



Cardholder Information Security Program (CISP) Compliance Questionnaire

Page 1 of 2

Visa U.S.A. is currently developing the Automated Compliance Verification Program for merchants (other than Select Merchants) to verify their compliance with CISP. Merchant enrollment in this program will be required immediately upon release (1Q04.)

To help merchants prepare for the Automated Compliance Verification Program, we have created the *CISP-Compliance Questionnaire*. Merchants may wish to complete this questionnaire to assess the security of their networks.

For technical assistance, please download the *Glossary of Terms*, which can be found in the merchant section of the CISP website at www.visa.com/cisp. For questions, e-mail AskVisa@visa.com.

Completing this questionnaire will not be a substitute for formal compliance verification.

1. Do firewalls exist on all Internet or Extranet connections? *yes* *no*
2. Are firewalls used internally to separate networks of different security levels? *yes* *no*
3. Is there a formal procedure for approving all external connections? *yes* *no*
4. Is the use of NAT or PAT implemented into your environment to hide internal network from the Internet? *yes* *no*
5. Is your firewall and router configured to conform with documented security standards? *yes* *no*
6. Is your firewall's CPU utilization monitored at least every 15 minutes? *yes* *no*
7. Are available security patches implemented within 30 days? *yes* *no*
8. Are security patches tested before they are deployed to production systems? *yes* *no*
9. Do all system changes go through a formal change control process? *yes* *no*
10. Does your cryptographic solution conform to applicable international and national standards, as well as all legal and regulatory controls? *yes* *no*
11. Are only crypto devices used that meet the approval standards and policies of your organization? *yes* *no*
12. Are there documented processes and procedures in place for encryption keys? *yes* *no*
13. Is access to keys restricted to the fewest number of custodians necessary? *yes* *no*
14. Is cardholder information retained when it is no longer needed for business reasons? *yes* *no*
15. Is a quarterly inventory audit performed to verify if any stored cardholder information exceeds your retention requirements? *yes* *no*
16. Is CVV2 or magnetic stripe data stored in the database or log files? *yes* *no*
17. Are all passwords on network devices and systems encrypted? *yes* *no*
18. Is stored cardholder data encrypted by one of the following, one-way cipher (hash indexes) such as SHA-1 (not MD5), Truncation, Simple ciphers, index tokens and PADS, strong cryptography such as PGP or Triple-DES with associated key management processes and procedures? *yes* *no*
19. Is telnet or Rlogin used for remote system administration? *yes* *no*
20. Is externally accessible account data transmitted in unencrypted format? *yes* *no*
21. Is confidential account information transmitted via unencrypted email format? *yes* *no*
22. Is strong cryptography and appropriate key controls in place to safeguard data during transmission? *yes* *no*
23. Are modems connected to the internal systems or DMZ systems? *yes* *no*
24. Is anti-virus software installed on all servers and workstations? *yes* *no*
25. Have anti-virus signature files been updated to the latest signature file? *yes* *no*
26. Is account information access on a need to know basis only? *yes* *no*
27. Are access control policies in place for data access privileges to cardholder information? *yes* *no*
28. Is firewall administration limited to only the network security administration staff? *yes* *no*
29. Is a unique username and password required for each non-consumer user that logs into a system containing cardholder information? *yes* *no*
30. Is at least one of the following methods used to authenticate all non-consumer users when accessing cardholder information: unique user name and password? token devices (i.e., SecureID, certificates, or public key)? biometrics? *yes* *no*



31. Are non-consumer users required to change their password every 60 days? yes no
32. Are non-consumer user accounts locked within 6 invalid login attempts? yes no
33. Are password protected screen savers or terminal locks used on all critical systems? yes no
34. Are group passwords allowed on critical systems? yes no
35. Are passwords required to contain both numeric and alphabetic characters? yes no
36. Are individuals allowed to submit a new password that is the same as a previous password? yes no
37. Are all internal and external dormant accounts removed? yes no
38. Are applications run on default installations of operating systems? yes no
39. Is more than one application running as the primary function of a server at any given time? yes no
40. Are the minimum hardware components met on each network component for the software to function properly? yes no
41. Are all unnecessary services disabled on a server? yes no
42. Are security controls built into the application development process? yes no
43. Has the application code been tested for vulnerabilities prior to entering production? yes no
44. Do you perform penetration testing on your network and applications at least once a year and after any significant modifications? yes no
45. Is access to all audit trails logged on all critical systems? yes no
46. Do you log the following: success and failed logins by all users, access to audit trails, deletion of objects, identification of affected components, root/administrator access origination and destination? yes no
47. Are actions related to encryption key management logged on all servers that utilize the keys? yes no
48. Do logs include date and time stamp on all critical systems? yes no
49. Are audit trails on all critical systems secured in a way that they cannot be tampered with? yes no
50. Do you review audit logs at least once a week on critical systems? yes no
51. Are audit logs retained for at least six months on all critical systems? yes no
52. Are vulnerability assessments performed on the internal and external network on a monthly basis and after updates and/or upgrades to systems? yes no
53. Is there a file integrity monitoring system in place to alert personnel of unauthorized modifications to critical systems? yes no
54. Are security alerts from the intrusion detection sensor monitored 24 hours a day, 7 days a week? yes no
55. Do you have Network IDS on perimeter related systems? yes no
56. Are the latest intrusion detection system (IDS) signatures installed on all IDS sensors? yes no
57. Are file comparison checks being reviewed on critical systems at least once a day? yes no
58. Is staff provided with adequate training on operational business and recovery plan execution responsibilities? yes no
59. Are the disaster recovery plan (DRP) and the business contingency plan (BCP) tested annually? yes no
60. Are security roles and responsibilities formally defined? yes no
61. Are critical data backed up on a daily basis? yes no
62. Are backup tapes stored in a location that does not require authorized access? yes no
63. Are all associated third parties with access to cardholder data contractually required to adhere to CISP data security requirements? yes no
64. Are information security policies documented, kept current and disseminated to all employees, vendors, contractors and partners? yes no
65. Is there a security awareness and training program in place? yes no
66. Are pertinent security alerts monitored, analyzed and distributed to appropriate personnel? yes no
67. Is a security incident response plan formally documented? yes no
68. Are employees required to sign an agreement verifying they have read and understood the policies and procedures? yes no
69. Are employees with access to cardholder data permitted to begin work prior to completion of a background investigation (including credit and criminal record checks)? yes no
70. Is access to the data center restricted and closely monitored? yes no
71. Are all paper and electronic media – e.g. computer, networking, and communications hardware, telecommunications lines, etc. – containing cardholder information located in a physically secure environment? yes no
72. Have all discarded media been erased or destroyed using a formal procedure that ensures the complete deletion of all sensitive data? yes no
73. Do you maintain strict control over the internal and external distribution of any paper or electronic media containing cardholder data? yes no
74. Are visitors, including vendors, permitted to enter data centers or access sensitive systems without an escort? yes no
75. Are visitors asked to sign out and turn in their badge or tag before leaving the building? yes no
76. Is a visitor log retained for at least three months to retain a log of physical activity? yes no
77. Are all media devices properly inventoried and securely stored? yes no



 Name of Merchant

 Signature of the Responsible Party

 Date