

Standards Guide for External Workers

December 2020

CONFIDENTIAL AND PROPRIETARY   
Any use of this material without specific permission  
of McKinsey & Company is strictly prohibited.

Contents

[About this document 1](#_Toc525671569)

[Who we are; Mission and Values 2](#_Toc525671570)

[McKinsey’s Values 2](#_Toc525671572)

[Our values in action 3](#_Toc525671573)

[Our External Worker policy 4](#_Toc525671574)

[Confidentiality 6](#_Toc525671575)

[Why](#_Toc525671576) confidentiality is so important …………………………………………………………………………………………………………….…6

[What do we consider to be confidential information? 7](#_Toc525671577)

[Protecting personal data 7](#_Toc525671578)

[Client services & other arrangements 9](#_Toc525671579)

[The three most common professional standards and risk issues 9](#_Toc525671580)

[External Workers and board memberships 10](#_Toc525671582)

[Direct Information gathering guidelines 10](#_Toc525671583)

[External Communications & Use of Name 11](#_Toc525671584)

[External Communications & Use of Name 11](#_Toc525671585)

[Use of social media 12](#_Toc525671586)

[Information Security 13](#_Toc525671587)

[Information security 13](#_Toc525671588)

[Remote access and wireless security 15](#_Toc525671589)

[Working remotely; security and anti-virus protection 15](#_Toc525671590)

[Personal conduct & investments 17](#_Toc525671591)

[Ensuring an environment free from discrimination and harassment 17](#_Toc525671592)

[Violence in the workplace 18](#_Toc525671593)

[Anti-corruption 19](#_Toc525671594)

[Monitoring and record keeping 20](#_Toc525671596)

[Personal investments 20](#_Toc525671597)

[Personal safety and security 21](#_Toc525671598)

[Office and travel 21](#_Toc525671599)

[Key contacts 22](#_Toc525671600)

[Appendix 23](#_Toc525671602)

# About this document

* As one of McKinsey’s External Workers, you are a valued member of our community, and your actions and contributions help to uphold the Firm’s distinctiveness and strong reputation
* The Firm’s distinctiveness has been, and always will be, driven by our Mission and Valueswhich were first articulated over 80 years ago by former Managing Partner, Marvin Bower
* Our Mission and Values guide the decisions we make each day, and permeate every interaction with clients and colleagues
* Regardless of whether you are engaged directly by McKinsey or through a Supplier/Vendor, this document is designed to introduce you to the Firm’s Mission, Values and professional standards, as well as detailing the policies and standards with which you are expected to comply whilst undertaking any work on the Firm’s behalf
* You have an important role to play in upholding our Mission and Values.Please note that as one of our External Workers, you might be required to complete specific training from time to time, e.g. Cyber Security
* Throughout the document we refer to your ‘Point of Contact’. This would normally be your Sponsor(s) – the person who contracted you to undertake any work for us - or someone in your Sponsoring practice/cell. If you are unsure who this would be in a particular situation, please check with your Sponsor(s)
* If you have any questions, please contact your McKinsey Point of Contact, the Professional Standards and Risk team (professional\_standards@mckinsey.com) or refer to the resources at the end of this document
* At the very end of this document you’ll find a page for you to sign, scan and send back to the Firm acknowledging receipt. The policies and standards included in this document apply to all External Workers regardless.

# Who we are; our Mission and Values

**OUR MISSION:**

To help our clients make distinctive, lasting and substantial improvements in their performance, and to build a great Firm that attracts, develops, excites and retains exceptional people.

**OUR VALUES:**

**Adhere to the highest professional standards**

* Put client interests ahead of the Firm’s
* Observe high ethical standards
* Preserve client confidences
* Maintain an independent perspective
* Manage client and Firm resources cost-effectively

**Improve our clients’ performance significantly**

* Follow the top-management approach
* Use our global network to deliver the best of the Firm to all clients
* Bring innovations in management practice to clients
* Build client capabilities to sustain improvement
* Build enduring relationships based on trust

**Create an unrivalled environment for exceptional people**

* Be non-hierarchical and inclusive
* Sustain a caring meritocracy
* Develop one another through apprenticeship and mentoring
* Uphold the obligation to dissent
* Govern ourselves as a ‘one Firm’ partnership

**HOW YOU MIGHT HEAR OUR FIRM MEMBERS TALKING ABOUT OUR VALUES IN ACTION**

*“Whenever I reach out for help, I always get a constructive response; if the person I ask doesn’t know the answer, they’ll refer me to someone else who might know. I pay it forward and follow the unwritten rule of responding to questions as soon as I can.”*

*“I schedule regular feedback discussions with my manager about my work – and it’s never a one-way conversation. I get feedback and the expectation is that I’ll also give feedback.”*

*“I’ve learnt never to try and solve a problem on my own. Someone somewhere in the Firm has thought about the same, or a similar problem and can help me.”*

*“The best idea can come from anyone from the room. If you can back up what you say with data and analyses, people will listen.”*

*“I’ve had explicit conversations with family and friends, so they understand why I can’t tell them who our clients are and what we’re doing for them. People really respect us for taking client confidences seriously.”*

*“McKinsey leaders don’t talk in terms like profitability or hours worked. They value the size of our impact, or the depth of our relationships.”*

# Our External Worker policy

**We engage External Workers to bring the best to our clients and to our Firm. All External Workers are required to comply with the following:**

**Required arrangements**

* Have a Sponsor representing your sponsoring practice/cell or Firm Function. They are ultimately responsible for ensuring that you are engaged in a manner consistent with our policies. If you are doing any client facing work your primary Sponsor must be a Partner
* Have a signed current contract or Statement Of Work (SOW, linked to a Supplier Master Service Agreement (MSA)) and Non-Disclosure Agreement (NDA)
* You must have undergone a background screening as part of the engagement process (where applicable)

**Immediate action points upon/during engagement by McKinsey**

* Agree to comply with the Firm’s Information Security requirements, particularly concerning use of the Firm’s hardware, email usage, data handling, systems access and devices (see section on Physical & Information Security)
* Read and confirm that you agree to comply with the **Standards Guide for External Workers** (this document)
* Obtain up-front approval from the Firm if sub-contractors might be required (this must be addressed in your contract/MSA/SOW)
* Inform your Sponsors of any work (or requests for work) you may potentially do in the field of procurement/suppliers. Your sponsors will need to ensure this is compliant with our PSE (Purchaser-Supplier Engagement) policy
* Ensure you have visas/work permits required to undertake your work; only when it is legally required for McKinsey to sponsor an External Worker’s immigration process will it do so

**Ongoing action steps:**

* If engaged directly by McKinsey, all invoices should be submitted on a monthly basis to your Sponsors/Point of Contact
* If engaged through a Supplier/Vendor, please follow their invoice process
* Inform your Sponsors immediately if:
  + You accept a full-time job elsewhere
  + You are considering joining a board (includes all types of board, whether private sector, pro bono and so on)
* As an External Worker to McKinsey you may include your work with us in written or online CVs (unless prohibited by the Supplier/Vendor if you are engaged through one), so long as you comply with our confidentiality requirements, and both your role and method of engagement are accurately characterized (e.g., ‘employed by Manpower, assigned to McKinsey’, ‘Advisor to McKinsey’), there is no mention of McKinsey clients, and you do not represent yourself as being a Firm employee.

# Confidentiality

It is vital that in your work with us you comply with our policies at all times. It is your responsibility to:

**Be discreet about the Firm and our work**

* Never mention clients by name (or implication) or discuss confidential details with anyone, including close friends and family
* Risks may be higher if you handle Firm or clients’ personally-identifiable information (e.g., names, emails, or other individual identifiers). Consult your Point of Contact in these situations.
* Take precautions working in public, e.g., use a security screen, disguise names and details

**Share confidential information safely and securely**

* Follow sanitization guidelines provided by the Engagement Manager (EM) or CST before sharing documents or work products with Firm members or other External Workers outside your working team. Never share documents or work product outside of McKinsey without explicit approval from the ED (for client work) or your Point of Contact (for all other work)
* When sharing electronically, only use Firm approved devices (e.g., Firm-issued laptop or remote desktop), and systems (e.g., Firm email, Box). **Never use personal email addresses or social media accounts (e.g., direct messaging services such as Messenger or WhatsApp) for any work being done on behalf of the Firm**
* Do not use any service providers (e.g., event coordination) or software (e.g., analytics tools) or information (e.g., third party data sets) **unless approved by the Firm for use** both generally and specifically in the context of your work
* **Securely discard/delete confidential information once done –** e.g., shred documents, erase whiteboards, delete non-final documents. In the case of client work, submit final documents to the EM of the study

**Safeguard belongings; your own, the client’s and the Firm’s**

* Do not leave anything unattended (e.g., lock team rooms/computers, keep your laptop with you at all times)
* Immediately report missing electronic devices (e.g., laptop, phones, USB sticks) to Global Helpdesk[[1]](#footnote-1)

**Take care online**

* Never post information about clients or the Firm
* Use the highest privacy settings possible

## What we consider to be confidential information

**Client information**

* Identity of the client, or information that allows someone to identify the client (e.g., “I’m serving the largest TelCo. in Japan”)
* Information disclosed to McKinsey by a client or its representative
* Purpose or content of the engagement
* Our recommendations to the client
* Materials developed for the client
* Non-public information about organization strategy, finances, personnel

**McKinsey proprietary information**

* The Firm’s Policies and Guidelines, financial information, compensation, personnel structure and processes
* Frameworks, tools, methodologies, software, applications and industry knowledge developed by Firm members or by third party contractors or vendors for use by the Firm and/or its clients
* Third party information purchased or licensed by the Firm
* Information or materials found on our Global Intranet, KNOW or Learn portals

## Protecting Personal Data

**If your work might include the processing of personal data, please speak with the Engagement Director (ED) (for client work) or your Sponsor (non-client work) to ensure you are handling this in the appropriate manner.**

* Data privacy laws require personal data be protected by appropriate safeguards since individuals can be harmed when the confidentiality, security or integrity of their data is compromised. It is our responsibility to safeguard the personal data of our colleagues and of our clients’, as well as any data our clients share with us. In addition to regulatory requirements, clients frequently impose stringent contractual obligations on the Firm to protect their personal data. Ensure all personal data is transferred, stored and accessed following McKinsey’s information security best practices[[2]](#footnote-2)
* “Personal data” consists of all data relating to an identified or identifiable person. An identifiable person is one who can be identified, ***directly or indirectly***, by reference to one or more characteristics. This includes personal data that directly identifies an individual (e.g., name, employee number, national ID number, email/physical address). It also includes data that indirectly identifies an individual – data that identifies an individual only in combination with other data elements (e.g., date of birth, IP address, demographics). “Sensitive personal data” is subset of personal data for which data privacy laws and McKinsey have imposed additional restrictions, obligations, privacy and security measures
* **You must:**
  + Know when you are processing personal data
  + Ensure you have the necessary rights to process personal data
  + Process personal data only at the client’s or your sponsor’s direction
  + Ensure appropriate client agreement
  + Process the minimum personal data necessary only for the purposes of the engagement, and within the bounds of McKinsey’s policies
  + Retain personal data only for so long as it remains necessary whilst deploying risk-mitigation strategies
  + Appropriately protect personal data

# Client services & other arrangements

## The three most common professional standards and risk issues

It is the **Firm’s long-standing practice to serve competitors** and to do so without compromising our professional responsibility to maintain the confidentiality of client information**.** As an External Worker, we expect you to:

1. Preserve client confidences by **protecting their confidential, critical, business-sensitive information**
2. Proactively **manage potential conflicts** to ensure confidential information from one client is not used to the (dis)advantage of another
3. Preserve our reputation for objectivity and ability to have impact, and avoid competitive sensitivities by **not allowing clients to use the McKinsey name** for advocacy or to build credibility for their initiatives

We must all be vigilant and take responsibility– it takes concerted and collective effort to maintain the Firm’s reputation and professional independence. It takes just one, even unintentional, breach to tarnish it.

No member of the Firm or External Worker who has served a client or, in the Firm’s judgement, acquired confidential information about a client, may serve a competitor if, based on the anticipated role of the individual and the nature of the engagement, such confidential information could be used to the first client’s material (dis)advantage.

## Proactively manage conflicts to ensure confidential information from one client is not used to the (dis)advantage of another

**Proactively flag actual, potential or perceived conflicts of interests to your McKinsey Point of Contact/Sponsor** and discuss these prior to starting work with a new client, team or individual. Conflict is not limited just to client-facing advisors but could be relevant to all External Workers.

**Potential sources of conflict to highlight:**

* You have confidential informationabout an organization which could (dis)advantage a potential client (including the Firm)
* You have personal or professional affiliationsto a potential client (e.g., Board member/advisor, family member is an employee)

Please raise with your Sponsors or Point of Contact any questions or concerns about potential conflicts;they will involve the appropriate practice leaders and other risk professionals to help determine the right approach.

## External Workers and Board memberships

* If you are an External Worker who spends more than half your time with the Firm, you are prohibited from retaining for-profit board positions while working with us
* If you are spending less than half your time working with the Firm, you may serve on not-for-profit or corporate boards, subject to the following restrictions to protect the Firm’s reputation and client relationships:
  + Avoid contact with the CSTs (Client Service Teams) supporting these companies or institutions
  + Abstain from any board vote to retain McKinsey
  + Ensure the McKinsey teams working with you are aware of the board membership(s) and can therefore be circumspect regarding what information may be shared
  + Ensure no McKinsey or client resources or materials are used for a board role
  + Do not serve on the boards of businesses whose primary purpose is to make proprietary investments (e.g., hedge funds, Private Equity (PE) firms) i.e., where the board members have a fiduciary duty to investment firms. However, you may serve on the board of a PE-owned portfolio company (as the fiduciary duty is to the portfolio company, not the PE firm)
* You must disclose all new board memberships being considered to your Sponsor(s) prior to any commitment being made
* If you have any questions regarding board memberships, please contact your Sponsor/Point of Contact.

## External workers and purchaser-supplier engagements

* If you are doing work outside McKinsey relating to commercial terms a McKinsey client might have with suppliers/buyers, you may not work on our behalf as an External Worker for any teams supporting that client

## Direct Information Gathering Guidelines

* To ensure we meet international requirements and our own high professional standards, we may use multiple means of gathering current data to inform our client work
* Whilst doing this, we follow these guidelines:
  + We do not misrepresent who we are or what we are doing
  + We do not seek confidential or proprietary information
  + We do not trespass on private property
  + We do not use spam or related techniques to identify recipients who have no pre-existing basis to be contacted
* If you are asked to gather information on our behalf or for our clients, you should also follow these guidelines. If you require more information, ask your Sponsors to share the Firm’s Direct Information Gathering Guidelines.

# External communications & use of name

## External Communications & Use of Name

The Firm has several policies which guide our approach to communicating externally, and which govern the use of McKinsey’s name. It is important that you ensure these are upheld at all times.

**External Communications**

* **Do not disclose client names** (past or present) in any public forum
* **Do not disclose information** about the workings or performance of clients, individual cells, special initiatives, or the Firm as a whole
* **Do not refer to McKinsey as a customer or a client**, without the prior permission of your Sponsor and Firm Communications
* Contact your Sponsor if you are asked to **speak in any official capacity on behalf of the Firm, or if a journalist contacts you with questions about McKinsey or a client you are serving with McKinsey**. Do not comment, even to confirm factual information
* Do not disclose details of your agreement with the Firm and ensure you comply with the associated clause(s) of your contract/SOW

**Use of Name**

* Mention of the Firm’s name or association in relation to any external activities of an External Worker (e.g. speeches, public appearances, blogs or publications including books) must be approved in advance by your sponsors, the relevant Practice/Industry leader(s) and Firm Communications
* Any public use of the Firm’s name by a client must be approved by the affected Practice/Industry leader(s) and Firm Communications. You must immediately notify your Sponsor if you see/hear a **client’s public disclosure of our involvement**
* All public use of the McKinsey logo must be approved by the Firm’s Director of Communications.

Always contact your Sponsor firstregarding any potential public use of the Firm’s name. Your sponsor should then contact Firm Communications[[3]](#footnote-3).

## Use of social media

**Our intent is not to censor External Workers on social media. Rather, these guidelines promote safe use of social media that aligns with our values and professional standards.**

**Three main principles that underpin our approach to social media:**

1. Maintain client and Firm confidentiality
2. Enhance and protect your and the Firm’s reputation
3. Uphold Firm values and policies

* **Always use your McKinsey external email address** whenever doing anything for, with, or connected to the Firm
* **If you indicate a relationship with McKinsey on social media or elsewhere**, you should include the following disclaimer: “Any views or statements expressed are mine and not those of any company or organization I work with”
* **Be professional and respectful of others when using social media**
* Email [social\_media@mckinsey.com](mailto:social_media@mckinsey.com), if you plan to regularly publish onto an online platform or if you see anything online of which the Firm should be aware.

**Practical examples:**

* If the client you are helping to serve is the only major company in a small town, do not “check-in” on social media sites or enable location services on your smartphone
* Do not share data from a research report the Firm purchased, or insights from a client engagement
* Your LinkedIn or other social media profiles should not provide information which would allow a reader to identify current and previous clients (e.g., by allowing others to see numerous contacts at one company where you participated in a McKinsey client engagement). This continues to apply when you are no longer an External Worker to McKinsey.

# Information Security

## Information security

**Email**

* As an External Worker, you must use only your McKinsey external email account for all Firm-related activities. No personal or other company accounts or email should be used for any work being done for or with McKinsey
* **McKinsey email should not be used for purposes other than McKinsey-related work;** do not share opinions over email
* No internal emails containing Firm or client confidential information can be forwarded to personal external email accounts

**Data**

* External Workers cannot download data to any external device (USB, physical media etc.) unless approved in advance in writing by their Sponsor
* External devices must be encrypted
* McKinsey data cannot be stored or transferred via any means (e.g., software, file sharing services, code repository) except for providers pre-approved by the Firm for use in connection with the External Worker’s work
* All McKinsey data must be securely deleted with written confirmation at the end of the project or study
* Box should be used to share and store all McKinsey and client data; documents should be sent as Box links within emails rather than attachments

**Devices**

You must use Firm devices or remote desktop (Citrix) anytime you require access to McKinsey email or IT systems to undertake work being done at the request of or on behalf of McKinsey.

McKinsey devices should not be left unattended in public spaces or checked in luggage when travelling. If a device is lost or stolen, report it to GHD and your Sponsor immediately.

In addition to the above you must also comply with the following:

* No McKinsey or McKinsey client data should be backed up to any non McKinsey device or service
* McKinsey provided devices should only be used for work being done at McKinsey’s request
* A process should be in place by which any Intellectual Property of McKinsey (e.g. code, models, designs) is transferred to or stored in a McKinsey system prior to the end of your engagement with the Firm
* Access to the McKinsey environment should only be via Firm approved mechanisms with appropriate business approvals

If using a personal mobile device, that device must meet the requirements of McKinsey’s Bring Your Own Device (BYOD) program and a BYOD agreement must be signed.

**Technology Security and usage**

* All information technology resources should have passwords that meet the following criteria:
  + Minimum of 12 characters
  + A combination of 2 of the following 3 attributes
    - Letters and numbers
    - Uppercase and lowercase
    - Special characters (e.g., # & \* ! $)
  + There will be a forced password change every 90 days; re-use of the same password is only allowed after 8 further changes
  + The password for your McKinsey device(s) must be different to all other passwords you use elsewhere
* Web browser/computer security settings are not to be changed (as this increases risk of compromised data)
* You must protect your laptop against theft when traveling and in client team rooms
* Avoid communicating sensitive information via cellular phones or instant messaging software
* Exercise reasonable judgement before using email to transmit highly sensitive material
* Do not send email under another user’s email identity without express and specific authorization
* Restrict email distributions to appropriate recipients and verify external recipient email addresses before sending messages
* Be mindful in emails; assume that anything you write could end up in the public domain
* You must promptly return any McKinsey owned devices at the end of an External Worker arrangement

The Firm reserves the right to review, monitor, and disclose any information communicated (including records of such communications) by anyone using the Firm’s information technology resources to prevent, investigate, or detect any activity that conflicts with this or other Firm policies or with criminal or other laws.

**Cyber Security**

* Act within the requested timeframe if asked to undertake any Cyber/IT security training by McKinsey
* Participate in the Firm’s ‘Phishing’ awareness exercises
* If you believe an email you have received could be a phishing attempt, send the email to [phishing@mckinsey.com](mailto:phishing@mckinsey.com) for investigation

## Remote Access and Wireless Security

**Remote Access**

For all remote access from McKinsey laptops, McKinsey’s VPN solutions (e.g. VPN Pulse Secure or Global Protect), must be used. All implementations of GRA (Global Remote Access) and Pulse Secure are ‘one-time’ installations and may not be reused for access from multiple devices.

**Wireless Security**

Device security settings should not be changed or removed

When working remotely do not connect a McKinsey-approved device to unsecured wireless networks (e.g., airports, coffee shops); the preferred option is to use tethering or a McKinsey mifi device, but always enable VPN (Virtual Private Network).

If using a Firm-supported device (e.g. McKinsey iPhone) for personal hotspot or tethering:

* Do not allow anyone to tether or connect to your device without your permission
* Turn tethering off when not in use
* Use strong encryption (WPA-2) with complex passwords

When using wireless, do not connect a network cable or create a bridge between networks.

## Working remotely; Security and Anti-Virus protection

**Working remotely security**

All External Workers working remotely must ensure reasonable security measures are in place and, at a minimum, that they are consistent with the standards outlined on this page:

* The space has windows and doors that can be secured
* Strong locks with keys held only by appropriate persons
* Lockable security cabinets/containers to secure documents, media and devices

Appropriate levels of visual and auditory privacy to be ensured:

* Client or Firm confidential material must not be visible to other members of the household or visitors
* Confidential conversations must take place out of the hearing of other household members or visitors
* Working papers must not be left unattended
* Privacy screens must be used
* Unwanted confidential documents to be shredded or placed in secure recycling bins in a McKinsey office

In the event of a burglary, this must be reported to both your Point of Contact and to Firm Security **immediately.**

**Anti-virus and anti-malware protection**

Protecting McKinsey data from infection by viruses and malicious code is an important part of the Firm’s security strategy

* All laptops must have the latest anti-virus software installed and running
* Anti-virus software updates must always be accepted when requested and the software should never be disabled or removed
* Report any virus infection incidents immediately to the GHD
* Hard disks should be scanned no less frequently than monthly

# Personal conduct & investments

## Ensuring an environment free from discrimination and harassment

The purpose of the Firm’s policy – which goes beyond what is prohibited by law – is to ensure that all Firm Members and External Workers can work in an environment free from harassment or discrimination.

McKinsey expressly prohibits:

* Any form of discrimination, harassment, bullying, or other offensive conduct toward any individual on the basis of race, color, religion, sex, sexual orientation, gender identity, marital status, pregnancy, age, disability, national or ethnic origin, military service status, citizenship, or other characteristic
* Any behavior that makes the work environment hostile, intimidating, or offensive to colleagues because of any characteristic listed above
* Any form of retaliation against an individual who in good faith reports a complaint or who assists in an investigation.

Behavior prohibited above is unacceptable both on Firm premises and in any work-related setting outside the Firm, such as business meetings, business trips, Firm-sponsored events or other business-related social events.

If you believe that discriminatory, harassing, or offensive conduct, or retaliation, is occurring or has occurred, you should report it immediately to your Sponsor, Point of Contact or the relevant HR/Professional Development representative. The Firm will promptly investigate and take appropriate disciplinary action as required, up to and including separation from the Firm, against any Firm member or External Worker who is in violation of this policy.

Complaints will be treated confidentially, and information collected will be restricted to those with a need to know, subject to any applicable disclosure obligations that the Firm is required to comply with.

For further information on what McKinsey believes constitutes unacceptable behavior, including harassment and discrimination, please ask your Sponsors/Point of Contact to share with you the full Firm policy on this topic.

## Violence in the Workplace

**McKinsey is committed to providing our colleagues, those conducting business at and with the Firm, and our guests with a non-threatening work environment free of violent behaviour of any kind.**

The Firm expressly prohibits, and will not tolerate any actual, attempted or threatened acts of violence including, but not limited to:

* Violent behaviour of any kind
* Threats to engage in violent behaviour whether made in person, orally or in writing
* The sabotage of, or threats/attempts to sabotage, Firm property or facilities
* Causing, or threatening/attempting to cause, physical damage to Firm property or facilities

Weapons of any kind are prohibited in all premises leased or owned by McKinsey unless the individual is an active government law enforcement official conducting official business. This prohibition applies regardless of whether an individual has a valid permit or license to carry a weapon.

## Anti-Corruption

**McKinsey is committed to the highest ethical, professional and legal standards, including compliance with the anti-corruption laws of all the jurisdictions in which we operate, including but not limited to the US Foreign Corrupt Practices Act and the UK Anti-Bribery Act.**

The Firm’s policy on anti-corruption prohibits the Firm, Firm Members and External Workers from:

* Giving, paying, promising, offering, or authorizing the payment of anything of value either directly or indirectly (e.g., through another party) to any party including any government officials
* To persuade any party to help the Firm (or anyone else, including an External Worker) secure an improper advantage (such as preferential treatment in securing an engagement, favorable immigration or customs treatment, lower tax assessment, expedited payment for services, etc.)

The Firm’s prohibition on bribery extends to benefits in all forms, including monetary payments and kickbacks, lavish meals, gifts, travel, entertainment, and other items of value. Please consult your Point of Contact before:

* Receiving gifts, meals or hospitality
* Giving gifts
* Providing hospitality

All transactions on behalf of the Firm – including third party transactions, gifts, meals, hospitality, and other expenditures – must be handled by the relevant DCS (Director of Client Service) and not an External Worker

Further, like Firm employees, External Workers are prohibited from making contributions (cash or in-kind) to political parties, party officials, or candidates for office on the Firm’s behalf or using the Firm name.

**Responding to requests for improper payments**

If someone suggests a potentially improper transaction (e.g., if there is reason to suspect a person may be suggesting a bribe, overtly or not, or if a third party offers to obtain a government approval in a surprisingly short time for an additional fee), you must

* Refuse to make the payment and explain that you are not authorized to make the payment or take such decisions on the Firm’s behalf
* Explain that it will be necessary for you to refer the request to the relevant partner, cell leader, or supervisor
* Immediately contact your Point of Contact and Firm Legal for guidance

## Monitoring and record keeping

To protect against and promptly detect potential corruption issues, the Firm's Finance and Internal Audit Departments will monitor transactions on an ongoing basis and conduct periodic testing and audits. Therefore, an External Worker must

* Ensure all charges or fees invoiced are supported by and in line with the details contained within their signed contract, SOW or NDA (type of document dependent on whether engaged directly or through a Supplier/Vendor)
* Provide a full explanation for any unusual or excessive charges
* Undertake any anti-corruption learning programs when requested to do so.

## Personal Investments

To safeguard the confidential information of our clients and the Firm’s reputation for integrity and professionalism, External Workers shall not during the term of their engagement with the Firm (and for such defined period thereafter as may be required by applicable law or as per your contract, SOW or NDA[[4]](#footnote-4)) undertake either of the following

* Trade in the securities of any Firm client to whom you provide services
* Trade in any company - or recommend to others trades in any company - about which you learn material non-public information in connection with the services.

Material Non-Public Information (MNPI) is any non-public information about a company or its securities that a reasonable investor would consider to be important in determining whether to trade in those securities. MNPI can relate to, but is not limited to, matters such as earnings estimates, the significant expansion or curtailment of operations, potential M&A transactions, regulatory or other legal proceedings, changes in senior management or R&D information.

If you have any questions about personal investments, please contact your Sponsor/Point of Contact, DCS or Firm Legal for help.

External Workers **must not** trade on any information that they learn whilst working with McKinsey.

# Personal safety and security

**Safety and Security**

The Firm is committed to ensuring that all Firm members and External Workers can work in safe and secure environments. Importantly, we also share a common responsibility to maintain the safety of these environments and of our co-workers.

**Working in the office**

* Protect our perimeter – don’t let unidentified individuals follow you into our offices. Politely direct them to reception/security. Restrict client visits to designated client areas and escort all visitors within offices at all times.
* Protect confidential information in physical form – don’t leave confidential information unattended on desks and shred any confidential documents which are no longer required.

**Safety in the office**

* If you see a hazard, alert office staff and block it off/put a sign in the area so others don’t get hurt
* Keep all work areas clear of clutter and walkways free of obstacles
* Attend all evacuation drills
* Know where the emergency features of the office are (exits, assembly points, extinguishers etc.).

**Travel bookings advice and approvals**

On occasion External Workers may be asked to travel on the Firm’s behalf. Some important safeguards exist:

* All Firm-related travel should be booked through the McKinsey travel office unless you are engaged through a Supplier/Vendor and are required to use their travel service
* Personal travel should not be booked through McKinsey Travel
* The Firm Security team ([Firm\_Security\_Team@mckinsey.com](mailto:Firm_Security_Team@mckinsey.com)) is available to provide travel advice to colleagues & External Workers travelling for the Firm
* If you travel on our behalf, you will have access to the services of International SOS and should request current membership information from HR
* Any travel to high or extreme risk locations (determined by McKinsey’s travel risk consultants) requires approval in advance by the relevant geographic leader as well as potentially the Client Service Risk Committee and Regional Leaders
* If in doubt about the risk rating of a location, contact the Firm Security team
* Travel to any countries subject to international sanctions should be syndicated by the relevant DCS with Firm Legal.

# Key contacts

Each of us is responsible for living McKinsey’s Mission and Values – if in doubt, contact others in the Firm for help/guidance:

* **Your McKinsey Sponsors or main Point of Contact**
* **Consultant Leaders** (e.g., Office/Location Manager*,* Practice Leader, DCS)
* **Firm Functions experts** (e.g., Legal, HR, Communications, Professional Development, IT*,* Firm Security, Professional Standards and Risk)
* **Professional Standards and Risk website[[5]](#footnote-5)**
* **Firm Risk contacts webpage[[6]](#footnote-6)**
* **Global Helpdesk;** if your McKinsey-enabled laptop or mobile device is lost or stolen or if you have a technical/IT issue.

**If you think you have triggered a risk or see a potential risk, tell someone immediately. It is much better to proactively engage the relevant personnel as quickly as possible than to let the situation worsen.**

# Conclusion

The Standards Guide for External Workers and the McKinsey Values and Mission highlight that each of us working with or for the Firm has an obligation to maintain the highest professional standards and to uphold the Firm’s reputation.

Firm Members and External Workers are responsible for applying the standards outlined in this document and for taking the responsibility to speak up and voice any questions or concerns related to possible violations.

This document is intended to be ‘living’ and will be regularly refined and updated.

# Appendix

## Firm Policies and Guidelines refenced in this document

**Client conflicts & confidentiality**

* Final Docs
* Information sharing
* Serving competitors
* Processing of Personal Data

**Client services & other arrangements**

* External Workers
* Direct Information Gathering
* PSE policy

**External Communications & use of name**

* Social media
* Use of name
* External Communications and publishing

**Physical & Information Security**

* Anti Malware protection
* Global Data Protection & Privacy
* Information backup and retention
* Information tech security and usage
* Remote Access Security
* Telecoms equip & services
* Wireless/mobile security
* Working from home security

**Personal conduct & finance**

* Anti-corruption
* Board Membership
* Ensuring an Environment Free from Discrimination and Harassment
* Violence in the workplace
* Personal Investments

**Travel & Entertainment**

* Travel safety
* General security & safety responsibilities

Standards guide for external Workers – confirming receipt

**I confirm I have received and read the document ‘Standards Guide for External Workers’**

**Printed Name:**

**Signature:**

**Date:**

1. Email: Global\_Helpdesk@mckinsey.com ; International direct dial: +1-212-798-0813; McKinsey VoIP phone: 313 [↑](#footnote-ref-1)
2. See ‘Get Smart about Security’ on the McKinsey Intranet [↑](#footnote-ref-2)
3. Click here to find your local Communications colleagues: <https://our-firm.intranet.mckinsey.com/ourfirm/firm-communications> [↑](#footnote-ref-3)
4. Please check your contract, SOW or NDA to note the applicable defined period during which the above restrictions apply [↑](#footnote-ref-4)
5. To access, go to the Global Intranet home page. Look for “Quick Links” on right hand side of window and click on Professional Standards. Or type “Professional Standards’ into the Internet Explorer web browser. If you do not have access to the website, please contact Professional\_Standards@mckinsey.com with your questions [↑](#footnote-ref-5)
6. Can also be found on the ‘Professional Standards and Risk’ webpage (see above footnote for how to find) [↑](#footnote-ref-6)