Goldman Sachs

CLIENT SECURITY STATEMENT

VERSION 7.0
APRIL 2019

Table of Contents

Introduction

Goldman Sachs understands the importance of information security, including cybersecurity, to protect against external threats and malicious insiders. The firm's cybersecurity strategy prioritizes detection, analysis and response to threat intelligence, cyber risks and malicious activity. The firm continuously strives to meet or exceed the industry's information security best practices and applies controls to protect our clients and the firm.

This document provides an overview of the firm's approach to information security and its practices to secure data, systems and services, including:

- Risk Governance and Regulatory Oversight
  Risk governance and risk management are a function of the firm's management culture, embedded practices and formal oversight. The firm's governance model is achieved by the day-to-day activities of managers and their teams, supported by various working groups and committees.
- Information Security and Cybersecurity Policies and Standards
  The firm maintains a comprehensive set of information security policies and standards to document the firm's approach to compliance with laws, rules, regulations, or firm management directives.
- Identity and Access Management
  The firm has implemented controls which identify, authorize, authenticate and manage individuals' access to the firm's systems and information assets.
- Applications and Software Security
  The firm manages application and software security through its software management process which includes a centralized inventory, secure software development practices, vulnerabilities testing, sustained resilience of applications and logging capabilities.
- Infrastructure Security
  The firm protects its infrastructure through a control framework which includes a tiered network architecture, vulnerabilities testing, system hardening and malware protection.
- Data Security and Data Privacy
  The firm has implemented controls designed to safeguard firm and client information which covers data classification, secure storage, handling, transmission and destruction.
- Mobile Security
  The firm's mobile solutions allow employees to conduct business activities on their personal devices while also ensuring that internal systems are secured and firm and client information remains protected.
- Security Incident Management
  The firm's security incident management program addresses security threats and incidents that have a potential impact on the confidentiality, integrity or availability of the firm's information and technology environment, including notification to clients as required by applicable laws and regulations.
- Business Continuity and Technology Resilience
  The firm has a mature and comprehensive global Business Continuity Program for Disaster Recovery (BCP/DR). The program covers both business and technology resilience. The main features of the program include dispersed capabilities, near site recovery, far site recovery and dispersed recovery. The description of the firm's Business Continuity & Technology Resilience Program for Disaster Recovery is available on the firm's public website.
- Physical Security
  The firm has implemented physical access controls on all firm facilities including office spaces, near site and far site locations, data centers and storage facilities.
- Vendor Security
  Information security risk management is built into the firm's vendor management process, which covers vendor selection, onboarding, performance monitoring and risk management.

While information security measures will naturally change over time and may differ across the range of Goldman Sachs' services, this overview should answer many of your questions regarding our 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.

Risk Governance, Audit and Regulatory Oversight

Risk Governance Framework

- The firm's risk governance employs a three-line defense model to increase accountability, oversight and assurance. The model organizes risk management activities across the firm's business units that own and manage risk (first line), independent risk oversight functions (second line) and internal audit (third line).
- The firm performs ongoing risk assessments, aligned to industry standards, which include the identification, monitoring and analysis of control performance. When appropriate, risk issues are created and managed to closure.

Governance Committees

- The firm's internal risk committees are globally responsible for the ongoing approval and monitoring of the risk frameworks, policies and limits which govern the firm's overall risk.
- The Firmwide Technology Risk Committee reviews matters related to the design, development, deployment and use of technology. This committee also oversees cybersecurity matters as well as technology risk management frameworks and methodologies and monitors their effectiveness. The CISO provides regular updates to the Firmwide Technology Risk Committee on relevant risk topics, program status and incidents.
- The Global Business Operational Resilience Committee is responsible for oversight of business resilience initiatives, promoting increased levels of security and resilience and reviewing certain operating risks related to business resilience.

Technology Risk Program

- The Technology Risk Program covers the firm's Information Security ("InfoSec") and Cybersecurity initiatives. The program is frequently adjusted to ensure ongoing suitability.
- The firm's Chief Information Security Officer ("CISO") is responsible for managing and implementing the Technology Risk Program and reports directly to the Global Head of Core Engineering.
- As part of the firm's second line of defense, a dedicated team of operational risk specialists provide independent oversight of the Technology Risk Program and assesses the operating effectiveness of the program against industry standard frameworks.
- The written Technology Risk Program is approved by the firm's Board of Directors annually. The Board of Directors takes an active interest in information security and cybersecurity matters and sets the firm's risk appetite in these areas, monitors progress and receives updates.

Internal Audit

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

Regulatory Oversight and External Audit

- The firm is regulated by numerous regulatory authorities in all jurisdictions in which we operate, including the Federal Reserve Board, New York State Department of Financial Services, Commodity Futures Trading Commission, Securities and Exchange Commission, Consumer Financial Protection Bureau, Financial Conduct Authority and Prudential Regulation Authority.
- PricewaterhouseCoopers LLP, the firm's external auditor, independently tests applicable controls as part of their audit of the firm's financial statements, their Service Organization Control (SOC) 1 reports and their audit of the firm's Business Continuity Program.

Industry Engagement

- Goldman Sachs is a founder or leading participant in many relevant industry initiatives, such as the Securities Industry and Financial Markets Association (SIFMA), the Financial Services Sector Coordinating Council (FSSCC) and the Financial Services – Information Sharing and Analysis Center (FS-ISAC). Please note this list is not exhaustive.

Information Security and Cybersecurity Policies and Standards

Policies and Standards

- The firm maintains a comprehensive set of information security and cybersecurity policies and standards which take into consideration data privacy laws and regulations that are applicable to jurisdictions in which the firm operates.
- Policies and standards are reviewed and approved by the relevant firmwide governance bodies. The firm's global information security and cybersecurity policy is reviewed annually.
- A dedicated policy task force maintains the process to develop, review, update and decommission information security policies and standards. These documents are subject to a pre-determined review cycle based on the nature and content of the material. The policy task force performs continuous monitoring driven by review cycles for information security policies and standards. Additionally, reviews may be triggered by changes in the environment or regulatory landscape.
- Firm policies and standards are aligned with recognized industry standards, including those dictated by the National Institute of Standards and Technology (NIST), the Federal Financial Institutions Examination Council (FFIEC) and the International Organization for Standardization (ISO).
- Firm policies and standards are available to all personnel through an internal compendium. These policies cover all aspects of the Technology Risk Program. Topics governed by information and cybersecurity policies and standards include:
  - Identity and Access Management, for example entitlement management and production access
  - Applications and Software Security, for example software change management, open source software and backup and restoration
  - Infrastructure Security, for example capacity management, vulnerability management, networks and wireless
  - Mobile Security, for example Bring Your Own Device (BYOD) and mobile applications
  - Data Security, for example cryptography and encryption, database security, data erasure and media disposal

Training and Education

- The firm conducts a global awareness campaign to help employees and contractors recognize information and cybersecurity concerns and respond accordingly; we focus on risk prevention and incident escalation. In addition, a training curriculum builds knowledge and skills to facilitate control adoption and promote individual accountability.
- Information security training, including cybersecurity and privacy, is required of all firm personnel annually. Additional training is provided for new joiners and individuals transferring within the firm. Specific information security training is provided based on roles, for example secure coding training for developers.
- Topics in the Technology Risk Information and Cybersecurity curriculum include:
  - Information and Cybersecurity Essentials
  - Bring Your Own Device (BYOD)
  - Social Engineering and Phishing
  - Data Risk Management
  - Insider Threat Awareness and Escalation
  - Vendor Technology Risk
  - Application Information Security
  - Managing Application Privileges
  - Email and Other Electronic Communication Security
  - Role-based Technology Training
  - Application Risk Curriculum for developers
  - Focused topical training for technology teams

Identity and Access Management

User Identity Management

- The firm has well-developed access controls that are based on the general principles of no privilege without identity, no privilege without approval, need-to-know, least privilege access and entitlements commensurate with role or job duties.
- The firm performs background checks on employees, consultants and contractors. Where permissible by applicable law, the background check process includes a credit check and a criminal records check. Worker identity is subsequently verified at the initiation of employment via standard human resources processes.
- Upon joining, the firm's personnel sign a non-disclosure agreement that requires them to abide by the firm's client confidential data protection policies.
- A unique identifier is assigned to every worker. Employees are prohibited from sharing their individual credential information, for example usernames and passwords.
- Staff identification badges are issued to all workers when they join the firm.

Entitlements Management

- The firm has a system of checks and balances designed to ensure that different people perform different parts of a critical activity.
- Firm approved authentication and entitlement solutions are used throughout the infrastructure. Production applications leverage firm approved solutions to implement identity and access management and to enable reporting of user entitlements. These solutions are used to process people who join or leave the firm or whose role within the firm changes.
- System entitlements are reviewed by management at least annually on a risk-adjusted basis. More frequent reviews occur for high-risk entitlements. Entitlements are also reviewed when a worker transfers to new roles or departments within the firm.
- When a worker leaves the firm, access to the firm's facilities and general access to the information systems are revoked within 24 hours. In special circumstances, access is revoked immediately.

Access Management

- Strong password controls are enforced wherever possible, for example via Active Directory policy settings. The firm's password standard calls for change at initial login, minimum password length, alphanumeric composition, expiration after a defined period, maximum number of unsuccessful login attempts before lockout, a password history and an inactivity lockout.
- Client data is maintained in production repositories, which reside within data centers with strong physical and logical security controls in place. Access to client data and administrative access to systems that store client data must be approved by authorized managers.
- Access by technology staff to production systems is limited to authorized individuals, time bound, subject to logging and periodic review, limited to necessary functions and regularly monitored. Each access session requires pre-approval. Access to source code is restricted to authorized personnel and requires approval.
- Activity performed during the production access period is logged and must be reviewed by an authorized individual.
- Firm personnel are prohibited from using third party, Internet-based (webmail) or email-like systems and functions 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.

Application and Software Security

Centralized Inventory

- The firm tracks its applications in a centralized inventory tool. The tool is used to record information describing the application as well as the associated hardware and technical ownership. In addition, applications are classified and ranked according to application criticality, the type of data they process and resiliency requirements.

Change Management

- The firm has a formal software development lifecycle (SDLC) centered on control gates. Changes in the production environment are governed by policies and standards.
- All production changes require successful testing and authorized approvals.
- Application information security is incorporated throughout the SDLC on a risk-adjusted basis. Examples of SDLC controls include:
  - Design reviews and data risk considerations, for example identifying privacy data
  - Manual code review and automated code scanning with industry standard tools for applications exposed to high-risk environments, for example externally-facing applications
  - Periodic penetration testing of externally facing applications using industry standard automated tools and manual tests
  - Entitlement reporting, program change management and production access control
  - Separate development and quality assurance (QA) environments from production environments
  - Testing and validation of open source libraries as free from known vulnerabilities.
- Most applications in use throughout the firm are developed internally. Some applications leverage open source libraries and source code. The same application security standards are applied to internally developed applications, open source software components and third-party software.

Secure Coding Practices

- Application information security is incorporated through:
  - Implementation of industry standard security coding practices such as Open Web Application Security Project (OWASP)
  - Error message configuration that limits the disclosure of sensitive data to third-parties
  - Personally identifiable information (PII) or other sensitive information is non-cacheable in the client browser cookies.

Security Testing

- The firm hosts authorized simulated attacks on firm systems, performed to evaluate the security of the infrastructure.
- 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 Open Web Application Security Project (OWASP) Testing Guide. The approach combines manual and automated assessment techniques and the use of premier proprietary, commercial and open source assessment tools in a consistent and repeatable process. The methodologies typically cover the following activities:
  - Pre-test preparation with asset owners
  - Threat modeling and triaging
  - Automated dynamic / static scans and output verification of scans
  - Vulnerability identification and confirmation testing
  - Report preparation and delivery with peer and manager review
  - Socialization of findings with asset owners
  - Tracking and remediation of issues
  - Retesting of remediated issues

Application and Software Security

Data Backup and Recovery

- Backups are written to an online disk-based platform for recovery purposes. Periodically, data is written to encrypted tape media and shipped to off-site locations for storage.
- The firm's backup and recovery is performed using an industry-standard enterprise system. Processes are in place to identify, escalate and remediate exceptions as appropriate.
- Recovery efficiency is validated through the breadth and frequency of data restores performed in the course of normal business operations.
- User-driven recovery requests are streamlined through a ticketing system. Recovery attempts of backed up data are logged.

Logging

- The firm has enabled logging for key events including failed logins, administrative activity and change activity.
- Log file management follows the principle of least privileges. Only application processes have write access to log files. System accounts only have read access to log files.
- Logs are maintained in accordance with firm policy on records retention and legal and regulatory requirements. At a minimum, logs are retained for 30 days.
- Logs do not contain sensitive information such as personally identifiable information (PII), authentication credentials or encryption keys.

Infrastructure Security

Hardware Inventory

- The firm maintains asset information for hardware in managed inventories. Each inventory has an owner and the attributes required to manage operational risks and the asset lifecycle associated with the asset class. Inventory management is comprised of manual and automated processes and controls, including periodic review of inventories, and is governed by policies and procedures.

Enhanced System Configurations

- All 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 recommended logging.
- Hard drives on firm-provided laptops are encrypted using industry standard encryption software.
- An inactivity screen lock is enforced by a configuration policy on every endpoint.

Malware Protection

- Industry-standard anti-malware software is installed on all Windows endpoints and servers and on the firm's email infrastructure.
- Anti-malware alerts are monitored by the firm's staff. Malware is remediated and if need be, systems are rebuilt.
- Malware signature files are updated on a regular basis, at a minimum daily, by way of automatic requests from the systems on the firm's network.
- Runtime checks are performed on specific executables to reduce the possibility of exploit via malware.
- Application whitelisting is deployed to detect, report and prevent the execution of malware.
- The firm subscribes to an email pre-filtering solution to reduce the amount of malware received by the firm's email gateway.
- The firm utilizes an email protection system that is designed to block spam, phishing and viruses from reaching employee inboxes.

Perimeter Network Security

- The firm provides external access to selected resources through a tiered network architecture comprising of multiple secure zones to create a highly segmented environment consistent with the defense-in-depth strategy. Secure zones are implemented via a combination of firewalls and virtual local area networks.
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are deployed at the network perimeter to monitor for and block malicious activity, where possible.
- Separate Domain Name Service (DNS) servers are deployed for internal and external name resolution. The firm's internal DNS namespace is distinct from the external namespace.
- Management interfaces on perimeter firewalls, routers and other devices are not accessible from the Internet. Access to these network infrastructure devices is limited to dedicated management zones.
- The firm subscribes to Distributed Denial of Service (DDoS) monitoring and mitigation services from multiple service providers. In addition, the firm hosts its primary Internet web presence on a Content Delivery Network 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 reported.
- Wireless communications are encrypted and wireless access to the firm's infrastructure is only permitted from firm approved devices, for example GS issued laptops and employee BYOD. Public wireless access to the Internet is provided by third-party solutions and is not connected to the firm's network.

Infrastructure Security

System Monitoring and Vulnerability Management

- The firm has a comprehensive vulnerability management program that includes weekly network-vulnerability scans of the 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 regular basis. Vulnerabilities on externally-facing systems are resolved on a risk-adjusted basis with those that are classified as high-risk immediately remediated. Vulnerabilities are tracked until resolved.
- The firm has a defined treatment process for discovered vulnerabilities. Discovered vulnerabilities are given a risk-ranked profile with a corresponding patch deployment monitoring and remediation timeframe. The timeframes for systems patching are documented in a firm standard. These timeframes are based on the system type and the vulnerability risk the patch remediates.

Network Desktop Solution

- Virtual Desktop Infrastructure is deployed to all employees and contingent workers of the firm globally.
- Remote connectivity requires two-factor authentication, provides communication encryption and prevents users from direct access to data/storing firm data on personal devices.

Cloud Infrastructure

- The firm leverages public cloud-based solutions to augment our internal, enterprise offerings. Cloud solution engagements are approved by our Cloud Governance and Vendor Risk control programs.
- Firm use of public cloud solutions is limited to approved business use cases.
- General access to public cloud solutions is limited by enterprise controls including perimeter and desktop constraints.
- Cloud-based solutions must satisfy the firm's public cloud control requirements including the encryption of data at rest and in transit, firm controlled authentication, centralized logging, auditing and role-based access to resources.
- Cloud providers are subject to an enhanced vendor management review covering the secure delivery of services, audit provisions, and satisfying the firm's public cloud control requirements.

Mobile Security

Secure Mobile Access Solutions for Employees

- The firm provides employees with secure mobile access to its resources on both corporate-owned devices and on approved personal mobile devices through a Bring Your Own Device (BYOD) program.
- Personal devices can only connect to the firm's network through firm approved mobile applications. These applications store firm information in secure containers which are segregated from personal information on the devices and encrypted. Any other storage of firm or client information on personal devices is prohibited.
- The firm approved mobile applications allow employees to securely send and receive emails and access internal websites and documents. A limited set of third-party applications allow employees to conduct analytical and/or business-related activity only if they meet the firm's security criteria.
- The firm approved mobile applications utilize a range of security features include:
  - device whitelisting and blacklisting
  - secured network connections
  - multi-factor authentication
  - sandboxing
  - encryption
  - required device registration
  - required operating system (OS) patching
  - verification of non-jailbroken OS
  - remote data wiping when triggered for loss of device or theft
- All firm data, including email communications, is encrypted on all mobile devices.

Client Mobile Applications

- The firm has developed mobile applications for clients to access their portfolio data information and market news and to securely communicate with Goldman Sachs employees. Client mobile applications employ additional industry-standard security controls including prohibited local storage and cache clearing.

Data Security and Data Privacy

Data Leakage Protection

- The firm has implemented a number of controls designed to mitigate the risk of data leakage. These controls comprise communications surveillance and analysis via a variety of methods, including big data mining techniques.
- Data Loss Prevention (DLP) controls are designed and implemented to prevent content from leaving the firm that is not intended for external use and distribution. These controls include proactive alerting for a sender if the potential for unintended misdirection of data is identified as well as prevention of certain sensitive information from leaving the firm, such as personally identifiable information (PII).
- Access to removable media, such as USB flash drives, writable CDs and local administrative and enhanced system functionality, is strictly controlled and time-bound. Non-public data stored on removable media is encrypted.

Encryption

- Data is encrypted where it is outside the protected enclosure of the firm's security enclaves, such as the firm's network, systems with access control and data centers. This includes encryption at rest (such as tapes, media, laptops, mobile devices) and encryption in transit (communications) where possible.
- We use strong industry standard encryption methods and commercially available products. We regularly review the strength of those protocols.
- Firm-standard solutions are available for encrypting files transferred between the firm and third parties.
- Opportunistic email encryption, such as Transport Layer Security (TLS), is enabled with all clients where possible. Mandatory email encryption is supported and enabled by mutual agreements.
- Access to encryption keys is pre-approved, limited to authorized individuals, time-bound, subject to logging, and is regularly monitored.

Data Security

- The firm has clean desk guidelines which instruct employees to keep the workspace clear of paper containing sensitive data which can prevent unauthorized users from gaining access to non-public information. Practices include not leaving documents containing sensitive data visible, unlocked or unattended.
- The firm has implemented controls which lock the workstation after an idle period. Employees are advised to lock workstations when stepping away.
- The firm has implemented controls to ensure secure data destruction at the end-of-life of the storage device. Retired media are sanitized using a standard set of tools. 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 law and regulation and to conform to its internal retention policies.

Data Privacy

- In accordance with the firm's business principles and applicable laws, the firm has a number of policies, standards, procedures and tools for protecting client, employee and counterparty personal data. In particular, a firmwide standard specifies data security and access controls for the applications handling personal data. Additionally, a number of tools are available for encrypting data sent outside the firm and data stored on firm's systems.

Physical Security

Physical Security

- The firm has standardized physical security measures in its data centers and offices, including card 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 segregation exists based on business and regulatory requirements. All data center and office facilities access is electronically logged by card access systems.
- All visitors must 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 electronically. In addition, enhanced screening of carry-in materials is performed as needed based on the assessment of the existing risk conditions.
- The firm's critical data centers are geographically dispersed and on diverse utility and power infrastructure with no direct dependencies. These facilities have security personnel on duty 24 hours a day.
- The firm's facilities are protected from environmental hazards and power outages by the following controls:
  - Uninterruptible Power Supply (UPS)
  - Generators
  - Air conditioning units
  - Fire detection and suppression systems
  - Water detection systems
  - Earthquake resistant facilities and seismic designs, where applicable
- The firm applies the same physical security standards to all offices globally, including business recovery site locations.

Vendor Security

Vendor Security

- Third parties are viewed as an extension of the firm. As such, third parties are expected to design and implement controls similar to those at the firm. To understand the extent to which third parties are aligned with the firm's controls, all vendors that handle Goldman Sachs information go through an initial assessment. Subsequently, periodic assessments are conducted based on the vendor information security rating (which is calculated based on a number of factors including the type of data stored / processed by the third parties) of third parties.
- The assessments determine the maturity of vendors' information security and business continuity practices. Concerns found during these due diligence assessments are recorded and tracked to resolution.
- Vendor oversight requirements are systematically scaled based on the vendor risk assessment results. Critical vendors receive enhanced focus and due diligence. Changes in the vendor service provided or vendor engagement are captured as part of ongoing vendor oversight. Related changes in due diligence or oversight are systematically triggered and tracked.
- On site visits are performed as necessary; reports of these visits are distributed to business owners to identify areas of concern.
- Firm policy requires that non-disclosure agreements be in place before any sensitive information is shared with a vendor party. Vendor contracts also include the firm's set of requirements for information security practice.
- Designated resources are responsible for regular assessment and reporting on vendor information security controls. Vendor information is stored in a central vendor directory database.
- Monthly reporting of vendor risks and vendor review activity are provided to business management.

Security Incident Management

Security Incident Management

- The firm has a dedicated Security Incident Response Team (SIRT) responsible for handling information security threats and incidents that have a potential impact on the confidentiality, integrity or availability of the firm's information and technology environment. The team maintains procedures for identifying and responding to specific information security incidents and works with other areas within the firm to contain, mitigate and remediate technology risk. In addition, the team maintains protocols for escalation to relevant parties when clients are impacted by an information security incident, where required by applicable laws or regulations.
- The firm has established a dedicated threat management center that operates 24/7. Security intelligence and threat information are obtained from third party intelligence service providers, industry consortia, internal monitoring, as well as public and government sources. Surveillances are regularly conducted across the firm's infrastructure.
- Key metrics are leveraged 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.
- The firm has implemented a global security incident preparedness program to support security incident management. The program conducts business focused table top exercises with business units and regional teams to assess their processes, understanding and readiness. Externally, the program coordinates firm participation in financial sector and public–private sector cybersecurity exercises to ensure that the firm is well prepared to integrate and coordinate with other institutions, financial markets and relevant government agencies.
- The firm's security incident management program provides for notification to impacted individuals, clients and other third parties as required by applicable laws and regulations.
- Status updates of cybersecurity and data resiliency measures are included in the firm's corporate and financial filings, for example "Yearly 10K" and "Quarterly 10Q".

Logging

- 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.

Cyber Insurance

- The firm maintains a cybersecurity insurance program that, in addition to covering the firm's own liability, also covers the cost of notifying clients when their personal information has been disseminated due to a system breach or security failure and the cost of credit-monitoring services for affected clients.

Business Continuity and Technology Resilience

Business Continuity

- The firm's Business Continuity Planning/Disaster Recovery Program comprises six key elements: Crisis Management, Business Continuity Requirements, Technology Resilience, Business Recovery Solutions, Assurance and Process Improvement / Continual Assessment. The description of the firm's Business Continuity & Technology Resilience Program for Disaster Recovery is available on the firm's public website.
- Each business unit by region has a specific Business Continuity Plan (BCP) and assigned BCP coordinator. The BCP plans are reviewed and certified quarterly to ensure compliance with firm standards.
- The firm conducts extensive business continuity preparedness testing, including tests of technology failover, people recovery facilities, work from home, and regional handoff. The firm also participates in industry-level tests with major securities exchanges, federal agencies and local authorities. The firm's divisions perform micro-drills, as well as chain of command and automatic notification testing.
- The firm conducts periodic resilience impact analyses. Business Managers are asked to verify the criticality, recovery time objective, dependencies and recovery strategies of their core processes. These processes determine the type of assurance needed to record completeness; for example: people recovery tests, application failover tests, training, table top drills, etc.
- The firm's business continuity risk mitigation strategy includes near site, far site and dispersed recovery capabilities where appropriate in order 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.
- 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.

Technology Resilience

- The firm has a robust technology resilience program to ensure internal applications and dependent infrastructure components demonstrate the appropriate level of resiliency and recovery based on business criticality. Such controls include:
  - Processing dispersion (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
  - Annual testing
- Based on business requirements, many critical applications are deployed and tested across multiple data centers to ensure seamless 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.

Our Expectations of Your Information Security Practices

Client Information Security Practices

- Information security is everyone's shared responsibility and often involves cooperation between financial institutions and their clients. While we seek to provide as much assurance as possible for the services offered, we do rely on your adoption of standard information security control for the use of data and systems shared between you and the firm, for example:
  - Ensuring that only authorized users have access to the firm's data.
  - Protecting authentication credentials, such as username and password, 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 system.
  - Notifying the firm promptly in case of any actual or suspected compromise of its data or system.
- You should also consider aligning your information and cybersecurity controls to international standards such as the NIST Cybersecurity Framework and ISO 27001.