McKinsey & Company

Information Security Program Overview

Date of last review/update: March 4, 2025

Table of Contents

1. Introduction

One of McKinsey & Company's foundational values is protecting information, including personal data, and the McKinsey's information technology (IT) resources that store, transmit and process that information, against incidents that might compromise its confidentiality, integrity, and availability in an accidental, unlawful or unauthorized way and against all other unlawful forms of processing. Accordingly, the Firm has implemented the following technical, organizational and physical security measures to provide an appropriate level of information protection that considers the risks presented by the processing and the nature of the information to be protected, as well as the state of the art and the cost of their implementation. This document presents an overview of the digital information security measures and standards that McKinsey applies globally.

McKinsey may update these technical, organizational and physical measures from time to time, without notice, as long as such changes do not materially lower the protection of information and are not materially inconsistent with the protections described to its clients.

2. Requirements

2.1 Review and update process

Firm information security policies and standards are subject to periodic review, to ensure that they address new technologies and threats.

Changes to existing and the creation of new policies and standards are subject to review and approval by Firm leadership. All Cyber Risk-related policies are reviewed and approved by vote of a senior oversight committee.

2.2 Communication of policies to employees

McKinsey's employees and contractors with access to McKinsey systems and information (further called "McKinsey Personnel"), are made aware of and must comply with the information security policies and standards.

Exceptions to Firm policies and standards must follow an established exception management process for approval and documentation.

2.3 Consistency with industry best practices

Firm measures reflect (a) the principles set forth in the publication "ISO/IEC 27001:2013 – Information technology – Security techniques – Information

security management systems – Requirements"; and (b) industry best practices as ascertained from the review of appropriate publications and consultation with recognized industry experts. In addition, systems and information designated for special handling, such as healthcare or government data, comply with additional standards.

Annually, an independent third-party assesses the Firm's information security organization and its information security management program.

2.4 Management of the information security program

An advisory committee made up of senior stakeholders provides guidance, counsel and strategic oversight on key security and related compliance issues affecting McKinsey.

The Firm's information security program is led by the Chief Information Security Officer, who is accountable for its execution and continuous improvement.

Specialized teams are responsible for managing the Firm's standards for security, addressing cybersecurity risks, providing security operations across the technical estate, and providing teams and leaders with security intelligence.

2.5 Training and awareness

McKinsey personnel must complete cyber security training. This training covers some topics, such as:

- Routine phishing simulations.
- Periodic cybersecurity training on key topics (e.g., social engineering, business email compromise, safe use of devices).
- Professional Standards and Risk program, which includes the requirements to keep Confidential Information secure and confidential during their assignment and thereafter.

The Firm publishes information on cybersecurity, data privacy essentials and workplace security on its intranet.

2.6 Human resources security

McKinsey Personnel are required to sign a confidentiality agreement, which requires all colleagues to appropriately handle and protect confidential information and abide to the Firm's policies.

To the extent legally permissible, Firm Personnel and external workers are subject to background checks.

2.7 Office security controls

In addition to technical security controls, McKinsey has implemented the following:

- Firm premises are subject to controls that limit physical access to Firm personnel and approved third-party service providers and visitors.
- McKinsey offices require visitors to register with the lobby receptionist where visitor logs are maintained. After visitors register at the reception desk, Firm personnel escort them into the premises, where their access is restricted to a dedicated visitors' area, which does not hold client confidential information and is physically separated from the Firm workspace.
- Printed materials containing client confidential information must be secured in locked cabinets, drawers, safes, or other enclosures when not being used or under the control of personnel. The Firm has implemented a clean desk and clear screen policy.

2.8 Data classification

To be able to take appropriate measures to protect data residing on its systems, the Firm has adopted a matrix that establishes classification levels based on the sensitivity of the data. For each level, the Firm specifies appropriate handling and storage controls that protect confidentiality and integrity, with the most stringent controls assigned to the highest data classification level, and when required by law, regulation, or industry standards.

2.9 IT acceptable use guidelines

The Firm has an Acceptable Use of Technology Policy for McKinsey personnel. This policy applies to all members of McKinsey & Company and provides guidelines for the appropriate use of technology equipment and services provided by the firm. The policy covers the use of firm-issued laptops and mobile devices, email and messaging applications, password security, content filtering, investigations, connectivity, and security when working remotely. Users are responsible for complying with the policy and may face consequences for non-compliance

The Firm’s Code of Conduct defines a set of expectations for the behavior of all Firm members regarding the protection of data. Failure to comply with

internal policies may result in disciplinary action including termination of employment.

The Firm has risk-based procedures in place to lawfully review, monitor, and/or disclose information communicated via its IT resources to prevent, detect, investigate, and mitigate any activity that affects the security of its systems or Firm and client information, or conflicts with its policies or with applicable law or regulation.

Users are required to employ the mandated security controls to protect the information stored in or transmitted through IT resources assigned to them.

Users are instructed to ensure that internal emails, images or documents containing Firm or confidential information are not sent to personal (non-Firm) email accounts or to any unauthorized recipient inside or outside the Firm.

Users are prohibited from using unapproved software or services for the transmission of confidential information.

When working outside of McKinsey facilities, traveling or on a client location, users are required to maintain appropriate levels of security and privacy including following best practices for using Firm-supported devices, locking computers and safeguarding confidential information, and taking precautions to protect equipment against theft. Users must report lost or stolen devices immediately to the Global Help Desk (GHD).

Data storage devices such as: laptop hard drives, mobile device storage, and removable drives, employ full-disk encryption with strong cryptographic algorithms such as AES256.

Users are instructed to only use Firm standard encrypted device when storing confidential client or McKinsey data.

2.10 Authentication and access management

The Firm’s policy is to grant users only that level of access to data that is appropriate to their role and responsibilities.

Access controls are driven by the following three principles:

- Default to deny: All access not explicitly permitted/granted should be denied by default.
- Need to know: Access to data should be granted only if the recipient has a legitimate business need to access the data.
- Least privilege: Users should be assigned the minimum level of access necessary to fulfill their job responsibilities.

McKinsey honors the principle of segregation of duties to reduce opportunities for unauthorized modification or misuse of information or services, for example developer vs. tester or reviewer.

The Firm implements a password policy that reflects the requirements of NIST SP800-63-3, and as such it must satisfy the following criteria:

- Must be unique to McKinsey.
- At least twelve (12) characters long.
- Must satisfy a password complexity check:
- Cannot contain predictable words or phrases, keyboard patterns, or character substitutions.
    - Cannot contain the user's first or last name.
    - Must be different from the prior eight (8) passwords.
- Must use multi-factor authentication to access applications hosting confidential data.

Firm devices, applications, and systems are configured to automatically log off or lock the user's session if there is no keyboard, mouse, or touchscreen activity for a defined timeout period.

Access to Firm computers and mobile devices is disabled after ten (10) consecutive unsuccessful logon attempts.

Procedures have been implemented to disable and remove accounts no longer in use in the McKinsey environment. User accounts are disabled after 90 days of inactivity and deleted after 180 days. Service accounts are disabled after 180 days of inactivity, and disabled service accounts are automatically deleted 90 days after disablement.

When McKinsey personnel separate from the Firm, access to digital information, including access to computing and communications resources that may store or process information, is terminated in accordance with a documented and automated process.

2.11 Change management

The Firm's change management process has been designed to minimize the impact on operational stability, ensure transparency around change activities, account for rollback procedures, and promote efficiency and agility for both standard and emergency changes.

2.12 Data centers

To protect digital information at rest, in-transit, and in use, the Firm's IT infrastructure is designed and managed to adhere to industry best practices. These measures include the following:

- McKinsey leverages multiple geographically dispersed Tier III data centers with 24x7x365 on-site operations.
- Electrical power is protected by uninterruptible power supply (UPS) and diesel generators.
- McKinsey-employed data centers are highly resilient Tier III level colocation or cloud-based facilities that hold ISO 27001 certifications and SOC2 Type 2 reports.
- Physical access is granted to only those individuals with a legitimate business need. Data centers are physically protected by multiple layers of security including biometric access controls, CCTV cameras, and on-site security officers.
- Data is not permitted to leave the data centers unless it is protected by strong encryption such as AES256, either on encrypted tapes or other encrypted portable media, or transmitted via encrypted telecommunications channels.

McKinsey has implemented measures to ensure that information collected for different purposes is processed separately including, as appropriate and without limitation, adequate logical separation of Confidential information (e.g., internal client capability/purpose limitation).

2.13 Software and network

McKinsey products and networks use firewalls, filters, access-control lists, intrusion-detection software, anti-malware software, and encryption to protect against external digital threats and from unauthorized interception, monitoring, or modification.

There is an established secure development lifecycle process for product development, which employs multiple testing procedures (including design and code reviews, as well as functional and penetration tests) to mitigate potential vulnerabilities before the product goes live, and periodically thereafter.

Segregation of environments is in place (production and non-production) and promotion from non-production environments into the production environment must follow an established change management process.

McKinsey secures access to its non-public wireless networks within its offices through security controls that include enterprise authentication, strong cryptographic algorithms such as AES 256-bit, and multi-factor authentication (MFA).

Servers and network devices undergo vulnerability scanning on a periodic basis. Findings are classified into risk categories (critical, high, medium, low) which have patching time frames to address and/or patch within the time frame associated with the respective category.

The Firm engages a third-party to conduct penetration tests for applications and networks and performs remediation for findings based upon the level of criticality. On-going scanning for unauthorized devices is conducted by using a Wireless Intrusion Prevention System (WIPS) to provide wireless intrusion scanning capabilities, enabling detection and classification of different types of wireless threats, including rogue access points and wireless hackers. McKinsey's standards require removal of orphan assets identified in the on-prem network within a pre-defined time period.

Production data is not permitted to be used for test purposes in non-production environments, unless the non-production environment implements at least the same security controls as the production environment and enforces a need-to-know access policy, or the data is masked or sanitized first.

2.14 End-user computer and communication devices

The following measures are used to protect information stored on end-user computing devices:

- Endpoint devices are encrypted using strong cryptographic algorithms such as AES-256-bit.
- Endpoints are protected to guard against malware, spyware, and malicious attacks. On-access scans on programs and files and daily scheduled scans are performed. Malware signatures are pushed multiple times a day.
- Only McKinsey-approved devices may be connected to McKinsey's private networks. Visitors can connect to a guest network isolated from the private ones.
- Emails routed in and out of Firm mail servers are scanned and protected by our secure email relay.
- The drives and other non-volatile memory of mobile devices that have been lost or stolen, or that may be the target of malicious attempts to

access or compromise the device or any part of the McKinsey network, will, where technically feasible, be remotely wiped.

- Asset management processes are in place to identify, track and maintain in scope and Firm-owned hardware, software and IT infrastructure.

2.15 Third-party service providers

Third-party service providers are required to enter into agreements with the Firm that subject them to non-disclosure agreements, data protection and security controls that are no less stringent than those described in this document.

Before a third-party vendor may host or process data, the vendor’s security controls are assessed. Vendors are classified by 4 different levels of criticality, and are assessed periodically, as required by their respective tier.

McKinsey conducts security reviews on infrastructure managed by third parties to ensure that the provider adheres to Firm security standards. Security reviews may include an annual review of certifications, penetration testing and audit reports. McKinsey's vendor management review and approval process for cloud service providers includes completion and review of a data protection and security questionnaire and related supporting documents.

McKinsey uses third-party infrastructure providers, including AWS and Azure, to host solutions. McKinsey’s collaboration tools used during engagements include Box and Microsoft 365.

2.16 Business continuity and disruption resiliency

Business Continuity (BC) and Disruption Resiliency (DR) plans enable McKinsey to continue its business operations following a natural or manmade disaster or other major event affecting McKinsey operations, systems, and/or data.

Business Impact Analysis (BIA) is performed to identify critical processes and services to ensure they are restored in accordance with their classification, priority, and technical dependencies.

McKinsey is designed to operate as a single global firm. It has consulting and support staff based in offices around the world all of whom are highly mobile and available to deploy at extremely short notice to support clients.

The Firm has implemented plans for its largest offices; these plans are reviewed periodically. In addition, scenario exercises are conducted at its largest and higher risk locations.

Based on recovery objectives, DR Tiers are assigned to products:

- **Recovery Point Objective (RPO)** is the point in time to which the technology system state and data are recovered to after a disruption event.
- **Recovery Time Objective (RTO)** is the overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes.
- Firm Standards require that resilience testing is conducted annually, at a minimum.

The following measures have been put in place to mitigate the effects of such events:

- Products are being migrated to or built in the cloud, to take advantage of the resilience that cloud providers offer.
- Critical products are designed to be highly redundant and available, and utilize advanced fault-tolerant features and components.
- Each data center can be leveraged as a recovery site. If a major event impacts one facility, applications and services can be recovered to one of the remaining facilities using manual or automated procedures, or leveraging cloud providers' capabilities. Failover capabilities ensure that the infrastructure will be operational.
- DR backups can be used to bring applications back online and restore their data in case of a disaster.

2.17 Security incident management

McKinsey's Cyber Security Incident Response Plan (CSIRP) provides a formal and coordinated approach for responding to cyber security incidents affecting data and information assets.

McKinsey's Security Operations Center (SOC) provides cyber defense and response services involving threat intelligence fusion, threat detection and analysis, and incident response. The SOC maintains records and a final report and manages identified security incidents in accordance with the CSIRP to allow for recovery and future protection.

The firm's SOC is authorized to declare a cyber security incident and engage the Cybersecurity Incident Response Team (CSIRT) for the response and recovery of impacted Firm information systems.

Security incident responses follow documented response procedures, which includes review by members of the CSIRT. Incidents are classified according to a predefined set of criteria, taking into account, among other things, (a) the nature, date, and time of the security incident; and (b) the confidential information and information systems affected by the security incident.

After an initial review of an incident, the CSIRT will coordinate with additional Firm functions, such as Legal, Privacy, and Human Resources, as appropriate.

If an employee discovers a security incident, they are required to notify the Global Help Desk (GHD) or SOC.

Where a Security Incident impacts data owned by its clients, McKinsey will notify the client without undue delay and in accordance with the Client agreement.

2.18 Data retention

According to McKinsey's professional archival policy, the final engagement records (e.g., proposals, contracting documents, invoices, client deliverables, key communications and key supporting data and documents) will be archived and subsequently deleted by policy on the expiration of McKinsey's retention requirements, unless such requirements have been extended due to legal obligations or as otherwise authorized or instructed by the client.

Copies may still exist temporarily on encrypted, access-restricted backup systems, including where required by applicable law.

For data owned by a McKinsey client, retention shall be consistent with the safeguards discussed in this document and the representations made in the Client agreement.

2.19 Compliance with data privacy laws

McKinsey's global data privacy management program is based on well-recognized data privacy principles that are incorporated into global privacy laws, including the EU General Data Protection Regulation (GDPR). When McKinsey handles personal data in a Client engagement ("Client Data"), it applies policies and processes based on those data privacy principles to comply with applicable data privacy laws, including GDPR, the California Consumer Privacy Act (CCPA) and its successor, the California Privacy Rights Act (CPRA) and, for Protected Health Information (PHI), the Health Insurance Portability and Accountability Act (HIPAA), the Personal Information Protection Law of China (PIPL) and to provide guidance in situations where no privacy laws exist.

Where McKinsey is involved in data transfers, in particular, when Client Data is transferred to or accessed from another country, the following additional technical, organizational and contractual measures are applied:

- Technical Measures: Data in transfer between or stored at McKinsey operations will be encrypted in transit and at rest based on robust encryption algorithms such as AES256, implemented by properly maintained software, providing protection against active and passive attacks, including by public authorities, and does not contain back doors in hardware or software.

- Organizational Measures: Maintaining policies and procedures related to Client Data to address privacy and data risk management issues, including data minimization, de-identification, confidentiality, data security and data access requests, including from public authorities.

- Contractual Measures: McKinsey agrees contractually that is has not and will not purposefully create back doors or similar programming in its information technology system to facilitate government or other unauthorized access to Client Data or change its business processes to facilitate access to Client Data. To the best of McKinsey's knowledge, no applicable national law or government policy requires McKinsey to create such backdoors or provide direct access to Client Data and other Confidential Information or provide an encryption key without a valid legal request or order.

Where McKinsey engages third-party providers as sub-processors for the processing of Client Data, McKinsey will ensure that its sub-processors are required to implement security controls no less stringent than those set forth herein, are subject to a legally recognized transfer mechanism, and are bound by written agreements reflecting the same. A list of McKinsey's current sub-processors, which shall be updated when there is any addition, deletion or change in the sub processor list, can be accessed at https://solutions.mckinsey.com/msd/subprocessors/. McKinsey has implemented a notification mechanism under the link above to receive notifications of new sub-processors, which shall be considered as a valid method to notify any change in the list of approved sub-processors. If the Client does not approve of any new sub-processor within fourteen (14) days, such approval not to be unreasonably withheld, then Client shall notify McKinsey of such determination and the parties agree to work together in good faith to resolve such concerns. To the extent that they cannot be resolved, McKinsey shall either cease its use of the sub-processor to process the Client Data or notify the Client that it may terminate that portion of the services that require the use of the sub-processor in accordance with the terms set forth in the agreement pursuant to which such Services are provided.

McKinsey keeps assessment reports, and updates those, when necessary, with respect to surveillance laws and privacy practices of countries where McKinsey processes Client Data and which are not formally recognized as providing adequate protection of fundamental rights to individuals. On Client request, McKinsey will provide a copy of the relevant assessment report.

If permitted under applicable law, McKinsey will inform the Client of any requests of a government related to Client Data. If McKinsey is not permitted under applicable law to inform the Client, McKinsey will take reasonable steps to get judicial leave to inform the Client at the earliest possible time or request that the government authority will inform the Client directly. When McKinsey believes those government requests may be unlawful, McKinsey will take reasonable steps to challenge requests in court or in administrative proceedings.

Onward transfers of Client Data will only take place as agreed with the Client in the Client agreement or as otherwise allowed by law.

Compliance with laws: McKinsey will notify the Client, if it can no longer meet its obligations under any applicable law related to the processing or transfer of Client Data based on the agreement with the Client, for example in case of changes in the applicable law.

Selling or Sharing of Confidential Information: McKinsey will not sell or share Client Data, except as agreed with the Client in the Agreement or required by law.

McKinsey will allow a Client impacted by a regulatory request for Client Data to verify McKinsey's response to the request during an inspection or audit, consistent with the terms of the applicable Client agreement if Client Data was disclosed to public authorities. If an individual directs an "individual rights request" respecting his or her personal data to McKinsey, McKinsey will direct this individual to the Client and will provide support so that the client can meet its data privacy obligations.