Security Requirements for Suppliers and Business Partners

Version 1.5

Security Requirement for Suppliers and Business Partners

05 August 2025

This document defines the security controls that Mastercard expects suppliers and other third parties to implement if they have access to, store, or process Mastercard's information resources (including Personal Information). These controls must be implemented in addition to any legal, regulatory, or industry-defined standards or audit / certification requirements that may be applicable (e.g., the Payment Card Industry Data Security Standard).

If you have questions, visit procurement.mastercard.com or contact our Third Party Risk Management team at TPRM@mastercard.com. Additional resources regarding cybersecurity are also available at mastercard.com.

If you have experienced, or suspect you may have experienced, a security incident or potential data breach that could potentially affect Mastercard, you must **immediately** call Mastercard's global security operations center at +1 636 722 3600, and e-mail TPRM@mastercard.com and your Mastercard relationship contact.

This document applies to companies working with Mastercard as a supplier, strategic partner, or other non-customer relationship. Requirements for Mastercard's licensed customers and their service providers are different; more information is available on mastercard.com.

Contents

Information Security Organization 3
Risk Management 3
Personnel Security 4
Physical Security 5
Operations Management 5
Security Defense, Monitoring, and Response 7
Securing Data in Transit and at Rest 8
Access Control 9
Network Security 10
Third Party Services 11
Application Management 12
Enterprise Resilience (Business Continuity) 13
Compliance 13
Information Technology Management 14
IT Incident Management 14
Privacy 15
Audit Management 15
Artificial Intelligence 15
Cloud Security 16
Glossary of Terms 17

Information Security Organization

1. The organization must designate a person (e.g. a Chief Security Officer (CSO) responsible for establishing, implementing, maintaining, and enforcing the organization's Information Security department program.
2. Formal information security functions and responsibilities must be defined and implemented into an Information Security department.
3. The Information Security department develops and maintains a comprehensive security strategy.
4. Comprehensive security policies, standards and procedures are developed and maintained by the Information Security department.
5. Reviews are completed annually on the information security department policies and procedures.
6. An Internal Audit committee or similar separate function must review the Information Security policy with the Chief Security Officer at least annually.
7. Ownership for all information system or resources must be designated. Owners are responsible for oversight and alignment with organization policies and standards.
8. All organizational information systems and resources must have a designated resource administrator responsible for protecting and maintaining those assets.
9. The organization must designate teams whose mission is to address security incidents and vulnerabilities on organization-owned or leased information resources.
10. The organization must evaluate its security awareness training program for input for future curriculum definition and training sessions.
11. The organization's Information Security department must provide organization personnel, third party consultants and contractors with annual information security department awareness training or the organization must ensure that third party consultants and contractors are contractually required to receive annual information security awareness training consistent with the training provided by the organization.
12. The organization must designate a person responsible for privacy and data protection compliance (e.g. a Chief Privacy Officer) who is appointed and works with the Information Security department to ensure that the organization is following national and international legal and regulatory requirements that relate to data protection and privacy.

Risk Management

1. The organization must establish a risk management program complete with assessment roles and responsibilities.
2. The organization must ensure that all information resources are inventoried and operate in a secure manner so that they may be included as part of the organizational risk management program.
3. The organization must designate security requirements for classifying information resources which specifies procedures based on classification delegating the handling, retention, labeling, copying, distributing, storing, transporting, disposing, and printing.
4. The organization's personnel must handle any sensitive information (including Personal Information) of its clients (including Mastercard) with integrity and discretion and in accordance with all applicable laws. Information that is obtained by the organization, or through one of the organization's clients is considered 'sensitive'.
5. Organizational personnel, third party consultants, contractors, and vendors are required to adhere to the organization's defined guidelines with respect to the handling of information in hard copy form.

6. The organization must adopt a risk mitigation strategy which may involve accepting the identified risk, transferring the risk to third parties by purchasing insurance or contractual agreements or choose to shut down the risk prone services if they are not critical for organizational existence.
7. The organization must ensure information systems implement cryptographic mechanisms to prevent unauthorized disclosure and modification of sensitive information (including Personal Information). Security policies and operational procedures are in place for protecting sensitive information and are documented, in use, and known to all affected parties.
8. The organization employs automated mechanisms no less than quarterly to update the list of vulnerabilities scanned, track the continued the presence of security vulnerabilities on information systems and identify when new vulnerabilities are identified and reported.
9. The organization must establish processes and procedures for assets on its network to include, as applicable, Industrial Control Systems (ICS).
10. The organization must perform vulnerability and risk assessment for assets on its network to include, as applicable, Industrial Control System (ICS) components.
11. Workstations must be protected with a standard, secure configuration including both client/desktop controls and individual application controls, e.g. browser configurations.
12. Removable media drives must be specifically approved and based on business requirements. Removable media containing organization information (e.g. CDs, USB sticks, floppy disk, tapes, removable hard drives, DVDs, and printed media) must be registered with a designated owner and scanned automatically / manually for potential threats.
13. Access to offsite sensitive media storage areas must be restricted to authorized individuals. Transfer must be completed using mechanisms with appropriate security from the source to destination such as utilizing authorized courier with tracking mechanism, confirmation of receipt, encryption and/or tamper evident packaging, and chain of custody as appropriate with the data classification of the information.
14. The organization must establish processes and procedures for disposing information specific to electronic media.
15. The organization must establish processes and procedures for storing and destruction of information in hard copy form.

Personnel Security

1. The Human Resource Department must subject employment candidates (including contractors and temporary staff) to pre-employment screening. If contractors or temporary staff are provided through an agency, the contract with the agency must clearly specify the agency's responsibilities for screening and the notification they need to follow if screening has not been completed or if the results give cause for doubt or concern.
2. The organization employees and contingent staff sign a non-disclosure or confidentiality agreement prior to accessing organization facilities or information.
3. The organization's personnel sign an employment contract that clearly states their responsibilities related to information security.
4. The organization must develop and document an Acceptable Use & Responsibility standard relative to information security.
5. Disciplinary action must be consistent with the severity of the incident, as determined by an investigation, up to and including termination.
6. The organization must establish processes and procedures for revoking system access.

Physical Security

1. For all organization facilities, a secure physical perimeter must be established.
2. Access to organization facilities is appropriately restricted to authorized personnel. This may include the use of armed security, pass, badge and biometric controls, visitor sign-in and Staff requirements and regular review of physical access rights.
3. When constructing or selecting computing facilities, organization defined environmental concerns must be considered as part of a site risk assessment.
4. Requirements must be developed to ensure the Industrial Control System/Building Automation System (ICS/BAS) are logically and physically separated, minimal access points exist, and the appropriate firewalls are configured.
5. Physical security controls are in place over information assets and systems at all organization computing facilities to address security threats, environmental hazards, and disaster recovery requirements.
6. Access to facilities dedicated to computer processing (e.g., data centers, operations centers, media libraries, telecommunications rooms, UPS rooms, etc.) are physically restricted and access is only granted to those Staff, third party consultants, contractors and vendors who have legitimate business responsibilities in the facility.
7. Access to the facility and restricted areas of the facility must be recorded and retained for 90 days, unless otherwise restricted by law, to enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity. This includes, but is not limited to, physical access and video logs,
8. Access logs, whether maintained in electronic or printed form, are reviewed on a regular basis relative to the classification of assets at that location.
9. Physical intrusion detection devices must be implemented in organization facilities.
10. The organization must develop and document procedures for security guards or other personnel designated with protecting the physical security environment.
11. Recordings / videos from cameras used to monitor sensitive areas of computing facilities are audited Video recordings must be retained on secure organizational premises for no longer than 90 days, unless needed to retain the data to complete an investigation, or as otherwise required by applicable laws and regulations.
12. The organization must establish requirements to secure offices and work areas where sensitive information is processed. This includes clear desk and clear screen requirements, office lock-up procedures and use of secure cabinets and containers.
13. Computing systems processing highly sensitive data (such as Sensitive Personal Information) must ensure physical and logical control from unauthorized access, and securing information stored on mobile computing devices.
14. The organization has developed, documented and implemented policies and procedures to protect sensitive information (including Personal Information) stored on mobile computing devices.
15. Requirements must be established for the use of equipment outside organization's premises for information processing must be authorized and approved by management. Staff must not remove property off organization premises, without prior authorization.

Operations Management

1. The Information Technology function is defined and responsible for establishing and maintaining operational control procedures. These operational control procedures are used by resource administrators when installing or maintaining information resources of the organization. Access to the operational control procedures is made available only to authorized personnel.

2. All organization information resources are established and maintained in accordance with information technology standard builds and the applicable platform-specific security baseline (i.e., CIS Benchmarks).
3. The organization must establish processes and procedures to disable, restrict, or secure unnecessary functions, services, utilities, and commands.
4. Platform and application administrators are responsible for the following:
    - Testing of patches prior to implementation
    - Perform, coordinate and support responses to identified security vulnerabilities
    - Notification of patch updates
    - Installation of patches, fixes, and service packs
    - Testing applications after operating system patch changes
    - Vulnerability management processes
5. Vendors are responsible for ensuring that an inventory in electronic form is maintained for all information resources.
6. Measures are taken for the protection of system documentation that contains sensitive information (e.g., descriptions of applications, processes, procedures, data structures, and authorization processes).
7. The organization network architecture is clearly documented to facilitate identification of components during network analysis operations and incident investigations.
8. All information resources (networks, applications, systems, etc.) must follow a formal change control procedure, and Information Technology Infrastructure Library (ITIL) best practices, to ensure that only authorized changes are committed to production.
9. All change control documentation reflects an audit trail of the change including the date and time of change, reason for change, the name of the person making the change, and the person or persons who authorized the change.
10. When deploying off-the-shelf software, resource administrators must harden the resulting software and document the minimum hardware, software, and services to be included on the system by installing the minimum hardware, software and services necessary to meet the requirements using a documented installation procedure.
11. The organization must have established processes and procedures for installation and use of bespoke vendor software.
12. System lifecycle and change management processes and controls are established.
13. The organization has established activities that are to be logged by information resources. These must include, at the minimum, the following activities: application start/stop times, system boot/restart times, system configuration changes, abnormal system events, confirmation that files and output were handled correctly and critical file changes.
14. The organization must implement automated monitoring and alerting strategies to generate warning when allocated audit record storage volume nears or reaches the defined maximum audit record storage capacity.
15. Development, test, and production environments must be separated physically, or at a minimum logically, to reduce the risk of accidental change or unauthorized access to production software and data.
16. Development and production maintenance duties are assigned to separate Staff to ensure separation of duties.
17. The IT Operations Manager must establish a change control process for the change of Backup and Restore documentation.
18. The change control process must include proper authorization and business documentation for all changes to the

Backup and Restore documentation. The IT Operations department must deploy appropriate up to date technologies to manage backup and restore tasks.

19. The organization must have designated technical personnel to provide operational and technical support for all network related issues.
20. Management must establish procedures for timely monitoring of the clearance of customer queries.
21. The Information Security department and Information Technology department are responsible for developing, implementing, maintaining, and communicating a malicious code control program to limit the attack surface.
22. Within the organization computing environments. They are also responsible for reviewing and selecting approved anti-malware and virus detection software to be used by organization.
23. The organization must update and continuously run anti-malware software once a week to ensure system scans can identify all known attacks.
24. All organization computing devices that are at heightened risk to be affected by malware have approved virus detection and file integrity software installed and active.
25. Virus scans and file integrity checks must be completed prior to the first use of each executable file that is brought into the organization computing environment.
26. Virus scans, file integrity checks and processes to ensure data contents are encrypted must be performed prior to any removable media being sent outside organization.
27. The organization must establish processes and procedures for anti-malware software configuration.
28. The organization provides centralized SPAM protection and spoofing protection as part of its email infrastructure.
29. The organization has a defined operations department which is responsible for developing, documenting, and implementing backup schedules, outlining the type of backup, interval, storage location and the number of copies of information resources requested to be backed up by the resource owners.
30. The organization must establish processes and procedures for backup classifications and associated schedules.
31. The organization must establish processes and procedures for regular information system backups and verifying these are being performed.
32. The organization's data is stored offsite based on the data's level of classification and policy governing the backup of classified information.
33. The organization has a defined record retention schedule which document types of records and relevant retention for a period commensurate with the record's usefulness within organization legal and regulatory requirements and other organization directives.
34. The organization must establish a record retention schedule that supports regulatory requirements.
35. The organization employees, third party contractors and vendors must adhere to all copyright laws and packaged software license agreements.
36. Configuration management and software standards are established, based on recognized industry best use practice (for example NIST, CIS)

Security Defense, Monitoring, and Response

1. The organization must employ centrally managed automated tools to reassess the integrity of software and information by performing daily integrity scans of the information system, detect unauthorized changes to the software and information and notify the designated individuals upon discovering discrepancies during integrity verification. (e.g. file integrity monitoring tools).
2. The organization must continuously monitor network/system activity to ensure secure operation and alert the

designated individuals of any anomalies.

3. The organization ensures boundary protection processes and procedures are established.
4. Organization systems are configured to log to centralized systems.
5. The organization ensures that all its information resources are subject to audit logging, which is continuous and protected from unauthorized access, modification, and destruction. Audit logs must be stored for defined periods of time for audit trail analysis and retained for at least one year (twelve months).
6. Intrusion Detection Systems/Intrusion Protection Systems (IDS/IPS) must be implemented on network perimeter to protect the organization from threats, vulnerabilities, and malicious code. All file-based servers and workstations such as Windows/MacOS laptop computers must use a host-based malware protection software.
7. Endpoints must centrally log all malware events and findings to centrally managed Security Information and Event Management (SIEM) system.
8. The Information Security department is responsible for developing, implementing, maintaining, and communicating a security incident reporting process and related procedures that includes cardholder information.
9. A designated Incident Response Team must be established and held responsible for documenting information security incidents.
10. Incident team roles and responsibilities are established to include appropriate 'authority to operate' rights while responding to incidents. The organization must develop an incident response procedure for all security and privacy related incidents involving a 'breach of security' to Personal Information.

Securing Data in Transit and at Rest

Encryption standards are established to protect sensitive information (data classified as confidential or highly confidential, including Personal Information and PAN data) when being transmitted, processed, and/or stored on organization information resources. Sensitive data must be encrypted both in rest and in transit.

- Data at rest must be encrypted with a minimum of AES 128, and use appropriate modes of encryption (either GCM, or CBC with HMAC protection for integrity).
- Data in transit should be encrypted using TLS 1.2 or higher.
- All encryption keys must be managed by the supplier (as opposed to the cloud platform provider such as AWS, Azure, google, etc.). This is typically referred to as "customer managed keys". All vendors must comply by September 30, 2025.
- The lifetime of encryption keys should be defined, and vendors must provide upon request a key inventory that includes key type, use, and crypto period.

1. Where required, sensitive information within memory must be protected to prevent unauthorized access.
2. Employees responsible for implementing encryption technologies must sign a statement acknowledging their responsibilities. Employees must not install any encryption software not validated and approved by the Information Security department.
3. Connections to wireless access points must be authenticated over an industry best practice, using Wireless Protected Access 2 (WPA2) at a minimum.
4. Sensitive Information, such as customer name, cardholder information, must not be sent over the Internet, via Remote Access or transmitted over public or external networks unless the transmission utilizes a strong encryption method or protocol as defined above.
5. The organization must have a policy governing appropriate web usage.
6. All web browsing activities by organization personnel are intercepted by a web proxy which authenticates the system user and logs attributes necessary to identify malicious or unapproved activity.

Access Control

1. The organization must manage information system accounts by implementing automated centralized control of user access and administrator functions.
2. The performance of privileged functions is appropriately segregated and monitored.
3. The organization must establish processes and procedures for periodic review of general access accounts.
4. The Human Resources department is responsible for reporting changes in user's duties or employment status to resource administrators and access management personnel to ensure entitlements are updated in a timely manner.
5. Controls and procedures are in place to revoke unnecessary access privileges.
6. Access is assigned and periodically reviewed to ensure least privilege access is granted.
7. The organization must complete an annual review and certification of local access accounts.
8. All users with access to organization's information resources must utilize User IDs that are specifically assigned to them.
9. User IDs must be unique across all systems and forever connected with the single user to whom it has been assigned. For those vendors that process Primary Account Number (PAN) information for Mastercard, PANs as a unique ID must be prohibited, unless this is explicitly authorized by Mastercard.
10. User IDs are not utilized by anyone except the individual to whom the IDs have been issued. It is prohibited to reveal or share your account password or other credentials with others or allow use of the user account by others under any circumstances. Users are responsible for all activity performed with their personal User IDs.
11. Controls are in place to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
12. All default, pre-set, or temporary passwords and accounts assigned internally must be set to a unique value per user and changed immediately after first login. Vendor-supplied defaults must be changed prior to installation of third-party software on the network, which must be disabled if not necessary for business purposes.
13. Access control systems must be implemented that are tamper proof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.
14. The organization must establish processes and procedures for password strength requirements in line with applicable regulatory or industry guidelines.
15. Passwords for device or non-user identifiers must be forced to expire automatically on all systems at least every ninety (90) days. Exception: Identifiers that are logically restricted to an approved path or source may have a non- expiring password.
16. All user-generated PINS should follow Industry best practices and be at minimum of 8 numerals.
17. Users must be provided the capability to change their password through secure protocols.
18. Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable using strong cryptography, during transmission and storage on all system components.
19. Passwords cannot be coded into login scripts, dial-in communications programs, files, browsers, or any executable program.
20. Storage of passwords and use of automated systems to record, replay or provide authentication must be protected through strong cryptography and patched according to vendor recommendations.
21. Authentication controls are in place to ensure personnel are positively identified and authenticated prior to

granting access.

22. Designated access control personnel, whether it is the information owner, resource administrator or help desk, verify the identity and access level of the user prior to resetting their password.
23. Temporary passwords that are provided to users who maintain their own passwords must be unique to each individual, not be easily guessable; meet password complexity requirements, expire upon initial use and require users to create a new one, follow established procedures for verifying the identity of the user prior to providing them with the temporary password and be distributed to the user in a secure manner (never be sent in clear text).
24. The organization must establish processes and procedures to disable and remove inactive login IDs within a 24-hour period.
25. The organization's Human Resources department must notify access management administrators of extended absences to ensure that access is temporarily disabled.
26. The organization must establish processes and procedures for password history in line with applicable regulatory and industry standards.
27. The organization must establish processes and procedures for session management, requiring reauthentication after a period of 15 minutes of inactivity.
28. Users cannot leave any organization information resource unattended that contains sensitive information or is connected to an organization network and must logoff or activate a screen saver program if the information resource in not used for more than 15 minutes.
29. Access to information resources is restricted to users with the correct information classification level.
30. The organization utilizes a centralized access management system to avoid the need to independently grant privileges to users.
31. User activity reports must be reviewed regularly to identify misuse or inappropriate access rights.
32. All external and local connections to the organization's systems, networks or information resources, including Personal Information that the organization processes on behalf of Mastercard, whether managed onsite or by a third party, require strong multi-factor authentication for (privileged and non-privileged) accounts.

Network Security

1. Requirements are established for ensuring users only have direct access to the network services for which they have been specifically authorized to use and will be restricted based on established security controls.
2. The Industrial Control System (ICS) network must be logically separated from the corporate network on physically separate network devices. The organization must ensure that minimal access points exist between the ICS network and the corporate network and document them. Firewalls between the ICS network and corporate network must be configured to reject all unauthorized traffic.
3. The organization must ensure that administration of network and network devices is carried out on different networks.
4. Internal system which accesses external networks must be logically isolated from internal networks. Logical isolation must result in the inability for systems to communicate unless intentional action is taken by authorized personnel.
5. All external access from untrusted systems or networks (i.e. Extranet) to any internal network must be controlled through the implementation of an Information Security approved layer 4 stateful firewall.

6. The organization must establish and implement a firewall rule base to include a default-deny rule to prohibit traffic which is not specifically permitted for valid business purposes. Any allowed access must be explicitly added after an appropriate security review.
7. All firewall rules must be reviewed on a quarterly basis.
8. Router configuration standards must include security considerations such as disabling source routing, blocking of FTP, TFTP and telnet, strong authentication for router administrative access, what is required to be logged and audited, change management processes, and synchronization of startup and running configurations.
9. A baseline configuration of the network device host operating system must be developed and maintained and under configuration control. Baseline configurations must consider business need, vendor recommendations and "best practices". Additionally, the baseline configuration must be minimized to reduce the change of an exploit from an unused service or feature.
10. The organization must establish processes and procedures for email systems with configurations following existing Network Security policy.
11. All administrative management functions must use industry standard encrypted protocols.
12. SNMP v3 is recommended to monitor and manage network devices.
13. Utilizing a Zero Trust Security model based on industry best-practices, vendors must:
    - Identify and authenticate all user endpoint devices (vendor-managed, BYOD).
    - all user endpoint devices must be subjected to continuous monitoring to ensure compliance.
    - All access from user endpoint devices must be enforced based on device type, in accordance with least privilege principles.
    - The Principle of Least Privilege must be followed when determining the number of vendors Staff needed to support systems, and associated permissions.
    - For connectivity protected by micro segmentation, including ingress and egress traffic, Least Privilege Principles must be applied.

Third Party Services

1. The organization must establish processes and procedures for analysis of technology/services to be outsourced and any sub processor of Mastercard data must meet all these minimum-security requirements outlined in this document.
2. The organization must evaluate and perform thorough due diligence before engaging a third-party service provider.
3. If the service provided to Mastercard is deemed critical or material to an operational resilience it must be included in the supplier resilience process. Depending on the sensitivity and criticality of the services provided, the organization must commission a review of the service provider's security control structure.
4. The organization employs safeguards to ensure that the interests of third-party service providers are consistent with and reflect organization interests.
5. All Value-Added Resellers (VARS) require additional due diligence.
6. A written agreement containing the appropriate terms and conditions must be executed for all third-party service provider relationships.

7. It is the responsibility of those signing the contract and the business unit funding the effort to assign a relevant member of Mastercard Technology staff to the role of business relationship owner who is responsible for managing all aspects of the relationship with the Third-Party.

8. Security requirements of the third-party information service are defined and incorporated into all formal agreements. This includes the following security provisions as applicable:
    - Security Requirements that govern all Third-Party relationships.
    - Performing Third-Party Risk Assessments.
    - Approval of Third-Party Security agreements and mitigation of issues
    - Business continuity considerations of Third-Party services
    - Third-Party development services
    - Termination clauses when appropriate security requirements cannot be met.
    - Third-Party Certification Requirements
    - Right to Audit
    - Notification of violations and incidents involving Mastercard Data or the Mastercard Security Requirements or Critical and High Risks.
    - All requirements covered by Third Party Service Agreements and the supporting standards.
9. The organization is responsible for ensuring that an assessment is performed for each outsourced or subcontracted activity through third party service providers.
10. If a third-party service provider, onshore or offshore, is being considered for the provision of critical information processing services (including PII), the organization requires outsourcing service providers to develop and establish a business continuity and disaster recovery framework, which defines its role and responsibilities for documenting, maintaining, and testing its contingency plans and recovery procedures. The vendor must review, update, and test its business continuity plans regularly in accordance with changing technologies, conditions, and operation requirements.
11. The organization must establish processes and procedures for monitoring third party service providers.
12. When granting customer access to organization information or assets, procedures must be in place to ensure compliance with the organization Security Monitoring and Response Policy.

Application Management

1. The Application Management Lifecycle must include a formal methodology (SDLC) defining standards & incorporate controls into each stage of the management cycle for the building of applications.
2. All open-source software libraries are subject to additional due diligence and review.
3. The organization requires the integration of security requirements in system design that are consistent and supportive of the organization security architecture.
4. Corporate Security must review and approve security requirements for systems that will be used to process sensitive information (including PII & PCI) before the initiation of project design. The review process must address requirements related to information security, internal controls, privacy protection and legal/regulatory considerations.
5. The organization must establish processes and procedures for addressing risks of internet-based applications.
6. The disclosure of application configuration information that could be exploited by outsiders must be prevented.
7. The organization has designated and Enterprise Architecture or other IT technology selection working group responsible for defining an overall IT technology selection and acquisition framework consistent with IT strategies.

8. Data input into application systems must be validated to ensure the completeness and accuracy of the information processed can be confirmed.
9. The organization must establish processes and procedures for maintaining a secure encryption key infrastructure and keys must be kept secure.
10. The organization must compile audit records into a system-wide (logical or physical) time-correlated centralized audit trail. Auditing must be continuous and protected from unauthorized access, modification and destruction for the organization's information resources. Critical files are to be identified by the application team.
11. The organization must implement processes and procedures for thorough testing of security features and controls as part of application testing, which must include unit testing, acceptance testing, integration testing, performance testing & security testing.
12. Organizations must control and monitor updates attempted for deployment against any Products or Services provided to Mastercard using a staged rollout approach.
13. All significant modifications, major enhancements, and new systems must be integration tested prior to deployment in production environments. System stress testing and volume testing must be performed, and in some cases, parallel testing will be required. Integration testing must be conducted in a separate, independently controlled environment.

Enterprise Resilience (Business Continuity)

1. Redundant power supply systems (External, UPS, Generator) must be in place for all Critical or higher operational systems.
2. The organization must perform preventive maintenance regularly on all equipment used to support information systems or data center operations in conformance with manufacturer recommendations.
3. The organization must establish processes and procedures for the use of backup generators, to include fuel vendors, for maintaining power during electrical supply outage.
4. The mission and purpose of Business Continuity Management must be clearly defined within a policy or charter.
5. The organization's Disaster Recovery Program Manager is responsible for the development, maintenance, and testing of organization's technical recovery plans.
6. Business continuity plans are formulated to ensure that employees are aware of the steps they would be required to take in the event of a business disruption or disaster.
7. The organization must establish processes and procedures for identifying extreme but plausible scenarios against business disruptions and impacts.
8. Management is responsible for ensuring that an annual review of business continuity plans is completed. The business continuity plan must be referenced against an inventory of information resources and applications to ensure that all critical processes are adequately protected.
9. Ensure backup data is stored securely and can be quickly restored.
10. Have established communication protocols for notifying Mastercard in the event of business disruption. Adhere to industry regulations related to Business Continuity and Disaster Recovery.

Compliance

1. The organization must establish processes and procedures for documentation of legal and compliance obligations.
2. The organization must have an established privacy and data protection program specifying management practices, roles and responsibilities and technical and organizational measures to ensure that Personal Information is processed in compliance with applicable laws.

3. Personal Information must not be transferred to a country or territory outside the European Economic Area (EEA), unless that country or territory ensures an adequate level of protection of the rights and freedoms of the data subjects in relation to the processing of Personal Information.
4. Personal Information must only be obtained by organization for specified and lawful purposes and must not be further processed or disclosed in any manner incompatible with those purposes.
5. The organization must have procedures for the data subjects to exercise their rights relating to their personal information held by organization. The procedures must allow for data subjects to specify legitimate reasons regarding the challenges, updates, or corrections regarding the organization processing of their Personal Information. The procedures shall also identify any fee associated with such challenges, updates, or corrections.
6. Standards are defined for protecting personal information, including customer data, when processing is outsourced to a third party. The same standard of protection must be required from all third parties, contractors and vendors who have access to systems of record that maintain personal information.
7. The organization has designated a specific department to ensure that independent audits, assessments, and penetration tests are performed on an annual basis, or as otherwise necessary (i.e. segmentation controls, significant infrastructure or application upgrade or modification).
8. Audits must ensure compliance with organization security policies, standards, procedures, and other documented security requirements.
9. The organization must employ automated mechanism to scan the network no less than quarterly to detect the addition of unauthorized components/devices into the information system.

Information Technology Management

1. IT management must institute a security training program, at least annually, to provide education and awareness of internal practices and policy as well as external guidance towards the proficiency and use of technology within organization.
2. A training program must institute and provide sufficient funding for both internal and external events to further the education and skills of IT resources.
3. All IT practices and standards must be overseen through formal review processes approved by the Chief Information Security Officer.
4. The organization must establish processes and procedures for access control for mobile devices, which must include:
    - Prevent unauthorized access by remotely locking out the device.
    - Remotely track device information and traffic data in the mobile device, based on jurisdiction.
    - Retrieve device information and traffic data remotely from the mobile device, based on jurisdiction.
    - Retain the ability to securely destroy/delete all organizational proprietary information stored on the device and any attached storage, if required, for regulatory purposes.

IT Incident Management

1. The organization must review log files and audit trails at least every 24 hours for anomalous activity. Log files and audit trails must include, at the minimum: system records initialization sequences, logons and errors, system processes and performance, system resources utilization anomalies and network traffic, bandwidth utilization rates. Where possible, automated mechanisms are employed to integrate audit review, analysis, and reporting processes to support the investigation and response to suspicious activities.

2. Administrative groups must be inspected at least every 7 days to ensure unauthorized administrator accounts have not been created, or authorized administrator accounts have not been used in an unauthorized manner, and spot checks of system audit records must be completed at least once every thirty (30) days to validate ongoing integrity.
3. The organization must create event logs, which must include, but are not limited to: User identification (source and destination), Success or failure indication, Origination of event (system and application), Internet Protocol (IP) address of systems (source and destination [for many events, the source will be the user's IP]), Ports in use (source and destination), Identity or name of affected data, system component, or resource Date and time stamp, Description of the activity performed must include Event ID or event type, Reason for logging event (e.g., access failure).
4. Event logs are reviewed on a regular weekly basis to identify security incidents and potential vulnerability in the security structure.
5. The organization must establish IT event monitoring processes that identify relevant IT events, alert proper personnel of anomalous IT activities, filter, correlate and analyze event data and provide the appropriate response to IT events, in real time.
6. The information security department must establish a channel for the reporting of IT incidents; in particular, security incidents and potential vulnerabilities in the security structure.
7. Incident management is responsible for establishing processes that follows through the five phases of the Incident lifecycle: Identification, logging, categorization, prioritization, and Incident response.

Privacy

1. The organization must establish processes and procedures for the collection, processing, and retention of Personal Information in accordance with defined Mastercard privacy and information security procedures, and the Data Protection Agreement (DPA) and other contractual data protection and privacy terms, as applicable.
2. If the organization or any of its personnel process any Mastercard U.S. "sensitive personal data" within the meaning of 28 C.F.R. part 202, (a) the organization must not enable access by a "covered person" within the meaning of 28 C.F.R. part 202 without implementing the Cybersecurity and Infrastructure Security Agency requirements, and (b) Section 3 of Appendix 2 of the DPA shall govern such processing.

Audit Management

1. The organization must provide meaningful procedures for timely hearing and resolving enrollee grievances. A grievance may also include a complaint that an organization refused to expedite a coverage determination or redetermination, complaints regarding the timeliness, appropriateness, access to, and/or setting of a provided item.
2. The organization must define, develop, and document a bribery prevention policy that covers activities related to bribery, inclusive of public officials, penalties and prosecution of offenders, periodic review, and training /dissemination to the organization's staff.
3. The organization must define, develop, and document a policy that covers activities related to prohibited foreign trade practices, inclusive of public officials, penalties and prosecution of offenders, periodic review, and training/dissemination to the organization's staff.
4. An independent internal audit committee chaired by a member of the Board of Directors must be established. The audit committee must be responsible for designating roles and responsibilities for audit functions, performance of audits, effectiveness, and oversight of external auditors. The audit committee must meet periodically to review outstanding audit issues, ongoing projects, findings, and recommendations from audit projects.
5. Findings (control deficiencies, gaps, or issues) and recommendations for improvements must be reported to

the appropriate management as well as the audit committee and/or Board of Directors.

Artificial Intelligence

1. The organization must secure-by-design and secure-by-default any Artificial Intelligence (AI) systems or services being developed and/or operated by the organization in support of Mastercard services or products.
2. Organizational staff who utilize AI systems or services must be trained on the latest security threats.
3. Appropriate use of AI will be included in the organization's acceptable use and responsibility standard.
4. Prior to training and/or deployment, AI models must be classified appropriately.

Cloud Security

Supplier must ensure that Cloud Services (whether performed by Supplier or by a third party) be contractually bound to protect organization information stored and/or processed in the cloud including implementing the following:

- Information requirements protection requirements
- Identity and Access Management (IAM) requirements
- Availability, capacity management and performance management requirements
- Monitoring, alerting and response requirements.
- Compliance and audit evidence requirements

1. Protections must be in place for data movement, including the end-to end path where data is sent, and where it will reside, to address regulatory, statutory, or supply chain agreement compliance.
2. CSP provided root and enterprise administration identities with unrestricted access must be secured. The following is required:

- Multi-Factor Authentication (MFA) hardware tokens must be utilized unless otherwise approved by Corporate Security. Hardware tokens must be stored in a secured location.
- Access keys for API access must not be assigned and must be rotated on an annual basis.
- Utilization must be restricted to initial provisioning, administration actions requiring the CSP provided account, or to provide break glass emergency access.

3. Cloud security alerts must be integrated with an appropriate Security Information and Event Management (SIEM). Continuous monitoring must be in place to detect network, configuration, and access anomalies. Incident remediation processes must be defined for these event types.
4. CSP must have granted Mastercard a right to audit or a right to access independent assurance reports related to security, e.g., audits and penetration testing results. The method to initiate these processes must be documented.
5. Logs and audit trail history must be maintained for a minimum of one year in a location that is protected from unauthorized modifications or deletion.

Glossary of Terms

Backup and Restore - Backing up files and recovering them after a system failure.

Chief Privacy Officer – a senior level executive responsible for managing data protection and privacy risks, and for the development and oversight of related policies and programs.

Chief Security Officer - an organization's most senior executive accountable for the development and oversight of policies and programs intended for the mitigation and/or reduction of compliance, operational, strategic, financial, and reputational security risk strategies relating to the protection of people, intellectual assets, and tangible property.

Event ID - unique ID related to any observable occurrence in a network or system.

Incident Response Team - Group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents.

Industry Control System (ICS) - An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.

Intrusion Detection System/Intrusion Protection System (IDS/IPS) - software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

Internet Protocol (IP) – Standard protocol for transmission of data from source to destinations in packetswitched communications networks and interconnected systems of such networks.

Payment Card Industry Data Security Standard (PCI-DSS) – an information security standard for organizations that handle payment card information.

Personal Information – any information relating to an identified or identifiable natural person.

Port – the entry or exit point from a computer for connecting communications or peripheral devices.

Sensitive Personal Information – any Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, geo-location data, and information relating to criminal convictions and offences or related security measures.

Revision/Approval History

Version	Revised By	Date Revised	Approved By	Date Approved	Revision Description
1.0		March 07, 2024		March 07, 2024	Comprehensive Review Securing Data in Transit and at Rest -All encryption keys must be managed by the supplier (this includes any cloud HSM keys managed by AWS, google, etc.). All vendors must comply by March 31, 2025.
1.2		August 14, 2024		August 14, 2024	Review
1.3		February 7, 2025			Review Included staged roll-outs; Securing Data in Transit and at Rest section was clarified.
1.4		June 26, 2025			Review Legal update DPA
1.5		August 5, 2025		August 5, 2025	Legal Update