

MasterCard E-commerce Self-Assessment for Large Merchants and all Member Service Providers

MasterCard
International



Purpose of This Self-Assessment Form

The MasterCard Site Data Protection (SDP) Program establishes security requirements that an acquirer's e-commerce merchants and Member Service Providers (MSP) must satisfy in order for the acquirer to be eligible to receive certain benefits. These requirements are detailed in *MasterCard Security Standard Applicable to Merchants and Member Service Providers*. The goal of the SDP Program is to support the protection of MasterCard account data by providing e-commerce merchants and MSPs with the ability, and encouraging them to assess the effectiveness of their security measures.

This MasterCard E-commerce Self-Assessment is one component of the SDP Program. It provides a self-rating mechanism to help a merchant determine if its security measures meet the MasterCard guidelines.

For more information about the MasterCard SDP program, please visit the SDP Web site at <https://sdp.mastercardintl.com> or ask your acquirer for more information.

Who Should Complete This Form

The person in the organization, who is responsible for information security, and ultimately the security of MasterCard transaction data, should complete this form. Depending on the size and structure of the organization, this person may be the Information Security Officer, the Network Administrator, or the lead programmer.

How to Use this Form

This form is divided into six sections. Each section focuses on a specific area of security.

Within each section, symbols identify individual questions indicating the criticality of each requirement.

This symbol...	Identifies...
●	A critical security requirement. If this requirement is not followed, MasterCard account data may be at risk.
▽	A security best practice. MasterCard recommends this practice to reduce the long-term risk of account data compromise.

Rating Each Section

A rating box follows each section. After completing each section, fill in the rating boxes as follows:

In each section, IF...	THEN the section rating is...
ALL questions identified with ● or √ are answered with “yes”	Green —means that the e-commerce merchant or MSP is compliant with the self-assessment portion of the SDP program.
ALL questions identified with ● are answered with “yes” but some questions identified with √ are answered with “no”	Yellow —means that although the e-commerce merchant or MSP has achieved compliance with the SDP self-assessment, there are security risks that need examination.
ANY questions identified with ● are answered with “no”	Red —means that the e-commerce merchant or MSP is not considered compliant. To reach compliance with the self-assessment, the risk(s) must be resolved and the survey must be retaken to demonstrate compliance.

Rating the Entire Assessment

An overall rating box appears at the end of the assessment. After completing the assessment, users should fill in the final rating box as follows:

IF...	THEN the overall rating is...
ALL sections register a “Green” rating	Green
One or more sections register a “Yellow” rating	Yellow
One or more sections register a “Red” rating	Red

Section 1: Security Management

Severity	Description	Response	
▽	Does an information security management process exist that involves the identification of assets, threats, and vulnerabilities to information security?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
▽	Are information security policies formally documented?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
▽	Are information security policies and other security-relevant information disseminated to all users (including vendors, contractors, and business partners)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
▽	Is the information security policy reviewed at least once a year?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
▽	Is the information security policy updated when the environment changes?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
▽	Have you made a formal risk analysis on your e-commerce environment and back office in the past year?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
▽	Is there an adequate information security awareness and training program in place for all people using the information systems?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
▽	Is the information security awareness and training program regularly updated?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
▽	Is a security incident response plan formally documented and disseminated?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
▽	Has an information security officer been assigned within your company?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
▽	Are the roles and responsibilities with regard to information security clearly defined within your company?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
▽	Are company and employee compliance to the security policy assessed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
▽	Do all contracts with third parties having access to sensitive cardholder information contain a clause that specifies cardholder account information must be kept confidential?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

Rating for Section 1: Green Yellow Red

Section 2: Access Control

Severity	Description	Response	
▽	Are all access control logs regularly reviewed, and do they contain both successful and unsuccessful login attempts?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Do access control measures for customers at a minimum, include username and password authentication?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
▽	Do all users have an individual username and password that is not shared with any other user?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
▽	Are privileged users—whether customers, employees or business partners—who have access to sensitive cardholder information to payment processing platforms required to use a SecureID card, or some other two-factor or token-based authentication method?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
▽	Is user access restricted on a need-to-know basis?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are maintenance accounts and remote support access controlled; if they are not required, are they disabled?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Is there a password policy that enforces the use of strong passwords for both employees and customers?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
▽	Are users required to change their password on a pre-defined, regular basis?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Is there an account lockout mechanism that blocks a malicious user from obtaining access to an account by multiple password retries or brute force?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are privileged and administrative accounts strictly controlled?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	When customers, employees, or business partners remotely access systems via the Internet, is encryption such as Secure Socket Layer (SSL) used to protect from eavesdropping?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
▽	Are password protected screen-savers used on systems and consoles that provide access to sensitive information and critical systems?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	When an employee leaves the company, is the user account and password immediately revoked?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are all user accounts reviewed on a yearly basis to ensure that malicious, out-of-date, or unknown accounts do not exist?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are accounts that are not used for a pre-defined length of time (sleeping accounts) automatically disabled in the system?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

Rating for Section 2: Green Yellow Red

Section 3: Operational Security

Severity	Description	Response	
▽	Are security incidents reported to the information security officer for investigation?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Is there an incident response team ready to be deployed in case of an account data compromise?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Is a security assessment and/or penetration test performed on your environment at least quarterly?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
▽	Is separation of duties enforced and does it prevent developers from accessing the production system and installing modified software without authorization?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
▽	Is separation of duties enforced and does it prevent backup operators from being actively involved in the operations?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
▽	Are media containing sensitive cardholder information protected against unauthorized access?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Is sensitive cardholder data encrypted in databases and in backup media?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
▽	Are audit logs regularly reviewed?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Is sensitive cardholder information sanitized before it is logged in the audit log?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are strong two-factor authentication and secure encrypted communications used for remote administration of production systems and applications?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are vendor default security settings changed on production systems before the system goes into production?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are all production systems hardened by removing all unnecessary tools installed by the default configuration?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are all production systems updated with the latest security related patches released by the vendors of various components?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
▽	Are production system and application modifications planned, authorized, and traced?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Is there a virus scanner installed on all servers and on all workstations?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Is the virus scanner regularly updated?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
▽	Do all workstations have a personal firewall installed?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Is all cardholder information printed on paper or received by fax adequately protected against unauthorized access?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are procedures in place to handle secure disposal of backup media and other media containing sensitive cardholder information?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
▽	Are all changes to the environment formally authorized and logged before being implemented?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

Rating for Section 3: Green Yellow Red

Section 4: Application and System Development

Severity	Description	Response	
▽	Is information security included throughout the software development life cycle (SDLC) process?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
▽	Is your software and application development process based on an industry standard?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Is a security assessment and/or penetration test performed on all of your e-commerce applications before they go into production?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	If production data is used for testing and development purposes, is sensitive cardholder information sanitized first?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Is there a dedicated and separate test environment?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are all but the last four digits of the Primary Account Number (PAN) masked when displaying cardholder information?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Is sensitive cardholder data stored in databases encrypted with sufficient strength keys, such as 128-bit triple DES or other strong algorithms based on industry standards?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are data and communication encryption keys stored in a hardware device or tamper resistant security module?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Does encryption and decryption of data occur within a secure hardware device?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are key manipulations on the secure hardware device done under dual control?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Is there a separation of duties between the development, production, and test staff?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Is there a separation between the development, production, and test environments?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are all input controls implemented at the server side to prevent the bypassing of client side input controls?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are controls implemented at the server side to prevent SQL injection?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
▽	When authenticating over the Internet, is the application designed to prevent account harvesting by malicious users trying to determine existing user accounts?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are cookies secured or encrypted?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

Rating for Section 4: Green Yellow Red

Section 5: Network Security

Severity	Description	Response	
●	Is the router configuration secured?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are egress and ingress filters installed on all border routers to prevent impersonation with spoofed IP addresses?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	If routers and other network devices are configured remotely, is a secure communication protocol used to protect the communication channel from eavesdropping?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are routers configured to drop any unauthorized packets?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are the router logs regularly reviewed for unauthorized traffic?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are routers configured to prevent remote probing?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Is a firewall used to protect the network, and to limit traffic to only that required for business?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Do changes to the firewall need authorization, and are the changes logged?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are firewall logs regularly reviewed?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Is the network segment containing the servers for the Web presence separated from the Internet with a firewall?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
▽	Is the network segment containing the servers for the Web presence separated from the network segment containing the internal servers with a firewall?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Is the firewall configured to translate the IP addresses used on the internet to different internal IP addresses(for example, using network address translation, NAT)?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
▽	Does the network configuration prevent network mapping from the outside (for example, ping, trace route)?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are all Internet accessible hosts (for example, firewall, Web server, router, etc.) periodically updated and patched for security vulnerabilities?.	Yes <input type="checkbox"/>	No <input type="checkbox"/>
▽	Is a network based intrusion detection system (IDS) used on your network?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Are transmissions of cardholder data encrypted through the use of SSL or other industry acceptable methods?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
▽	If SSL is used for transmission of cardholder data, is it using version 3.0 with 128-bit encryption?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	If wireless access is used, is the communication encrypted?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	If wireless access is used, is network access limited to only know network cards?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
▽	Are personal modems configured to only allow dial-out connections?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

Rating for Section 5: Green Yellow Red

Section 6: Physical Security

Severity	Description	Response	
▽	Are there multiple physical security controls (badges, escorts, mantraps, etc.) in place that would prevent unauthorized individuals from gaining access to the facility?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Is key storage physically protected?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Is cardholder information deleted or destroyed before physically being disposed (for example, shredding papers, destroying backup media)?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
●	Is sensitive cardholder data physically separated from other data stored in the e-commerce environment?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

Rating for Section 6: Green Yellow Red

Overall Rating: Green Yellow Red
