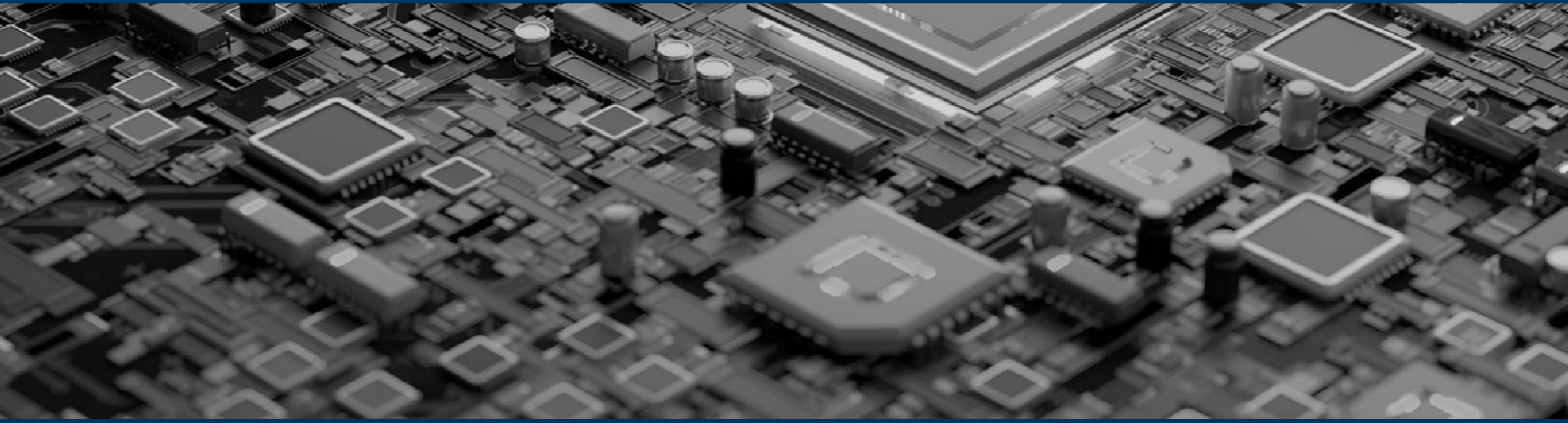

CLIENT SECURITY STATEMENT

Version 11.0 | October 2024

© 2024 Goldman Sachs. All rights reserved.

Table of Contents

No part of this material may be (i) copied, photocopied or duplicated in any form by any means or (ii) redistributed without our prior written consent. This material is for informational purposes only and is not intended to form the basis of any investment decision and should not be considered as a recommendation by Goldman Sachs & Co. LLC, its subsidiaries or affiliates (collectively, "Goldman Sachs" or "we"). This material does not constitute an offer to provide advisory or other services by Goldman Sachs. Nothing herein is an offer or promise to procure any product or service or to make an investment in any entity.

This document applies to the Goldman Sachs Group Inc. (the "firm"), its affiliates; and its subsidiaries, and supersedes all prior statements, commitments, agreements, and writings with respect to the subject matter hereof and all such have no further force or effect.

Introduction

Goldman Sachs places great importance on information security, including cybersecurity, to protect against external threats and malicious insiders. The firm's cybersecurity strategy prioritizes detection, analysis and response to known, anticipated or unexpected cyber threats, effective management of cyber risks, and resilience against cyber incidents. Goldman Sachs does not embrace a one-size-fits all approach. Each organization within the firm has both common and unique risks, as well as varying risk appetites and tolerances, specific missions, and objectives to achieve those missions. The firm continuously strives to meet or exceed current industry standard information security practices as they evolve over time and applies controls to protect our clients and the firm. Goldman Sachs maintains a formal cybersecurity program based upon the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and the related Cyber Risk Institute Profile.

This document provides an overview of the firm's approach to information security and cybersecurity, and its practices to secure data, systems, and services, which align to the six functions of the NIST CSF: Govern, Identify, Protect, Detect, Respond and Recover.

While information security and cybersecurity measures will naturally change over time and may differ across the range of Goldman Sachs' services, this document provides an overview of the firm's security practices. Goldman Sachs does not represent that this document will be appropriate or adequate for your intended purposes.

Please contact your Goldman Sachs representative if you have any additional questions.

GOVERN

Risk Governance and Oversight

Risk Governance Framework

The firm has established an enterprise risk management framework that employs a comprehensive, integrated approach to risk management and is designed to enable comprehensive risk management processes through which risks are identified, assessed, monitored and managed. The firm's risk management structure is built around three core components: governance, processes and people.

The firm's revenue-producing units, as well as Treasury, Engineering, Human Capital Management, Operations, and Corporate and Workplace Solutions, are considered the first line of defense. They are accountable for the outcomes of the firm's risk-generating activities, as well as for assessing and managing those risks within the firm's risk appetite.

The firm's independent risk oversight and control functions are considered the second line of defense and provide independent assessment, oversight and challenge of the risks taken by the first line of defense, as well as lead and participate in risk committees. Independent risk oversight and control functions include Compliance, Conflicts Resolution, Controllers, Legal, Risk and Tax.

Internal Audit is considered the third line of defense, and the director of Internal Audit reports to the Audit Committee of the Board and administratively to the Chief Executive Officer. Internal Audit includes professionals with a broad range of audit and industry experience, including risk management expertise. Internal Audit is responsible for independently assessing and validating the effectiveness of key controls, including those within the risk management framework, and providing timely reporting to the Audit Committee of the Board, senior management and regulators.

The three lines of defense structure promotes the accountability of first line risk takers, provides a framework for effective challenge by the second line and empowers independent review from the third line.

Each of the firm's divisions is ultimately accountable for managing technology risks affecting their applications and other information system assets.

Governance Committees

The Board of Directors, both directly and through its committees, including its Risk and Audit Committees, oversees the firm's risk management policies and practices, including cybersecurity risks, and information security and cybersecurity matters. The firm's Chief Risk Officer, Chief Information Officer (CIO) and Chief Technology Officer, among others, periodically brief the Board on operational and technology risks. The Board also receives regular briefings from the Chief Information Security Officer (CISO) on a range of security topics, including the firm's Information Security and Cybersecurity Program ("Program"), evolving cybersecurity risks, emerging cybersecurity threats, mitigation strategies and related regulatory engagements. The Board maintains ongoing dialogue and oversight of risk management with senior leadership.

The CISO is responsible for managing and implementing the Program and reports directly to the CIO. The CISO oversees the Technology Risk Division, which assesses and manages material risks from cybersecurity threats, sets firmwide control requirements, assesses adherence to controls, and oversees incident detection and response.

GOVERN

In addition, the firm has a series of committees that oversee the implementation of the cybersecurity risk management strategy and framework. These committees are informed about cybersecurity incidents and risks by designated members of Technology Risk and Operational Risk, who periodically report to these committees about the Program. These committees enable formal escalation and reporting of risks, presented by the CISO and Technology Risk leadership .

The following are the primary committees and steering groups that oversee the Program:

- The Firmwide Operational Risk and Resilience Committee (FORRC) is globally responsible for overseeing operational risks and seeks to ensure the business and operational resilience of the firm. This Committee is co-chaired by the firm's Chief Administrative Officer for EMEA and the head of Operational Risk.

- The Firmwide Technology Risk Committee (FTRC) reviews matters related to the design, development, deployment, and use of information technology. This committee oversees cybersecurity matters as well as information technology risk management frameworks and methodologies, and monitors their effectiveness. This Committee is co-chaired by the firm's Chief Information Security Officer and the Chief Technology Officer.

- The Digital Risk Office (DRO) Steering Group is a subordinate group under the FTRC, with the mandate to oversee Engineering risks. The DRO provides strategic oversight and direction of the Technology Risk portfolio and streamlines escalation and decisions while sharing information across pillars on key initiatives. This group is co-chaired by the firm's Chief Information Security Officer and the Chief Technology Officer.

Information Security and Cybersecurity Program

The firm's cybersecurity risk management processes are integrated into the overall risk management processes. The firm has established an Information Security and Cybersecurity Program ("Program"), administered by Technology Risk within Engineering, and overseen by the CISO. The Program is designed to identify, assess, document and mitigate threats, establish and evaluate compliance with information security mandates, adopt and apply the security control framework, and prevent, detect and respond to security incidents. The Program is periodically reviewed and modified to respond to changing threats and conditions.

A dedicated Operational Risk team, which reports to the Chief Risk Officer, provides oversight and challenge of the Program, independent of Technology Risk, and assesses the operating effectiveness of the Program against industry standard frameworks and Board risk appetite-approved operational risk limits and thresholds. The firm's process for managing cybersecurity risks includes the critical components of the risk management framework, as well as the following:

- Training and education, to enable personnel to recognize information and cybersecurity concerns and respond accordingly;

- Identity and access management, including entitlement management and production access;

- Application and software security, including software change management, open-source software, and backup and restoration;

GOVERN

- Infrastructure security, including monitoring the network for known vulnerabilities and signs of unauthorized attempts to access firm data and systems;
- Mobile security, including mobile applications;
- Data security, including cryptography and encryption, database security, data erasure and media disposal;
- Cloud computing, including governance and security of cloud applications, and software-as-a-service data onboarding;
- Technology operations, including change management, incident management, capacity and resilience; and
- Third-party risk management, including vendor management and governance, and cybersecurity and business resiliency on vendor assessments.

Internal Audit

The firm's Internal Audit division is an independent function that reports to the Audit Committee of the firm's Board of Directors. Internal Audit independently assesses the firm's overall control environment and raises awareness of control risks. Internal Audit also communicates and reports on the effectiveness of the firm's governance, risk management and controls that mitigate current and evolving risks, while monitoring the implementation of management's control measures.

Regulatory Oversight and External Audit

The firm is regulated by numerous authorities in all jurisdictions in which we operate, including (but not limited to):

- Americas: The U.S. Federal Reserve System, New York State Department of Financial Services, U.S. Commodity Futures Trading Commission, U.S. Securities and Exchange Commission, U.S. Consumer Financial Protection Bureau;
- Europe, Middle East and Africa: The European Central Bank, European Banking Authority, U.K. Financial Conduct Authority, the German Federal Financial Supervisory Authority, the Saudi Arabian Capital Markets Authority, the South African Reserve Bank, the U.A.E. Securities and Commodities Authority;
- Asia Pacific: The Monetary Authority of Singapore, the Japan Financial Services Agency, the Australian Securities and Investments Commission, and the Hong Kong Monetary Authority.

PricewaterhouseCoopers LLP (PwC), an external auditor, performs Service Organization Control (SOC) 1 and 2 assessments for select firm businesses and independently tests applicable controls.

GOVERN

Industry Engagement

Goldman Sachs is a founder or leading participant in many relevant industry initiatives both domestically and internationally. In the United States, these partnerships include the Financial Services Sector Coordinating Council (FSSCC), the Financial Services – Information Sharing and Analysis Center (FS-ISAC), the National Cyber-Forensics and Training Alliance (NCFTA), the Cyber Risk Institute, the Analysis and Resilience Center (ARC) for Systemic Risk, and the Sheltered Harbor initiative.

The firm maintains direct relationships with government entities globally. In the United States, the firm actively collaborates with the Federal Bureau of Investigations (FBI), the Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA). The firm also engages with international partnerships, such as the Cyber Security Information Sharing Partnership (CiSP – UK) and the Computer Emergency Response Team (CERT - India).

The firm additionally participates in industry efforts to manage technology risks, including those coordinated by the Securities Industry and Financial Markets Association (SIFMA), Asia Securities Industry and Financial Markets Association (ASIFMA), Association for Financial Markets in Europe (AFME), Bank Policy Institute (BPI), the American Bankers Association (ABA) and the Australian Financial Markets Association (AFMA).

Information Security and Cybersecurity Policies and Standards

Policies and Standards

The firm maintains information security and cybersecurity policies and standards that take into consideration information security and cybersecurity, data privacy laws and regulations that are applicable to jurisdictions in which the firm operates.

Policies and standards are reviewed and approved by relevant firmwide governance bodies. The firm's Global Information Security and Cybersecurity Program and Policy are reviewed annually. Other firm policies and standards are reviewed at least every three years, in accordance with the firm's periodic review requirements. Additional reviews may be triggered by changes in the risk environment or regulatory landscape.

A dedicated policy governance group, consisting of representatives from each of the firm's divisions, maintains the process to develop, review, update, and decommission information security and cybersecurity policies and standards.

Firm policies and standards are based upon recognized industry standards, including those defined by the National Institute of Standards and Technology (NIST), the Federal Financial Institutions Examination Council (FFIEC), and the Cyber Risk Institute.

Firm policies and standards are available to personnel through an internal compendium.

IDENTIFY

Risk Assessment

Risk Assessment

Goldman Sachs believes the identification of risks and related control assessments is a critical step in providing the Board and senior management with transparency and insight into the range and materiality of risks facing the firm. The firm has a comprehensive data collection process, including firmwide policies and procedures that require personnel to report and escalate risk events. The firm's approach for risk identification and control assessment is comprehensive across all risk types, is dynamic and forward-looking to reflect and adapt to the changing risk profile and business environment, leverages subject matter expertise, and allows for prioritization of the most critical risks. This approach also encompasses the control assessment, led by the second line of defense, to review and challenge the control environment and to help ensure it supports the firm's strategic business plan.

The firm performs risk assessments to gauge the performance of the Information Security and Cybersecurity Program, to estimate the firm's risk profile and to assess compliance with relevant regulatory requirements. The firm performs periodic assessments of control efficacy through the internal risk and control self-assessment process, as well as a variety of external technical assessments, including external penetration tests and "red team" engagements where third parties test the firm's defenses. The results of these risk assessments, together with control performance findings, are used to establish priorities, allocate resources and identify and improve controls.

Asset Management

Technology Asset Inventory

The firm maintains asset information for hardware in managed inventories throughout its lifecycle; such inventories are used to track each asset's attributes. Inventory management comprises manual processes and controls, including the asset's onboarding process, periodic reviews, and is governed by policies and standards.

Assets, which may include hardware, software or virtual assets like virtual machines, are assigned owners to assist in governance. The firm's applications include classifications based on their inherent risks.

PROTECT

Training and Awareness

Training and Education

The firm maintains a cybersecurity training program, which is designed to help personnel recognize information and cybersecurity concerns and respond accordingly. This program is designed to help provide personnel with the knowledge and skills to prevent, identify, and escalate cybersecurity risks.

Annual information security and cybersecurity training is required of firm personnel who access firm technology, e.g., full-time and part-time employees, and contractors. Additional training is provided for new joiners and individuals transferring within the firm. The firm conducts regular exercises on personnel to educate them on email-based cyber threats and appropriate escalation.

The firm incorporates training themes based on regulatory guidance, current industry standard practices as they evolve over time, and changes in the risk environment.

The firm additionally provides technical training to engineering personnel via specialized platforms. This training includes topics focused on information security, such as secure coding principles and updates on emerging threats.

The firm maintains processes to track, measure and escalate personnel who fail to complete mandatory training, including cybersecurity training.

Identity and Access Management

User Identity Management

The firm's access controls are based on the general principles of no privilege without identity, no privilege without approval, and least privilege access. Entitlements are provisioned to be commensurate with role or job duties.

As permitted by local law, firm policy requires background checks on employees, consultants and contractors who have access to firm systems, firm or client non-public information or unescorted access to firm premises. Worker identity is subsequently verified at the initiation of employment. Prior to joining, the firm's personnel sign a non-disclosure agreement that requires them to abide by the firm's policies to protect client information.

A unique digital identifier and physical access card are assigned to all personnel requiring access to firm-managed digital or physical spaces. Personnel are prohibited from sharing their individual access cards and credential information, including usernames and passwords.

PROTECT

Entitlements Management

Authentication and authorization are required for high-risk applications. Entitlements associated with critical and sensitive applications are required to be reviewed by management at least annually. More frequent reviews may occur for privileged access. Entitlements may also be revoked and/or reviewed when personnel transfer to new roles or departments within the firm.

The firm maintains a segregation of duties program as a part of its internal control framework. Segregation of duties requires that the same individual is not in a position to initiate, approve, and reconcile the same critical transaction or process. An automated system is used to monitor entitlement stores and identify violations in segregation of duty requirements.

When a worker leaves the firm, access to the firm's facilities and general access to the information systems are revoked.

Access Controls

The firm maintains defined password requirements documented in a formal standard. Password requirements include establishment of a new password at initial login, minimum password length, alphanumeric composition, password expiration after indications of compromise, maximum number of unsuccessful login attempts before lockout, a password history and an inactivity lockout. In addition, passwords cannot match common dictionary words or other common patterns or phrases.

When required, data segregation is accomplished through logical segregation with data-level access controls. Administrative access to systems that store, transmit or process client non-public information data must be approved by authorized managers.

The firm maintains strict controls over access to production environments, including access authorizations, logging, and time limits on access. As part of the firm's segregation of duties, access by technology staff to production systems requires pre-approval before access is granted. In addition, production access is limited to authorized individuals, time-bound, subject to logging and periodic review, limited to necessary functions, and regularly monitored. Changes made to production environments are subject to mandatory reviews.

The firm requires multi-factor authentication (MFA) for remote access by GS personnel to the firm's network and for internet-facing applications that store, transmit or process firm or client non-public information.

Application and Software Security

Centralized Inventory and Risk Classification

The firm leverages a centralized inventory to record key information about applications. Applications are required to complete a risk profile to determine regulatory and risk-based requirements. Accordingly, each application is assigned one or more risk classifications, which in turn are associated with specific required controls and resiliency thresholds.

Risk classifications are required to be reviewed and updated on an annual basis. Risks identified through annual and quarterly assessments are recorded in centralized inventories that detail key information about applications.

PROTECT

Software Development Controls

The firm has a formal Security Software Development Lifecycle (SSDLC) process, which is documented and incorporates appropriate control gates. Application security requirements and associated assessments are incorporated throughout the SSDLC on a risk-adjusted basis. Examples of SSDLC and related application security controls include design reviews, code reviews, penetration testing, and use of Dynamic Application Security Testing (DAST) scanners. Detective and preventative controls make use of Static Application Security Testing (SAST), identification of vulnerable dependencies, and infrastructure-as-code scanning.

Firm procedures require that production changes undergo testing and receive authorized approvals.

Several applications in use throughout the firm are developed internally. Comparable application security standards are applied to internally developed applications, open-source software components, and third-party software deployed on the firm's infrastructure.

Firm policy provides that sensitive data must be masked, or subject to other equivalent controls, prior to being used in nonproduction environments. Controls are implemented based on the risk profile of the application, in adherence to legal, regulatory, or contractual data protection requirements.

Security Testing

The firm conducts annual penetration tests, as well as red team, joint offensive-defensive team (commonly referred to as "purple team") and hunt team assessments to discover and evaluate the security of applications and infrastructure, focusing on high-priority themes and risks. Internet-facing applications are regularly scanned using DAST tools.

The firm maintains a Bug Bounty and responsible disclosure program, covering a majority of public Goldman Sachs sites, which allows researchers to report vulnerabilities through a dedicated portal.

The penetration testing methodology used by the firm internally and by the firm's vendors is based on several published industry guidelines such as the CREST STAR/CBEST Implementation Guide, NIST SP800-115, and the OWASP Testing Guide. The approach combines manual and automated assessment techniques and the use of proprietary, commercial and open source assessment tools in a consistent and repeatable process.

Infrastructure Security

Change Management

The firm maintains change management processes to protect the integrity and availability of the firm's technology products and services, minimize change-related incidents and enhance operational practices.

PROTECT

Production infrastructure changes are managed using firm-approved change management systems and recorded. Changes must undergo risk assessments, tested in non-production environments, and verified, prior to applying changes to production systems. Testing results must also be recorded.

Firm standards require that changes are recorded and authorized by designated approvers prior to deployment to the production environment.

Change implementations must be verified to ensure only intended changes have been made. The results of the change verification must be documented and retained in firm-authorized change management systems, per the firm's retention policy.

Configuration Management and Hardening

The firm employs configuration management to validate from a security perspective that firm systems continue to perform consistently in accordance with the Information Security and Cybersecurity Program.

Firm systems are hardened on a risk-adjusted basis to meet or exceed industry standards and deployed using standard security practices, such as restricted file access permissions and logging.

Hard drives on firm-provided laptops, which are only used for a small number of specific business purposes, are encrypted using industry standard tools.

An inactivity screen lock is enforced by a configuration policy on endpoints administered by the firm.

Network Security

The firm's network environment is designed to emphasize security and resilience, including through the implementation of a tiered architecture separated by firewalls and other controls.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are deployed at the network perimeter to monitor for and block malicious activity.

Management interfaces on perimeter firewalls, routers and other devices are not accessible from the Internet. The firm subscribes to continuous Distributed Denial of Service (DDoS) monitoring and mitigation services from multiple service providers. In addition, the firm hosts its primary Internet web presence on Content Delivery Networks with DDoS mitigation and absorption capacity, which implements network request throttling to limit the number of referrals and requests made by client IP addresses. Alerts generated by DDoS activities are monitored and mitigated as needed.

Access to the firm's IT infrastructure is restricted to authorized users and devices and established through network access patterns such as secure virtual desk or virtual private network solution.

PROTECT

System Monitoring, Capacity and Vulnerability Management

The firm maintains a capacity management program, which establishes documented processes for defining capacity objectives, scope, and requirements for key business services and related dependencies.

The firm's vulnerability management program includes frequent network vulnerability scans of internal and external network environments using an industry standard scanner. The firm also engages third parties to scan its externally facing infrastructure and provide findings on a regular basis. Vulnerabilities are addressed on a risk-adjusted basis, as required by a formal standard.

The firm has a defined treatment process for discovered vulnerabilities. Vulnerabilities are assigned criticality ratings based upon industry-standard processes and aligned with remediation plans. Where applicable, the timeframes for systems patching are documented in a formal standard. In cases where a vulnerability is identified for which a patch is not yet available, the firm may evaluate the adoption of appropriate compensating controls to minimize the likelihood of unauthorized access.

Virtual Desktop Solution

The firm uses Virtual Desktop Infrastructure for desktop computing. In this model, all users use a thin client to access their virtual desktop hosted in a GS data center.

Remote access from outside the firm's premises is enabled through a secure connection to a user's virtual desktop using multi-factor authentication.

The firm's virtualized infrastructure is designed to provide the equivalent level of control as the firm's on-premise infrastructure, regardless of the geographical location from which it is accessed. Non-Virtual Desktop computing models are conducted on an exception basis, when required by business functions.

End User Device Security

Secure Remote Access for Personnel

Personnel are permitted to use either issued corporate devices or their personal devices (Bring Your Own Device (BYOD)) when working remotely to securely access firm resources.

The Firm utilizes Mobile Device Management data loss protection (DLP) and other security controls to ensure data remains secure on corporate-issued mobile devices. In addition, the firm employs a Mobile Application Management (MAM) & Mobile Threat Defense (MTD) Strategy for BYOD. These MAM security controls are designed to protect data within the secure container. Firm information can be accessed only by appropriately patched and secure personal devices. The firm-approved mobile applications allow personnel to securely send and receive emails and access internal websites and documents. A limited set of third-party applications allow personnel to conduct analytic and/or business-related activity only if such applications meet the firm's security criteria.

Mobile applications used by the firm generally utilize a range of security features, including mobile threat defense, device allow-listing, secured network connections, multi-factor authentication, sandboxing, encryption, required device registration, required operating system (OS) patching, verification of non-jailbroken or rooted OS, and remote data wiping.

Personnel may be issued a firm device for specific business purposes. All data on firm-issued devices is encrypted at rest and in transit for remote access and mobile computing.

Client Mobile Applications

The firm has developed mobile applications for clients to access their accounts, perform and approve transactions, access market news and securely communicate with Goldman Sachs personnel. Client mobile applications employ additional industry-standard security controls including multi-factor authentication, biometric authentication, and encryption of data at rest and in transit.

Data Protection

Data Governance

The firm has an enterprise-wide data governance framework that defines how firm and client data is governed, including how data is controlled for quality at the point of origination, aggregation and publication. The framework assigns accountability for data quality and provides the necessary structure to ensure data is appropriately managed as an asset.

Data Protection

Data Loss Prevention (DLP) controls are designed and implemented with the objective of preventing content from leaving the firm that is not intended for external use and distribution. These controls include proactive alerts to notify a sender if an email to an external recipient contains potentially sensitive information, such as personally identifiable information (PII). The firm additionally maintains various surveillances to identify potential incidences of data exfiltration or insider threats, including using big data techniques.

Access to removable media, such as USB flash drives, writable CDs and local administrative and enhanced system functionality, is prohibited by default. When access to removable media is approved for specific business purposes, such access is strictly controlled and time-bound. Non-public data stored on removable media is encrypted.

Firm personnel are prohibited from using third-party systems and functions, such as webmail or unapproved analytics tools, for business purposes. In addition, firm personnel may not use firm resources to access such systems for personal use.

Staff access to selected websites and site categories is blocked or limited based on regulatory, information security, and internal control requirements. This includes social networks, file sharing and webmail.

Global Compliance oversees the firm’s electronic communications monitoring and surveillance program, including the review of alerts potentially indicative of a variety of risks resulting in potential non-adherence to regulatory requirements and/or firm policy.

PROTECT

Encryption

Firm policies and standards establish security principles regarding encrypting sensitive personal information, which are encrypted in transit over public and untrusted networks and at rest. Other types of data are encrypted and/or protected with compensating controls based upon regulatory, security, and contractual considerations.

The firm uses strong industry standard encryption methods. We regularly review the strength of our encryption protocols.

Firm-standard solutions are available for file encryption transferred between the firm and third parties.

Opportunistic email encryption, such as Transport Layer Security (TLS), is enabled with clients by default. Mandatory email encryption is supported and enabled by mutual agreements.

Key generation and management occur in firm-standard key management solutions that are backed by hardware encryption modules. Firm policy provides that access to encryption keys be pre-approved, limited to authorized individuals, subject to logging, and regularly monitored.

Data Security

The firm has formal, structured data privacy and security programs that include mandatory controls and processes for applications and assets storing or processing personally identifiable information. This program is updated as needed and in accordance with applicable laws and regulations, and with the firm's internal standards.

The firm has clean desk guidelines which instruct personnel to keep the workspace clear of paper containing sensitive data.

The firm has implemented controls which lock user workstations after a defined idle period. Personnel are advised to lock workstations when away from their desk.

The firm maintains controls to ensure secure data destruction at the end-of-life of a storage device. The firm has established a program to identify end-of-life systems, prioritize upgrades or demise of these systems based upon the criticality of supported services.

Firm policy requires that retired media are sanitized using a standard set of tools, and that physical media destruction is performed according to pre-defined procedures. Asset decommissioning is internally managed through workflow, inventory, and scanning processes.

The firm retains records for various periods as needed to comply with applicable laws and regulations and to conform to its internal retention policies.

PROTECT

Physical Security

Physical Security

Physical security measures are deployed to protect data centers and offices. These measures include card access, biometric access, video surveillance, on-site security staff, environmental controls, and visitor management.

Physical access is granted based on need, aligned with firmwide access controls, approved by designated access approvers and reviewed periodically. Physical separation of teams and offices is in place based on business and regulatory requirements. Access to data centers and offices is electronically logged by access card or biometric technology.

Firm procedure requires that visitors present photo identification and have a confirmed host before being granted access to the firm's offices or data center facilities. Visitor logs are maintained.

Critical data centers are geographically dispersed and on diverse utility and power infrastructure. These facilities have security personnel on duty 24 hours a day, and access is limited to only essential support personnel.

Facilities supporting Goldman Sachs businesses are protected from environmental hazards and power outages by the following controls, where applicable: Uninterruptible Power Supply (UPS), generators, air conditioning units, fire detection and suppression systems, water detection systems, earthquake resistant facilities and seismic designs.

Physical security standards are applied to all offices globally, including business recovery site locations.

Cloud Security

Cloud Governance

The firm leverages public, private, and hybrid cloud-based solutions where appropriate for certain compute, storage, and business purposes. The firm maintains a formal governance process and control framework for cloud-based applications, which are documented in formal standards.

Risk governance is embedded in the firm's global cloud governance framework to support the sustainable deployment and migration of the firm's cloud systems, applications and data on public cloud environments. Formal standards apply to cloud resources that are scoped to multiple offerings, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

The firm's public cloud environments are governed by committees responsible for overseeing the processes relevant to deploying and implementing cloud technology. In addition to the Firmwide Technology Risk Committee and Engineering Risk Steering Group previously mentioned, the following groups have oversight over cloud security:

- The Cloud Governance Steering Group provides oversight with a data-driven approach for usage of public cloud services and firmwide SaaS usage;
- The Third Party Risk Steering Group manages the vendor risk review process, including risk acceptance and remediation plans for cloud vendors.

Cloud Controls and Assessments

The firm has defined controls for cloud applications, including encryption and compensating controls, strict authentication, role-based access, centralized logging, network segmentation, and auditing. Continuous control monitoring and automated control enforcement gates are leveraged for cloud-based resources to detect misconfigurations.

Firm policy requires that cloud hosted applications undergo a formal risk assessment and architecture review on a risk-adjusted basis using a control inventory. New applications are required to complete a risk profile to determine regulatory and risk-based requirements.

Risk classifications are required to be reviewed on an annual basis. Risks identified through assessments are recorded in centralized inventories that detail key information about applications and findings.

The firm has established procedures, review processes, and control gates for onboarding data to cloud-hosted software platforms.

Cloud service providers are subject to an enhanced vendor management review covering the secure delivery of services and audit provisions and must satisfy the firm's public cloud control requirements.

Artificial Intelligence Security

Artificial Intelligence Security

Given technological developments in Generative Artificial Intelligence (GenAI) and Large Language Models (LLMs), the firm is carefully assessing its approach to Artificial Intelligence (AI) as it or its third-party vendors, clients or counterparties may develop or incorporate AI technology in certain business processes, services or products. As such, the firm has a Firmwide Artificial Intelligence Policy that establishes a framework for governing the use of AI across the firm.

The firm leverages a federated model for AI use case development to facilitate synergies between business segments with commercial expertise and platform teams with GenAI expertise. Formal firmwide and divisional governance and oversight ensures risk mitigation and alignment with business goals, regulatory requirements, firm policies, and investment considerations.

Access to external LLMs has been intentionally restricted by the firm and cannot be accessed from firm systems or used for business purposes without prior approval.

PROTECT

Vendor Security

Vendor Security

The firm has a Firmwide Vendor Management Policy and Program that documents a risk-based framework for managing third-party vendor relationships consistent with regulatory guidance and firm policy. Information security risk management is built into the firm's vendor management process, which covers vendor selection, onboarding, performance monitoring and risk management. Vendors are expected to design, implement, and maintain information security controls consistent with the firm's security policies and standards.

Firm policy requires that vendors that access Goldman Sachs sensitive data are expected to undergo an initial assessment on a risk-adjusted basis. Subsequently, the firm conducts re-certifications at a breadth and frequency determined by each vendor's information security rating, per the firm's vendor asset inventory, which is calculated based on several factors, including the type of data stored and processed by a particular vendor.

Such assessments may also include the use of third-party market scoring products to review vendors' internet-facing security posture. All assessments determine the maturity of the vendor's information security, cybersecurity and business continuity practices. Gaps found during these due diligence assessments are ranked by risk, recorded and addressed per the firm's standards.

The firm conducts ongoing oversight of vendors based on the criticality of each vendor's service to the firm and the results of the initial risk assessment. Critical vendors receive enhanced focus and due diligence. Changes in the service provided by a particular vendor are identified as part of a standard oversight process and may trigger an updated risk assessment prior to the firm onboarding additional services.

Firm policy requires vendors to sign standard contractual provisions before receiving sensitive information from the firm. These provisions have specific information security control requirements, which are negotiated with vendors that store, access, transmit or otherwise process sensitive information on behalf of the firm during onboarding or contract renewals, as applicable.

Dedicated teams across the firm are responsible for regular assessment and reporting on vendor information security controls. Periodic reporting of key vendor risk management metrics is provided to business management.

DETECT

Logging and Continuous Monitoring

Logging

The firm has enabled logging for key events including failed logins, administrative activity and change activity. Logs are maintained in accordance with firm policy on records retention and legal and regulatory requirements.

Log file management follows the principle of least privilege. Only application processes have "write" access to log files. System accounts only have "read" access to log files.

The firm has controls designed to prevent logs from containing sensitive information such as personally identifiable information (PII), authentication credentials or encryption keys.

Security event logging is enabled to allow for system forensic analysis and Technology Risk surveillance analytics. Security event logs are protected from unauthorized access, modification and accidental or deliberate overwriting.

Malware Protection

Industry-standard anti-malware software is installed on Windows, Mac and Linux endpoints and servers and on the firm's email infrastructure. Anti-malware alerts are monitored by the firm's staff. When detected, malware is remediated and if need be, systems are rebuilt. Malware signature files are updated on a regular basis by way of automatic requests from systems on the firm's network.

Runtime checks are performed on specific executables to reduce the possibility of exploit via malware. Application allow-listing is deployed to detect, report and prevent the execution of malware.

The firm utilizes an email protection system that is designed to block spam, phishing and viruses from reaching personnel inboxes. The firm subscribes to an email pre-filtering solution to reduce the amount of malware received by the firm's email gateway.

The firm mitigates spoofing using an email authentication policy and protocol to prevent spoofing of emails between the firm and its clients. The firm also assigns an imposter score to each email and flags emails above a threshold score for quarantine to assess potential email spoofing.

The firm has established key metrics to establish a baseline for continuously monitoring system state and anomaly detection in the firm's production environment. Pre-determined criteria are applied to security events to generate alerts. Monitoring tools are in place to notify appropriate personnel of security issues. Alerts are classified, prioritized and actioned by appropriate personnel for timely remediation based on business criticality.

DETECT

Security Monitoring and Intrusion Detection

The firm maintains a Hunt Team with dedicated experts focused on proactively identifying previously undetected malicious activity and opportunities to continuously improve Goldman Sachs' control posture. Additionally, the Hunt Team collects threat intelligence to actively identify potential indications of threat activity across the firm's network.

The firm maintains monitoring processes designed to detect anomalous activity in a timely manner. The firm collects, analyzes and correlates event data across the organization to perform real-time central aggregation to detect and respond to multifaceted cyber attacks, leveraging a variety of sensors distributed across the firm's environment.

The firm conducts periodic cyber attack simulations, micro-drills, quarterly drills and tabletop exercises to detect control gaps in personnel behavior, policies, procedures and resources.

The firm authorizes and monitors third-party connections and continuously collects and retains relevant information. The firm has automated alerts to monitor and prevent any unauthorized access to a critical system by a third-party service provider.

The firm performs threat intelligence collection to analyze threat actor tactics, techniques and procedures, which results in the tuning of controls to mitigate emerging adversary threats. The firm also shares threat intelligence with peer firms as an approach to actively maintain collective risk mitigation and improve security of external connections.

Insider Threat

The firm has an established insider threat program designed to detect and respond to malicious and unintentional unauthorized activity carried out by firm personnel.

The firm leverages a variety of telemetric, detective and preventive controls to address insider threats, including but not limited to, user endpoint monitoring and entitlements management.

RESPOND

Incident Management

Incident and Problem Management

The firm maintains an incident and problem management policy and procedures to mitigate risks and protect the confidentiality, integrity, and availability of the firm's production environments, while minimizing business disruption. The firm has established standardized procedures that allow for incident management, notification and post-mortem governance.

Security Incident Management

The firm has a dedicated Global Cyber Defense and Intelligence (GCDI) function responsible for detecting, investigating, and responding to information security threats and incidents that have a potential impact on the confidentiality, integrity, or availability of the firm's information and technology environment. GCDI maintains procedures for identifying and responding to specific information security incidents and works with other areas within the firm to contain, mitigate and remediate potential incidents. The firm's standardized security event and information management (SEIM) technology is used to aggregate and correlate platform, application and infrastructure logging across the firm to track and manage user-reported security events. In addition, GCDI maintains escalation protocols for appropriately notifying clients, regulators or other parties of security incidents. GCDI further maintains a dedicated threat management center that operates 24/7.

The firm has implemented a global security incident preparedness program to support security incident management. Technology Risk conducts business-focused tabletop exercises with business units and regional teams to assess their processes, understanding and readiness, with oversight from the Operational Risk Division. Externally, the program covers firm participation in financial sector and public–private sector cybersecurity exercises to enhance the firm's preparedness to coordinate with other institutions, financial markets and relevant government agencies.

Threat Intelligence

The firm recognizes that cyber threat actors target the firm's networks, vendors, suppliers and personnel, along with the broader financial sector, for a variety of reasons, including to conduct fraud, steal proprietary information and disrupt the firm's ability to conduct business and support its clients and customers. The GCDI Cyber Threat Analysis (CTA) team works to protect the firm from external adversaries by proactively identifying relevant cyber threats, evaluating the risk these threats pose to the firm's assets and working with personnel in the Engineering Division and affected business units to proactively reduce or mitigate risks to the firm.

Security intelligence and threat information are obtained from third-party intelligence service providers, industry consortia, internal monitoring, as well as public and government sources.

Cyber Insurance

The firm maintains a cybersecurity insurance policy that covers the firm's direct costs from a covered security incident along with applicable customer notifications and credit monitoring services, where necessary. The policy also includes coverage for Business Interruption issues. The firm's cybersecurity policy is serviced by a consortium of insurance providers.

RECOVER

Business Continuity and Technology Resilience

Business Continuity

Goldman Sachs has established a global, structured Business Continuity Planning (BCP) framework to coordinate the firm's response in the event of an operational disruption. The firm's Business Resilience Program comprises the following key elements: Crisis Management, Business Continuity Requirements, Technology Resilience, Business Recovery Solutions, Assurance and Process Improvement and Continual Assessment. The description of the firm's Business Resilience Program, including Disaster Recovery, is available on the firm's public website.

The firm has developed Business Continuity Plans (BCPs) to address operational disruptions. Plans must have identified BCP Coordinator(s) who develop and maintain the assigned BCP and ensure testing requirements. BCPs must be reviewed and updated by BCP Coordinators and certified by BCP Owners at the frequency required by firm standards. Under a BCP, each business unit identifies its critical activities, the dependent assets (people, facilities, systems, and third parties) that support those activities and the impact that a disruption to these dependent assets would have on the business unit's activities.

As part of a BCP, the business unit must complete business impact analysis. BCP Coordinators identify the criticality, recovery time objectives, dependencies and recovery strategies of their core processes. These processes determine the type of assurance needed to record completeness, *e.g.*, people recovery tests, application failover tests, training and tabletop drills.

The firm's business continuity risk mitigation strategy includes resilience capabilities such as near site, far site, work from home, and dispersed recovery capabilities where appropriate to mitigate risks and address threats to the region. The firm's far site recovery facilities reside on different power and utility grids from primary office locations.

The firm conducts ongoing business continuity preparedness testing, including tests of technology failover, people recovery facilities, work from home and regional handoffs. The firm also participates in industry-level tests with major securities exchanges, government agencies, and local authorities. The firm's divisions perform micro-drills, as well as chain of command and automatic notification testing.

Crisis Management Centers that operate 24/7 in every region allow the firm to monitor its environment, execute pre-established crisis management procedures and coordinate responses to incidents worldwide.

Data Backup and Recovery

The firm's record keeping, data backup and recovery processes are executed using an industry-standard enterprise system. Processes are in place to identify, escalate and remediate exceptions, as appropriate. Data backups are written to an immutable, disk-based platform for recovery purposes. Periodically, where practicable, data is written to encrypted tape media and shipped to off-site locations for storage.

The firm regularly tests the capability of applications to failover to alternate data centers as part of the BCP testing program. User-driven recovery requests are streamlined through a ticketing system. Recovery attempts of backed up data are logged.

RECOVER

Technology Resilience

The firm maintains a technology resilience program to review whether internal applications and dependent infrastructure components demonstrate the appropriate level of resiliency and recovery based on business criticality. Such controls include:

- Processing dispersion (reducing dependency on any one location);
- Network, telecom, and remote access resilience (multiple points of redundancy and resilience);
- Regional technology operating independently of critical market applications;
- Business application inventory and tiering (recovery time objectives);
- Inclusion of technology dependencies in all applicable business unit plans; and
- Resilience testing.

Based on business requirements, critical applications are deployed and tested across multiple data centers to ensure continued operation should a data center experience a disruption.

The firm participates in financial industry test initiatives, in jurisdictions where they are offered, to exercise alternative connectivity capabilities and to demonstrate an ability to operate through a significant business continuity and/or disaster event using backup sites and alternate recovery facilities.

The firm maintains a documented framework and recovery program to identify and mitigate cyber-destruction incidents like ransomware, including coordination among internal stakeholders and collaboration with external parties, such as law enforcement and regulators.

RECOVER

Our Expectations of Your Information Security Practices

Client Information Security Practices

Information security is a shared responsibility, which often involves cooperation between financial institutions and their clients. While Goldman Sachs seeks to provide as much assurance as possible for the services offered, the firm relies on your adoption of standard information security controls for the use of data and systems shared between you and the firm, for example:

- Aligning your information security and cybersecurity controls to international standards, such as the NIST Cybersecurity Framework, Center of Internet Security (CIS) Critical Controls, AICPA SOC reports and ISO 27001;
- Ensuring that only authorized users have access to the firm's data;
- Protecting authentication credentials, such as usernames and passwords, of users authorized to access the firm's data;
- Protecting computer equipment used in interactions with the firm with such tools as anti-malware software, a firewall and up-to-date operating systems;
- Notifying the firm promptly in case of any actual or suspected compromise of its data or system;
- Establishing a designated person to sponsor and drive information security, ideally from the executive leadership team who has the authority to make the right risk decisions across all lines of business and can effect change;
- Establishing a governance/oversight process where the leadership team can decide on risk management priorities;
- Retaining a third-party to test your security and determine if it is resistant to common attacks such as perimeter intrusion, malware infections, leakage of sensitive data or ransomware. As part of this exercise, identify internal owners, external partners, law enforcement and other key contacts who are best positioned to help during a security incident;
- Prioritizing risk mitigations based on criticality;
- Considering leveraging managed services to expand your security capabilities, including for security monitoring, vulnerability scanning, vendor assessments and incident response; and
- Considering commissioning "red team" tests from an independent third-party to evaluate security controls and incident response processes.