Morgan Stanley

Morgan Stanley Minimum Security Standards

Introduction

Morgan Stanley expects each Supplier to have controls that align with our Minimum Security Standards identified below ("**Standards**").

These Standards align with the National Institute of Standards and Technology (NIST, www.nist.gov) and The Cyber Risk Institute's framework (CRI, https://cyberriskinstitute.org).

Morgan Stanley recognizes that technology continuously advances as do the associated tools and processes. Morgan Stanley also recognizes that nationally/internationally recognized standards/frameworks, (e.g., NIST and CRI), evolve to align with these emerging technologies. Suppliers should ensure that they continue to adhere to these Standards relative to emerging technologies as well as evolving standards and frameworks.

Each bullet item that follows is a requirement that all Suppliers must comply with. In this context, 'service' means any process, activity, function, product, application or otherwise that an organization provides to Morgan Stanley regardless of whether data is or is not shared. A few of the requirements begin with a conditional clause, (e.g., "If the service Supplier provides to Morgan Stanley includes the use of APIs…"). In those cases, the requirement only pertains to services that satisfy the condition. The use of "Supplier" in the following statements is equivalent to your organization.

Governance, Policy, and Oversight

Human Resources Management

- Individuals assigned to Morgan Stanley must meet the terms of the contract between Morgan Stanley and Supplier.
- Supplier must provide ongoing training to individuals assigned to Morgan Stanley that includes data protection, cyber security, operational resilience, and safe usage of artificial intelligence. Associated metrics should be maintained and reported.

Data Integrity, Security and Management

- Controls and best practices to validate/verify data and/or to protect the confidentiality and integrity of information during transmission must be implemented.
- Encryption of all data at rest at various levels, (e.g., disk, file system, application, database, column, field, and storage service level, etc.), within all environments and devices is required.
- Encryption of data in transit between Supplier and Morgan Stanley and between Supplier and subcontractors is required.
- Data loss prevention controls must be implemented, (e.g., MFA required for privileged users; restricted access to tunneling, proxy and file hosting/sharing services; scanning of outgoing data; removable media prohibited; and use of production data in lower environments prohibited).
- "An encryption key management program that: keeps encryption keys separate from the data they protect; centralizes key management with a Key Management System (KMS) or secrets manager; prohibits hardcoding of encryption keys; uses a Hardware Security Module (HSM) or isolated cryptographic vaults for high-value keys; sets strict access controls for key use; manages key

rotation; uses secure key generation methods; limits each key to a single purpose; monitors and audits key activity; handles the full encryption key lifecycle; revokes and destroys keys safely; creates and maintains a key inventory; and has dedicated keys for Morgan Stanley services that use public clouds must be implemented.

- Secure storage in-house and/or chain of custody controls must be implemented and practiced throughout the lifecycle of the data and certified destruction of any Morgan Stanley data once required retention periods have ended, must be captured and shared with Morgan Stanley.Data must be backed up regularly and backups must be tested to ensure all data updates are auditable and that the backups are accurate and complete. Backups must be securely retained for the time-period Morgan Stanley and/or regulators require.
- All data must be classified and labeled, and appropriate handling procedures that align with the classification/sensitivity must be established, documented, and practiced.
- Logging of sensitive information, (e.g., PII, SSN, etc.) must be prohibited.

Identity and Access Management

- Access rights and privileges must be implemented for unique individuals or agents, (i.e., groups or shared user IDs must not be used); and be based upon the principles of need to know and least privilege. All access requests must be reviewed (to ensure access is appropriate and satisfies Separation of Duties requirements) and approved by the supplier before access is granted.
- Access rights must be reviewed at least annually and following any changes in responsibilities, (e.g., transfer or termination) and for any termination, access is promptly removed.
- Password controls around complexity, hashed in storage, required change at first login, defined reuse period, etc. must be implemented.
- Individual authentication methods, other than username and password, (e.g., MFA, smart cards, etc.), must be used to access systems that store, host and or process Morgan Stanley data.
- Controls must be implemented that monitor privileged access and identify inappropriate/anomalous activity, (e.g., alerts of suspicious activities, detailed logging, just-in-time access to limit duration of privileged access, etc.). Alerts must be reviewed and addressed as warranted.
- If Supplier provides Morgan Stanley's employees with access to any systems/applications, Morgan Stanley must be involved in such access approvals, entitlement reviews, etc.
- Local and remote desktops, servers, and mobile sessions must time out after a period of inactivity.

Physical and Environmental Security

- Security controls for public areas must include locks or electronic control mechanisms and corresponding alarm systems must be implemented.
- Access to non-public areas where Morgan Stanley data may be stored or processed must require enhanced authentication measures such as biometric access or card access.
- Physical access rights must only be permitted by authorized personnel only and access must be promptly revoked when no longer needed.
- A process must be implemented to ensure the collection and secure storage of access cards, devices and data storage medium upon termination or transfer.
- Personnel must wear photo IDs, visitors must provide identification, be logged and be escorted.
- Periodic environmental threat and vulnerability assessments must be performed that include fire prevention, flooding detection, etc., issues must be noted and tracked through resolution.

Network and System Security Management

- Suppliers must implement processes for baselining and monitoring systems activities, exception and information security events that include audit logs with relevant details to capture changes to systems configurations, files, etc.; monitoring and alerting for anomalous activity, intrusion prevention, defined process for investigation; responding to identified exceptions or anomalies; and regular review and updates of monitoring processes and baseline settings.
- Control principles for remote access security must be implemented, (e.g., MFA, endpoint security-posture checks, network segmentation and isolation of remote access, use of secure remote access gateways, geolocation/IP filtering, etc.).
- Firewall controls must be implemented and include: every connection to an external network must be terminated at a firewall; firewall rules must be documented, regularly reviewed, tested to ensure proper configurations, and maintained current; any changes to firewall rules require approval and must undergo security reviews prior to approval.
- Domain Name Service (DNS) controls must be employed, (e.g., NDS over HTTPS and/or TLS, DNS secure configurations, DNS logging, and monitoring for anomalies).

Threat and Vulnerability Management

- Threat and Vulnerability Management program must include scanning of all environments for recently disclosed vulnerabilities; pre-deployment scanning of code, images and other data sources for weaknesses, flaws and/or secrets; software component analysis to identify potential risks from use of open-source code; and review of cloud configuration settings.
- Vulnerability detection tools, threat signatures, and compromise indicators must be updated daily.
- Penetration testing must be performed regularly by an independent party and cover web/cloud-hosted and mobile applications and both internal and external networks. Weaknesses identified must be documented, rated, and tracked through resolution.
- Patch Management program must include a prioritization process with associated implementation timeframes, an emergency patch process, and monitoring to ensure patches are timely and successfully applied.

Cloud Security (applicable for any Suppliers that are CSPs or employ cloud technology in provision of services to Morgan Stanley)

- Service agreements must exist between Supplier and Cloud Service Providers (CSP) that Supplier uses that include the service scope, clearing delineates which party (CSP or Supplier) is responsible for which tasks, and ensures all information/cyber security and operational resilience controls and associated processes are addressed and responsible parties assigned including clearing delineating which party (CSP or Supplier) is responsible for each control.
- Supplier must monitor for and prevent cloud configuration drift.
- Access to CSP environments, applications, storage buckets of Morgan Stanley data, and systems must implement restricted-access only and access must be logged and monitored for anomalies with escalations when warranted.
- If Supplier is providing PaaS to Morgan Stanley, policies and procedures must also include application security, application development portability, and information processing interoperability.

Change Implementation Management

- A change management program must be implemented that includes documentation of all changes, tracking, a change impact assessment, rollback plans, an emergency change process, sufficient testing, approval of changes prior to implementation, monitoring post change and monitoring for changes implemented without approval.
- Suppliers must proactively notify Morgan Stanley of any changes that may impact Morgan Stanley.

System and Application Design and Development

- Secure system development practices must be employed that include security requirements, documenting of baseline configurations, use of a code repository, secure coding, integration, acceptance, and system security testing.
- Development, testing, and staging environments must be segregated from the production environment.
- Firewalls must be implemented between each tier, (e.g., between web and application servers and between application and database servers).
- Security methods must be implemented to protect application sessions, (e.g., prevention of concurrent logins from the same user account, session ID rotation after successful logins, clearing of client-side cookies at logout, cookies marked as secure of HTTP only, and configurable session timeouts).
- If APIs are used between Morgan Stanley's network and Supplier's network, authentication mechanisms must be implemented, and the API session must be managed.
- If a mobile application or portal is part of the service provided to Morgan Stanley, session expiration controls should be implemented.
- If the service provided to Morgan Stanley employs a model or GenAI, Morgan Stanley must be explicitly informed of such and the model and its basis (e.g., quantitative, judgement-based, etc.) must be thoroughly explained.
- Access to sensitive model data and training datasets must only be granted to authorized persons/processes and such access must be logged.

Asset Management, Secure Transport and Disposal of Assets

- Supplier must maintain asset inventories of both physical and software assets that include detailed information regarding ownership, location, data classification, etc.
- Suppliers must have a program to detect and manage end-of-life and unsupported system components that include identification, risk mitigation, alternative options, and disclosure to Morgan Stanley of such assets.
- If Supplier is employed by Morgan Stanley to securely ship/transport data-bearing assets Supplier must have secure shipping controls implemented that includes secure packaging, tamper proof containers, chain of custody detailed documentation, secure transport vehicles and associated practices, (e.g., point-to-point transport, the vehicle must always be under observation, and doors and containers must be sealed).
- If Supplier is employed by Morgan Stanley to dispose of Morgan Stanley data-bearing assets, Supplier must have asset disposal procedures and processes established and the requisite tools to meet Morgan Stanley requirements. Morgan Stanley data must never be sold or used for any purpose other than to provide the products and services to Morgan Stanley.

- Asset Disposal procedures must be documented and aligned with national or international disposal standards and certificates of destruction must be provided by Supplier at the request of Morgan Stanley.
- Supplier must comply with Morgan Stanley specific requirements relative to disposal including maximum size of remnant pieces and types of destruction.

Vendor Management

- Suppliers must have a documented vendor management program that is reviewed and updated annually and includes policies/procedures and senior management oversight.
- All material subcontractors must be assessed periodically relative to information, cyber security and operational resiliency controls and identified weaknesses must be documented and tracked through resolution.
- The assessment must ensure the material subcontractors have the requisite policies and procedures and associated controls implemented, (e.g., infosec policy, data handling, and business continuity/disaster recovery policy).
- For any subcontractors that have access to Morgan Stanley data, non-disclosure agreements between Supplier and those organizations must be in place. Any such subcontractor is prohibited from making changes to the environments/systems that provide the service to Morgan Stanley, and they must not forward any Morgan Stanley data without explicit approval from Morgan Stanley.

Incident and Problem Management

- Incident and Problem Management program must be established by Supplier and include established communication and escalation procedures, staff dedicated to resolving incidents in a timely and thorough manner, tracking and remediation of incidents through closure, identification of root causes, documented response plans that include actions to contain the incident and prevent further impact. Response plans should be tested annually and updated as warranted.
- In accordance with terms of the contract with Morgan Stanley, suppliers must notify Morgan Stanley in writing of any data compromises or incidents that cause service disruption or discovery of an incident.

Operational Resilience

- Supplier must provide their Business Continuity and Disaster Recovery plans to Morgan Stanley. Such plans must be documented, tested, and updated regularly to incorporate changes, recent technologies, and incorporation of resolution to weaknesses identified during testing. Single points of failure must be identified and resolved by Supplier.
- Supplier's recovery point objective and capability post-disaster for each service provided to Morgan Stanley must align with Morgan Stanley's requirements.
- Electrical and mechanical resiliency controls should be implemented at data centers to lessen the potential of a disaster and data centers should be geographically dispersed.

Suppliers with services deployed at Morgan Stanley premises have the following additional requirements:

- Identity and Access Management: Permanent privileged access to the host, (e.g., Linux root access, or local administrator access on Windows), must not be required.

- Change Management: Deployment of any software/firmware updates or new versions must be controlled by Morgan Stanley. Auto-updates and automatic downloads must be prohibited.