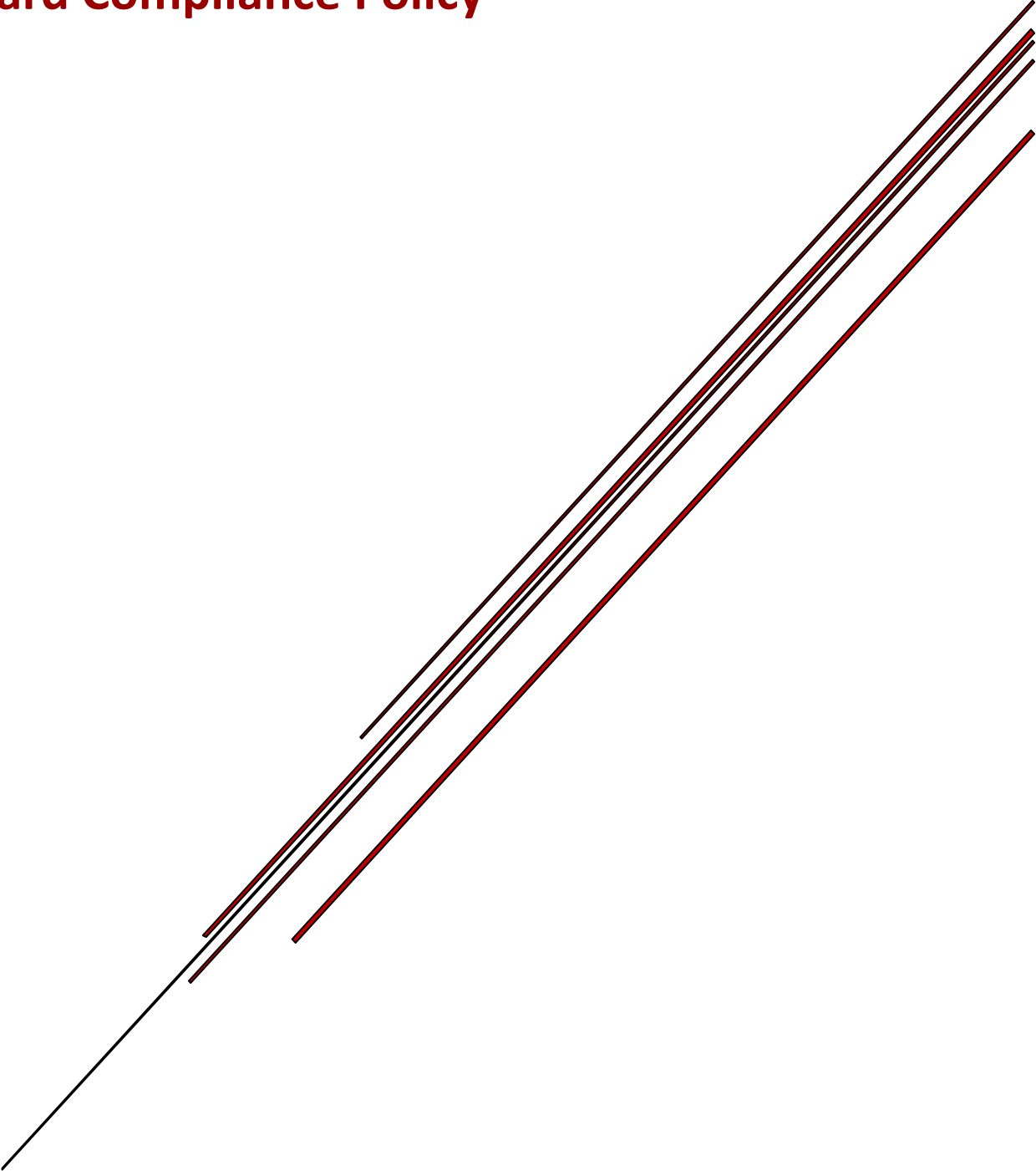


Payment Card Industry Data (PCID) Security Standard Compliance Policy



Payment Card Industry Data Security Standard Compliance Policy

STATEMENT

It is the Institute of Certified Management Accountant (ICMA)'s intent to protect all Cardholder Data (CHD) and Sensitive Authentication Data elements from unauthorized access, disclosure, and possible misuse or abuse, throughout the life cycle of the data. This policy addresses the people, processes and controls required to protect CHD received, processed, transmitted, stored by, or stored on behalf of ICMA.

The ICMA Secretariat, Branches and Regional Offices (ICMA Merchants) who accept payment via credit or debit cards, must comply with Payment Card Industry Data Security Standards (PCI DSS), must complete annual PCI DSS self-assessment questionnaires, must submit to periodic compliance inspections or audits, and may be required to submit to vulnerability scanning and penetration testing of systems which interact with and connect to the Cardholder Data Environment (CDE).

ICMA Merchants shall be responsible for costs associated with PCI DSS compliance as well as any fines or other fees associated with their non-compliance. In order to be able to interact with CHD and the CDE, ICMA employees and Third Party Service Providers (TPSPs) must also complete internal and or external training, as directed, and attest to their understanding of PCI DSS compliance and their agreement to abide by the conditions of this policy.

The policy applies to CHD received, processed, transmitted and/or stored on behalf of ICMA interests regardless of the processing channel or banking relationship, including but not limited to card swipe terminals, POS systems, e-Commerce/web applications, virtual terminals, paper forms, facsimile or telephone.

All individuals involved in the processing of debit and/or credit card payments or who otherwise are exposed to credit and/or debit card information must comply with the Payment Card Industry Data Security Standard. This includes but is not limited to:

1. Operational staff who handle, process, settle, reconcile, report on or otherwise interact with debit and credit card payments, or information.
2. Technical staff who develop and/or maintain systems and solutions used to process cardholder information including hardware, software, networks and firewalls; this can include IT security personnel, network administrators, web administrators, web developers/programmers, project managers and any individual responsible for developing, implementing, integrating, managing securing and maintaining solutions which interact with the CDE.
3. Third Party Service Providers (TPSPs) onsite or offsite (e.g. contractors, vendors, business partners, temporary help, etc.) who handle, process, settle, reconcile, report on or otherwise interact with debit and/or credit card payments, and information, or who are responsible for developing, implementing, integrating and managing solutions which interact with the Cardholder Data Environment, or which provider secure destruction of CHD.
4. PSPs with incidental access to the CDE and CHD, such as maintenance or custodial firms.

GENERAL REQUIREMENTS

All card processing activities and related technologies must comply fully with the Payment Card Industry Data Security Standard (PCI DSS). Any activity conducted or any technology employed that obstructs compliance with any portion of the PCI DSS is a violation of this policy and is subject to immediate remedial action. Unless specified otherwise, each of these requirements applies to all merchant card locations.

This policy shall be reviewed annually and updated as needed to reflect changes to business objectives, the risk environment or the applicable standards. Material policy changes will be communicated by email to ICMA merchants and through ongoing education in self-service or in-person presentation format.

ADDITIONAL GUIDANCE FOR DEPARTMENTS

Each merchant card location is responsible for compliance with PCI DSS. Please pay special attention to the following specific requirements where the ICMA merchant is usually the primary control point. ***This is not to imply that a merchant can focus on selected requirements, all merchants are required to ensure compliance with all PCI DSS requirements.***

1. Always change vendor-supplied defaults before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.
2. Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards.
3. Verify that system configuration standards are updated as new vulnerability issues are identified.
4. Verify that system configuration standards are applied when new systems are configured.
5. Verify that common security parameter settings are included in the system configuration standards.
6. Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes.
7. Implement a data retention and disposal policy
8. Do not store sensitive authentication data after authorization (even if encrypted).
9. Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).
10. Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.
11. Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).
12. Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.
13. Examine policies related to security patch installation to verify they require installation of all critical new security patches within one month.
14. Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.
15. Limit access to system components and cardholder data to only those individuals whose job requires such access.

16. Examine authentication policies/procedures to verify that group and shared passwords or other authentication methods are explicitly prohibited.
17. Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.
18. Maintain strict control over the internal or external distribution of any kind of media.
19. Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.
20. Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.
21. Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.
22. Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
23. Establish, publish, maintain, and disseminate a security policy
24. Addresses all PCI DSS requirements: This Includes:
 - an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment
 - a review at least annually and updates when the environment changes

Policy References

[Payment Card Industry \(PCI\) Data Security Standards – Document Library](#)

ICMA - Related Policies

[Privacy Policy](#)

[Privacy Management Framework](#)

[Records Management Policy](#)

Industry Resources

While the PCI SSC sets the PCI security standards, each of the card brands has its own compliance program, validation levels and enforcement policies. For that reason, please refer to the following links for more payment brand specific compliance information:

[American Express – https://www209.americanexpress.com/merchant/services/en_US/data-security](https://www209.americanexpress.com/merchant/services/en_US/data-security)

[Discover Financial Services – http://www.discovernetwork.com/fraudsecurity/disc.html](http://www.discovernetwork.com/fraudsecurity/disc.html)

[MasterCard Worldwide – http://www.mastercard.com/sdp](http://www.mastercard.com/sdp)

[Visa Inc. – http://www.visa.com/cisp](http://www.visa.com/cisp)

[Visa Europe – http://www.visaeurope.com/ais](http://www.visaeurope.com/ais)