conjunction with its Terms of Use. The Personal Information associated with your KPMGConnect profile, including but not limited to your name, address, e-mail address, telephone number, employment history, and your service on corporate boards and advisory councils, is visible to professionals who are enrolled in KPMGConnect, and may be made available upon reasonable request. KPMGConnect provides registered users with the ability to set privacy preferences through its portal settings.

Firm Personnel Data Privacy Notice

Data Security and Integrity

KPMG has, and requires its service providers to have, security policies and procedures in place to help protect Personal Information from unauthorized loss, misuse, alteration, or destruction. Despite KPMG's efforts, however, security cannot be guaranteed against all threats. We seek to limit access to your Personal Information to those who have a need to know. Those individuals who have access to such information are required to maintain the confidentiality of it. We also make efforts to retain Personal Information only for so long as such information is needed for legitimate business purposes or pursuant to applicable law, provided that we might in certain cases retain Personal Information for longer periods to comply with a data subject's request to do so, or until the data subject asks that the information be deleted, as permitted by law.

KPMG seeks to limit the collection of Personal Information to information that is relevant for processing purposes. Unless otherwise required or permitted by applicable law, KPMG does not process Personal Information in a way that is incompatible with the purposes for which it is collected or authorized to use.

Links to Other Sites

Please be aware that KPMG websites, applications, and social media platforms may contain links to other sites, including sites maintained by KPMG International and other member firms affiliated with KPMG International, that are not governed by this Data Privacy Notice, but by other privacy statements that may differ. KPMG is not responsible for the content or practices of these other sites. We encourage Firm Personnel to review the privacy policy of each website visited before disclosing any Personal Information.

Updates to This Data Privacy Notice

KPMG may update or modify this Data Privacy Notice from time to time to reflect our current privacy practices. When we make changes to this Data Privacy Notice, we will revise the "last updated" date at the top of this page. We encourage you to periodically review this Data Privacy Notice to be informed about how the firm is protecting your Personal Information.

Policy Questions and Enforcement

KPMG is committed to protecting the privacy of your Personal Information. If you have questions about our privacy practices, please contact the U.S. Privacy Office at us-privacy@kpmg.com. You may also use the foregoing email address or contact KPMG's Ethics and Compliance Office at us-eandc@kpmg.com, to communicate any concerns you may have regarding our compliance with this Data Privacy Notice.

1. *"KPMG," "we," "our," and "us" refers to KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited ("KPMG International"), a private English company limited by guarantee. KPMG International and its related entities do not provide services to clients.*

2. *"Third Party Personnel" means "Individual(s) engaged with KPMG through a third party," including Contractor Personnel, as such terms are defined in Ch. 16 of the U.S. Risk Management Manual. Note, if the data privacy terms in a Third-Party Personnel's agreement with KPMG conflict with this Data Privacy Notice, the terms of the agreement will prevail. Any additional questions may be addressed by contacting the Contingent Workforce Center of Excellence at us-hrsccwsupport@kpmg.com.*

Firm Personnel Data Privacy Notice

Privacy Policy Acknowledgement

I acknowledge that I have fully read, understand, and affirm my agreement to comply with the Privacy Policy.

Ajinkya Nimbhorkar
Print Name

Signature

Date

Whistle Blower Policy and Reporting Procedures Policy

All employees, partners, principals, officers, directors, and independent contractors ("Personnel") shall observe high standards of business and personal ethics in the performance of their duties. Personnel shall be responsible for conducting themselves in a manner consistent with the Firm's Code of Conduct (the "Code") and for ensuring that the values, commitments, and promises in the Code are met, including safeguarding KPMG's integrity, complying with all applicable laws and regulations, and reporting all potential violations of law or policy.

The Firm's Whistleblower Policy ("Policy"): (a) establishes procedures for reporting and addressing conduct that any Personnel reasonably believes may be a potential or actual violation of applicable laws, regulations, or Firm policy, including, without limitation, the Code, or any other matter that could cause serious damage to the Firm's reputation or operations; and (b) prohibits retaliation against anyone who reports their reasonable beliefs of actual or potential violations under this Policy.

BASIS OF POLICY

KPMG is committed to fostering a workplace that is conducive and welcoming to open discussion, where compliance is valued, and where everyone is involved in ensuring the Firm meets its ethical and legal obligations. This Policy is intended to supplement and not replace any laws or rules governing ethical or whistleblower laws or requirements applicable to the Firm and its Personnel.

The Firm is committed to acting lawfully and ethically and to encouraging lawful and ethical behavior in others.

PROCEDURE

Types of Complaints Covered by the Whistleblower Policy

Personnel shall report, in accordance with How to Report a Suspected Violation Procedure below, their reasonable belief of actual or suspected violations of the law or regulations or activity that may raise ethical issues or concerns for Personnel or the Firm pursuant to the Policy in all situations, whether it involves colleagues, clients, suppliers, subcontractors, vendors, or any other external parties with whom the Firm conducts business. Personnel shall additionally refer to and comply with professional ethics standards with respect to reporting actual or suspected non-compliance with laws or regulations by clients. See Code of Conduct for additional information.

As part of the Firm's commitment to maintaining ethical and legal conduct, the Firm encourages Personnel to bring to its attention information about suspected violations of law or improper or unethical conduct by anyone, without regard to the identity or position of the suspected offender. Such conduct includes, but is not limited to: suspected fraud, theft, embezzlement or other integrity issues; accounting, internal accounting controls, or auditing concerns; threats or other safety concerns; retaliation, harassment, discrimination, or any other violations of the Code or any Firm policies and procedures; human rights or child labor violations; misuse of resources or assets; or any other suspected violation of law, professional standards, or ethical standards that could cause harm to the business or reputation of the Firm (each, a "Complaint").

How to Report a Suspected Violation

Personnel may submit a Complaint using any of the following methods.

Whistle Blower Policy and Reporting Procedures Policy

Ethics and Compliance Hotline

The Firm has established the Ethics and Compliance Hotline, managed by an independent third party, which protects the confidentiality of individuals submitting Complaints and also allows for anonymous reporting. The Ethics and Compliance Hotline can be reached at 1-877-576-4033 or www.kpmgethics.com .

Additional Channels of Communication

The additional channels of communication available for Personnel to report Complaints include:

- The Chief Ethics and Compliance Officer
- The Office of General Counsel
- Talent & Culture
- Ethics & Compliance
- The engagement partner(s)
- Their PMLs, practice leader, service line leader, office managing partner, or KPMG's Ombudsman
- A Professional Practice Partner or Risk Management Partner
- Firm leadership, including the Chair, Deputy Chair, Vice Chairs, and Board Members

Complaints are forwarded to the Ethics & Compliance-Investigations Division, documented in the Firm's case management system, and triaged for investigation, as warranted.

Compliance Oversight Responsibility

The Regulatory, Risk & Compliance Committee of the Board of Directors (the "RRCC"); the Legal, Risk and Regulatory Committee; and the Management Review Panel (collectively, the "Committees") oversee the Firm's compliance program to help ensure fair and consistent enforcement of the Code. The Chief Ethics and Compliance Officer ("CECO") oversees the day-to-day operations of the compliance program. Under the auspices of the CECO, the Principal in Charge- Investigations ("PIC-Investigations") and/or his or her delegate oversees the receipt, retention, and treatment of Complaints, and reviews all Complaints and determines the steps to take with respect to any Complaint.

Any Personnel, including members of the Committees, who are the subject of a Complaint cannot oversee or handle the Complaint and cannot participate in any investigation or resolution related to that Complaint, except to provide information as may be necessary for investigating the Complaint.

Investigations

When possible, the Firm will promptly acknowledge receipt of the Complaint. Under the auspices of the CECO, the PIC-Investigation or his or her delegate will supervise investigations, if warranted.[1] The PIC-Investigations or his or her delegate shall determine the necessary and appropriate persons to notify of the

[1] It should be noted that certain matters fall outside the CECO's purview. In accordance with a Consent and Undertakings Agreement with the SEC, dated March 3, 2005, KPMG's Ombudsman has full authority to conduct his or her own investigation of any matter identified and raised by a KPMG professional, which they may believe has not been adequately addressed at the engagement team level, and which relates to professional practice concerns pertaining to a KPMG public company audit client. Aside from such matters being handled by the Ombudsman, the investigation process is conducted under the auspices of the CECO.

Whistle Blower Policy and Reporting Procedures Policy

Complaint and the nature and scope of the investigation to be done. The PIC- Investigations or his or her delegate may utilize resources from within the firm (including, without limitation, Office of General Counsel, Talent & Culture, Firm Security Services, Risk Management, and/or Forensics), to provide support as needed in the investigation. In certain instances, an investigation may also involve the assistance of external legal counsel, external forensic accounting or auditing firms, or other third parties. In response to a substantiated Complaint, the Firm shall implement appropriate remediation, including disciplinary action against the offender.

Personnel shall cooperate fully and truthfully in connection with any investigation. Anyone who provides false information pursuant to this Policy or knowingly attempts to alter, conceal, cover up, falsify, or destroy any documents, property, or information to prevent their use in or to influence an investigation, shall be subject to disciplinary action and may also be subject to criminal penalties and fines.

No Retaliation

Retaliation in any form is contrary to the Firm's Values. The Firm has a zero- tolerance policy against retaliation, which prohibits retaliation against anyone who, in good faith, reports a concern under this Policy or participates in an investigation, even if the allegation ultimately is not substantiated. Any person who engages in retaliation shall be subject to disciplinary measures, up to and including separation and potential legal consequences. Acts of retaliation shall be reported via the channels identified in the How to Report a Suspected Violation portion of this Policy.

Acting in Good Faith

All complaints shall be submitted in good faith. Individuals who knowingly submit false or fictitious reports or Complaints shall be subject to disciplinary measures and potential legal consequences. This is not intended to discourage individuals from filing concerns about suspected violations. The Firm recognizes that, in some instances, it may not be possible to determine whether a complaint or concern is warranted. In such instances, individuals shall use their best judgment and ethical responsibility in compliance with this Policy.

Confidentiality

In order to encourage individuals to come forward with any good faith report of suspected violations of laws or regulations or unethical behavior, all reports made under this Policy shall be treated as confidential to the utmost extent possible, consistent with applicable law, the parameters set forth under this Policy, and the Firm's obligation to investigate the Complaint and, if appropriate, take (or direct the taking of) corrective action.

Other Reporting

Government or Regulatory Reporting

Nothing in this Policy, the Code or any policies of, or agreements with, the Firm prohibits Personnel from (i) making truthful statements or disclosing information as may be required by applicable law or regulation, or pursuant to the valid order of a court of competent jurisdiction or an authorized government or regulatory agency, (ii) cooperating with or participating in any investigation by a governmental or regulatory agency, (iii) reporting a reasonable belief of possible violations of federal, state or local law or regulation to or filing a charge with any governmental agency, regulatory, or entity (including, but not limited to, the Department of Justice (DOJ), the Securities and Exchange Commission (SEC), Public Company Accounting Oversight Board (PCAOB), Financial Industry Regulatory Authority (FINRA) or the Equal Employment Opportunity Commission (EEOC)), or making other disclosures that are protected under the whistleblower provisions of

federal, state or local law or regulation and the prior authorization of, or notification to, the Firm is not needed to make any such reports or disclosures.

Contractor Personnel Whistleblower Rights

As a government contractor, the Firm is subject to Federal laws that provide certain additional rights for employees of government contractors or subcontractors. Accordingly, the Firm shall not discharge, demote, or otherwise discriminate against Personnel as a reprisal for disclosing "Certain Information" to:

- A Member of Congress or a representative of a committee of Congress;
- An Inspector General;
- The Government Accountability Office
- A Federal employee responsible for contract oversight or management at the relevant agency;
- An authorized official of the Department of Justice or other law enforcement agency;
- A court or grand jury; or
- A management official or other employee of the Firm or its subcontractor who has the responsibility to investigate, discover, or address misconduct.

"Certain Information" is defined as information that Personnel reasonably believes to be:

- Evidence of gross mismanagement of a Federal contract;
- A gross waste of Federal funds;
- An abuse of authority relating to a Federal contract;
- A substantial and specific danger to public health or safety; or
- A violation of law, rule, or regulation related to a Federal contract (including the competition for or negotiation of a contract).

In addition, the Firm shall not discharge, demote, or otherwise discriminate against any Personnel as a reprisal for providing information that the individual reasonably believes is evidence of contractor or subcontractor misconduct relating to waste, fraud or abuse on a Federal contract in any judicial or administrative proceeding.

In the event Personnel believes that they have been subjected to a reprisal for disclosing any information as described above, that individual may submit a complaint to the Inspector General of the agency involved. In accordance with 41 U.S.C. § 4712, a complaint must be filed no more than three (3) years after the date on which the alleged reprisal took place

After submission of a complaint to the relevant Inspector General, the head of the agency must determine within thirty (30) days whether there is sufficient basis to conclude that the individual has been subject to a reprisal and must issue a notice to the individual either denying relief or take one or more of the following actions:

- take affirmative action to abate the reprisal;
- reinstate the person to the position that the person held before the reprisal, together with compensatory damages (including back pay), employment benefits, and other terms and conditions of employment that would apply to the person in that position if the reprisal had not been taken;

Whistle Blower Policy and Reporting Procedures Policy

- pay the complainant an amount equal to the aggregate amount of all costs and expenses (including attorneys' fees and expert witnesses' fees) that were reasonably incurred by the complainant for, or in connection with, bringing the complaint regarding the reprisal, as determined by the agency; or
- consider disciplinary or corrective action against any official of the agency, if appropriate.

Ajinkya Nimbhorkar

Print Name

Authorized Signature

Date

Certificate Of Completion

Envelope Id: C1EBAE0B-408F-4894-ABDC-E37F6B93724B
Status: Delivered
Subject: Complete with DocuSign: CW Package 3 Ajinkya Nimbhorkar ajinkya.nimbhorkar@nitorinfotech.com
CandidateID:
cf_application:
Doc Code:
EmployeeID:
First Name:
Last Name:
Date Exam Passed:
Certification Name:
Effective Date:
Source Envelope:
Document Pages: 41
Signatures: 0
Certificate Pages: 4
Initials: 0
AutoNav: Enabled
EnvelopeId Stamping: Enabled
Time Zone: (UTC-06:00) Central Time (US & Canada)

Envelope Originator:
us-svc-sndocusignprd
200 E Randolph St
Chicago, IL 60601
us-svc-sndocusignprd@kpmg.com
IP Address: 199.91.136.12

Record Tracking

Status: Original
8/25/2025 1:01:47 PM
Holder: us-svc-sndocusignprd
us-svc-sndocusignprd@kpmg.com
Location: DocuSign

Signer Events	Signature	Timestamp
Ajinkya Nimbhorkar ajinkya.nimbhorkar@nitorinfotech.com Security Level: Email, Account Authentication (None), Access Code **Electronic Record and Signature Disclosure:** Accepted: 8/26/2025 12:01:21 AM ID: 3bb34f0c-9583-4a4b-953a-15b774573e9d Company Name: KPMG LLP		Sent: 8/25/2025 1:01:51 PM Viewed: 8/26/2025 12:01:21 AM

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	8/25/2025 1:01:51 PM
Certified Delivered	Security Checked	8/26/2025 12:01:21 AM

Payment Events	Status	Timestamps

Electronic Record and Signature Disclosure

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, KPMG LLP (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through your DocuSign, Inc. (DocuSign) Express user account. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to these terms and conditions, please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. For such copies, as long as you are an authorized user of the DocuSign system you will have theability to download and print any documents we send to you through your DocuSign user account for alimited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a $0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. To indicate to us that you are changing your mind, you must withdraw your consent using the DocuSign 'Withdraw Consent' formon the signing page of your DocuSign account. This will indicate to us that you have withdrawn your consentto receive required notices and disclosures electronically from us and you will no longer be able to use yourDocuSign Express user account to receive required notices and consents electronically from us or to signelectronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact KPMG LLP:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:
To contact us by email send messages to: us-hrkbstechdssup@kpmg.com

To advise KPMG LLP of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at us-hrkbstechdssup@kpmg.com and in the body of such request you must state: your previous email address, your new email address. We do notrequire any other information from you to change your email address.

In addition, you must notify DocuSign, Inc to arrange for your new email address to be reflected in yourDocuSign account by following the process for changing e-mail in DocuSign.

To request paper copies from KPMG LLP

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to us-hrkbstechdssup@kpmg.com and in the body of such request you must state your e-mail address, full name, US Postal address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with KPMG LLP

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;

ii. send us an email to us-hrkbstechdssup@kpmg.com and in the body of such request you must state your e-mail, full name, IS Postal Address, telephone number, and account number. We do not need anyother information from you to withdraw consent.The consequences of your withdrawing consent foronline documents will be that transactions may take a longer time to process.

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: https://support.docusign.com/guides/signer-guide-signing-system-requirements.

Acknowledging your access and consent to receive materials electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please verify that you were able to read this electronic disclosure and that you also were able to print on paper or electronically save this page for your futurereference and access or that you were able to e-mail this disclosure and consent to an address where you willbe able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format on the terms and conditions described above, then select the check-box next to ‘I agree to use electronic records and signatures’ before clicking ‘CONTINUE’ within the DocuSign system.

By selecting the check-box next to ‘I agree to use electronic records and signatures’, I confirm that:

- I can access and read this Electronic CONSENT TO ELECTRONIC RECEIPT OF ELECTRONIC RECORD AND SIGNATURE DISCLOSURES document; and
- I can print on paper this Electronic Record and Signature Disclosure, or save or send this disclosure to a place where I can print it, forfuture reference and access; and
- Until or unless you notify KPMG LLP as described above, I consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by KPMG LLP during the course of my relationship with you.