



85 Grove Street - Peterborough, NH 03458
voice 603-924-6079 • fax 603-924-8668

**CreditNow!® CN-3000™ & CN-3100™ AutoProcessor
Version 3.1.10.3
PCI Compliance Status
Version 1.0
28 June 2005**

Overview

Auric Systems International is in the process of achieving full compliance with the *Payment Card Industry (PCI) Payment Application Best Practices*. PCI Data Compliance is the new combined compliance procedure that includes compliance standards for American Express, Discover, MasterCard (SDP), and Visa (CISP).

This document details the current status of this process and will aid merchants in reaching their own PCI/CISP/SDP compliance.

Security is an on-going process. Auric Systems International will continue to improve our full compliance with the *PCI Payment Application Best Practices* as well as provide the information necessary to help our merchants meet their compliance needs.

The numbering system in this document matches the numbering system from the Visa CISP Payment Application Best Practices document available at:

<<http://www.visa.com/cisp>>

Required Actions

Following actions to be taken within the next 90 days:

- Card-validation codes must be deleted immediately after any transaction – whether successful or failed. Currently, we are only deleting them after a Capture.

Best Practices Compliance

Compliance Summary

TBD

Compliance Key

- Green is fully in compliance (In-Place).
- Blue is partial compliance and planned improvements.
- Yellow is not in compliance (Not In-Place).
- Red indicates improvements to be made within 90 days.

Compliance Details

1. Do not retain full magnetic stripe or CVV2 data.

1.1 Do not store sensitive authentication data subsequent to authorization (not even if encrypted): PCI Data Security Standard 3.2.

If sensitive authentication data (see 1.1.1 – 1.1.3 below) is received and erased, obtain and review methodology for erasing the data to determine the data is unrecoverable.

For each item of sensitive authentication data below, perform the following steps:

1.1.1 Do not store the full contents of any track from the magnetic stripe (on the back of a card, in a chip, etc.)

PCI Data Security Standard 3.2.1.

Subsequent to authorization, service codes, discretionary data/CVV, and Visa reserved values must be removed; however, account number, expiration date, and name may be extracted and retained.

Examine the following files created by the application, and verify that the contents of any track from the magnetic stripe on the back of the card (CVV data) is not stored under any circumstance:

- Incoming transaction data
- Transaction logs
- History files
- Debug logs
- Audit logs
- Database schemas and tables

1.1.1 Compliance Status: Full

- Application does not support card stripe.

- 1.1.2 Do not store the card-validation code (Three-digit or four-digit value printed on the front or back of a payment card (e.g., CVV2 and CVC2 data)). PCI Data Security Standard 3.2.2.
Examine the following files created by the application and verify that the three-digit or four-digit card-validation code printed on the signature panel (CVV2/CVC2 data) is not stored under any circumstance:
- Incoming transaction data
 - Transaction logs
 - History files
 - Debug logs
 - Audit logs
 - Database schemas and tables

1.1.2 Compliance Status: Partial

- Codes are not stored in: transaction logs, history files, audit logs.
- Codes are not stored once the transaction has been completed (authorized and captured).
- Codes are not stored when a transaction is 'closed'.
- Codes are not exportable.

1.1.2 Planned Improvements:

- Compliance is met only when Gateway Debug log is turned off.
- Document Gateway Debug log handling to meet compliance.
- Review appearance of Codes in the Gateway/Debug log. For in-house testing. Possibly allow unmasked in demo/test mode but always mask in live mode.
- Document best practices for handling import files after they have been imported.
- Review other ways to handle imported files in order to protect the Codes.

- 1.1.3 Do not store the PIN Verification Value (PVV)
PCI Data Security Standard 3.2.3.
PIN blocks must never be retained, even if encrypted, after
transaction authorization.
- 1.1.3.a Examine the following files created by the application, and verify that
the PIN Verification Value (PVV data) is not stored under any
circumstance:
- Incoming transaction data
 - Transaction logs
 - History files
 - Debug logs
 - Audit logs
 - Database schemas and tables
- 1.1.3.b Examine bulleted items above to verify PIN blocks are not present.
- 1.1.3 Compliance Status: In Place**
- PIN Verification Values not supported.

2. Protect stored data

- 2.1 Mask account numbers when displayed (the first six and last four digits are the maximum number of digits to be displayed).

Note that this does not apply to those employees and other parties with a specific need to see full credit card numbers.

Review displays of credit card data, including POS devices, screens, logs, receipts, etc., to determine that credit card numbers are masked when displayed.

2.1 Compliance Status: In Place

- Account numbers are never displayed in the AutoProcessor.

Planned Improvement

- Document that merchants should move away from needing the full account number exported. Either do not export the account number at all or only export the four-digit truncated value.
- Document best practices for handling import files after they have been imported.
- Review other ways to handle imported files in order to protect the Codes.

2.2 Render sensitive cardholder data unreadable anywhere it is stored, (including data on portable media, in logs, and data received from or stored by wireless networks).

The MINIMUM account information that needs to be rendered unreadable is the payment card account number PCI Data Security Standard 3.4.

Data should be rendered unreadable anywhere cardholder data is stored, even outside the payment application.

Verify that cardholder data is encrypted with strong encryption (at least 128-bit), such as Triple-DES or AES, anywhere it is stored (including databases, removable media, and logs), in accordance with PCI Data Security Standard 3.4.

2.2 Compliance Status: Partial

- Account number encrypted using 128-bit AES encryption.
- Batch files built for upload to processor are encrypted on-disk using 128-bit encryption and then decrypted on the fly when uploaded to processor.
- Batch files downloaded from processor are encrypted on-the-fly during the download process and then decrypted when read back into database.
- Auric Software complies with each processor's best practices for communications. Compliance of communication channel rests with processor providing the channel. Please contact your payment processor for details.

2.2 Planned Improvements:

- Account codes currently appear in the Gateway/Debug log. Need to be masked. Currently, Gateway logging should not be run in production mode unless closely monitored. Gateway logs should be destroyed after debugging or support issue is addressed.
- Document best practices for handling import files after they have been imported.
- Review other ways to handle imported files in order to protect the Codes.

- 2.3 Application should protect encryption keys against disclosure and misuse.
PCI Data Security Standard 3.5.
Verify the application protects encryption keys against disclosure and misuse, per PCI Data Security Standard 3.5.
- 2.3 Compliance Status: Partial**
- Standard encryption keys are protected at ASI.
- 2.3 Planned Improvements:**
- Review integration of encryption key management.
- 2.4 Application should implement key management processes and procedures.
PCI Data Security Standard 3.6.
Verify the application implements key management techniques, per PCI Data Security Standard 3.6.
- 2.4 Compliance Status: Partial**
- Access to AES encryption key for database is limited.
- 2.4 Planned Improvements:**
- Allow user to set/change encryption key.

3. Provide secure password features.

3.1 Application should require a unique username and complex password for all administrative access and access to cardholder data.

PCI Data Security Standard 8.1 and 8.2.

Note: These password controls are not intended to apply to POS access for employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for POS access by employees with administrative capabilities, or for server access controlled by the application.

Test the application to verify that usernames and passwords are required for administrative access and access to cardholder data.

3.1 Compliance Status: Partial

- Supports passwords up to 20-characters in length. Suitable for storing phrases.
- Passwords may be combination of digits, characters, and punctuation.

3.1 Planned Improvements:

- Currently allows four-character passwords. Increase to seven-character minimum.
- Increase maximum size to 40 characters for new 'long password' techniques.
- Document proper password procedures.

3.1.b Test the application to verify the application does not use (or require the use of) default administrative accounts for other necessary software (e.g., the application should not use the administrative account for database software)

3.1.b Compliance Status: In Place

- Uses embedded database not accessible over the network.

3.1.c Examine CISP Implementation Documentation (B) created by vendor to verify customers are advised against using administrative accounts for application logins (e.g., don't use the "sa" account for application access to the database). Documentation should advise customers to assign a strong password to these default accounts (even though they won't be used), and then disable or do not use the accounts. Documentation should also advise customers to assign strong application and system passwords whenever possible.

3.1.c Compliance Status: In Place

- Uses embedded database not accessible over the network.

3.1.c Planned Improvement:

- Document need for physical and operating system account security.

- 3.2 Access to PCs, servers, and databases with payment applications should require a unique username and complex password.
Examine CISP Implementation Documentation (B) created by vendor to verify customers are advised to control access, via unique username and CISP-compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data.
- 3.2 Compliance Status: Not In Place**
- Write CISP Implementation Documentation.
- 3.3 Encrypt application passwords.
PCI Data Security Standard 8.4.
Examine application password files to verify that passwords are encrypted.
- 3.3 Compliance Status: In Place**
- User's access passwords are one-way hashed and cannot be decrypted.
- 3.4 Application should allow complex passwords.
PCI Data Security Standard 8.5.
- 3.4.a Test the application to verify that complex passwords are allowed (e.g., no shared accounts or passwords, passwords changed every 90 days, password length of at least 7 characters long, passwords with both numeric and alphabetic characters, special characters are accepted, password history is maintained, etc.), per PCI Data Security Standard 8.5.8 through 8.5.15).
- 3.4.a Compliance Status: In Place**
- Complex passwords are allowed.
- 3.4.b Examine CISP Implementation Documentation (B) created by vendor to verify customers are advised how to create CISP-compliant complex passwords to access the payment application, per PCI Data Security Standard 8.5.8 through 8.5.15.
- 3.4.b Compliance Status: Not In Place**
- Write CISP Implementation Documentation.

4. Log application activity

- 4.1 Application should log all access by individual users (especially those with administrative privileges), and be able to link those activities to individual users.

PCI Data Security Standard 10.1.

Examine application settings to verify that application audit trails are automatically enabled or are available to be enabled by customers.

4.1 Compliance Status: Not In Place

- Not logging users.

4.1 Planned Improvements:

- Log user access.
- Log administrative actions.

- 4.2 Application should implement an automated audit trail to track and monitor access.

PCI Data Security Standard 10.2 and 10.3.

- 4.2.a Examine application log parameters and verify that logs contain the data required in PCI Data Security Standard 10.2 and 10.3. (A)

4.2.a Compliance Status: Not In Place

- Not logging users.

4.2.a Planned Improvements:

- Implement user logging.

- 4.2.b If application log settings are configurable by the customer or customers are responsible for implementing logging, examine CISP Implementation Documentation (B) prepared by the vendor to verify that customers are instructed on how to set CISP-compliant log settings, per PCI Data Security Standard 10.2 and 10.3.

4.2.a Compliance Status: Not In Place

- Not logging users.

4.2.a Planned Improvements:

- Implement user logging.

5. Develop secure applications

5.1 Develop web (Internet-based) software and web applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. See www.owasp.org—“The Ten Most Critical Web Application Security Vulnerabilities.” Cover prevention of common coding vulnerabilities in software development processes, to include following items.

PCI Data Security Standard 6.5.

Obtain and examine software development processes. Verify the process includes training in secure coding techniques for developers, and is based on guidance such as the OWASP guidelines. Interview a sample of developers and obtain evidence that they are knowledgeable in secure coding techniques. Alternatively, verify that an external code review or application penetration test was done based on OWASP guidelines (or similar secure coding guidance), and that all coding vulnerabilities were corrected and re-evaluated. For web-based (Internet) applications, determine that processes are in place to determine that applications are not vulnerable to the following:

- 5.1.1 Unvalidated input.
- 5.1.2 Broken access control (e.g., malicious use of user IDs).
- 5.1.3 Broken authentication and session management (use of account credentials and session cookies).
- 5.1.4 Cross-site scripting (XSS) attacks.
- 5.1.5 Buffer overflows.
- 5.1.6 Injection flaws (e.g., SQL injection).
- 5.1.7 Improper error handling
- 5.1.8 Insecure storage
- 5.1.9 Insecure configuration management.

5.1 Compliance Status: In Place

- Application does not have a Web interface.

5.2 Develop software applications based on industry best practices and include information security throughout the software development life cycle. Include the following:

PCI Data Security Standard 6.3.

Obtain and review written software development processes to confirm they are based on industry standards and that security is included throughout the life cycle.

From review of written software development processes, inquiry of software developers, and review of relevant data (network configuration documentation, production and test data, etc.), determine the following:

5.2.1 Testing of all security patches and system and software configuration changes before deployment.

PCI Data Security Standard 6.3.1.

All changes (including patches) are tested before being deployed.

5.2 Compliance Status: Partial

- Development uses industry practices.
- Security is considered throughout design and development process.

5.2 Planned Improvements:

- Formally document procedures.

5.2.2 Removal of non-essential (test, development, etc.) application accounts, usernames, and passwords before applications are released to customers.

PCI Data Security Standard 6.3.5 and 6.3.6^(A)

Non-essential application accounts, usernames, and passwords are removed before application is released to customers.

5.2.2 Compliance Status: In Place

5.2.3 Removal of unnecessary and insecure services and protocols (e.g., NetBIOS, file-sharing, Telnet, unencrypted FTP, and others). These services and protocols should not be used or required by the application.

PCI Data Security Standard 2.2.2.

Review system services, daemons, and protocols enabled or required by the application. Verify that unnecessary and insecure services or protocols are not enabled by default or required by the application (e.g., FTP is not enabled, or is encrypted via SSH or other technology).

5.2.3 Compliance Status: In Place

5.2.4 Review of custom code prior to release to production or customers, to identify any potential coding vulnerability.
PCI Data Security Standard 6.3.7.

5.2.4 Compliance Status: In Place

5.2.4.a Confirm the vendor performs code reviews, and that individuals other than the originating author of the code perform the reviews.

5.2.4.a Compliance Status: In Place

5.2.4.a Planned Improvement:

- Document review policy.

5.2.4.b Confirm that code reviews occur for new code as well as for code changes.

5.2.4.b Compliance Status: In Place

5.4.2.b Planned Improvement:

- Document review policy.

6. Protect wireless transmissions

6 Compliance Status: In Place

- Application does not support wireless transmissions.

7. Test applications to address vulnerabilities.

7.1 Software developers should establish a process to identify newly discovered security vulnerabilities (e.g., subscribe to alert services freely available on the Internet), test their applications for vulnerabilities, and for timely development and deployment of security patches and upgrades. Updates and patches should be delivered in a secure manner with a known chain-of-trust. Any underlying software or systems that are provided along with the payment application (e.g., web servers) should be included in this process. PCI Data Security Standard 6.2.

Obtain and examine development processes. Verify the process includes:

- Using outside sources for security vulnerability information
- Testing of applications for new vulnerabilities,
- Delivery of patches and updates in a secure manner with a known chain-of-trust, and
- Timely development and deployment of patches to customers.

Also verify that all software provided with the payment application (e.g., web servers) is included in this process.

7.1 **Compliance Status: Partial**

- Auric Systems tracks CERT and BugTraq mailing lists for new vulnerabilities.
- Auric Systems subscribes to mailing lists for components used in our products.
- Applications are tested for vulnerabilities.
- Auric Systems responds in a timely manner when new vulnerabilities are disclosed or patches are provided.
- Application is self-contained. No additional software is provided with the payment application.

7.1 **Planned Improvement:**

- Process needs to be formalized and documented.

8. Facilitate secure network implementation

8.1 The payment application should be able to be implemented into a secure network environment. Application should not interfere with use of network address translation (NAT), port address translation (PAT), traffic filtering network devices, anti-virus protection, patch or update installation, or use of encryption.

PCI Data Security Standard 1, 3, 4, and 5.

Test the application in a lab to obtain evidence that it can run in a network with NAT, PAT, traffic-filtering devices, anti-virus software, and encryption. Verify that the application does not inhibit installation of patches or updates to other components in the environment.

8.1 Compliance Status: In Place

- Able to run in a secured network environment.

9. Cardholder data must never be stored on a server connected to the Internet

9.1 The payment application should not require that the database server and web server be on the same server, or in the DMZ with the web server.

PCI Data Security Standard 1.3 and 1.3.5.

9.1.a To verify that the application stores cardholder data in the internal network, and never in the DMZ, obtain evidence that the application does not require data storage in the DMZ, and will allow use of a DMZ to separate the Internet from systems storing cardholder data (e.g., application should not require that the database server and web server be on the same server, or in the DMZ with the web server).

9.1.b If customer could store cardholder data on a server connected to the Internet, examine CISP Implementation Documentation (B): prepared by vendor to verify customers are told not to store cardholder data on Internet-accessible systems (e.g., web server and database server should not be on same server.)

9.1 Compliance Status: Partial

- This is a desktop application and not designed for direct exposure to the Internet.

9.1 Planned Improvements:

- Write CISP Implementation Documentation.

10. Facilitate secure remote software updates

- 10.1 If software updates are delivered via remote access into customers' systems, software vendors should tell customers to turn on modem only when needed for downloads from vendor, and to turn off immediately after download completes. Alternatively, if delivered via VPN or other high-speed connection, software vendors should advise customers to properly configure a personal firewall product to secure "always-on" connections.

PCI Data Security Standard 1.3.10 and 12.3.

If the vendor delivers software and/or updates via remote access to customer networks, examine CISP Implementation Documentation (B) prepared by vendor, and verify it contains:

- Instructions regarding secure modem use, per PCI Data Security Standard 12.3.
- Recommendation for use of a personal firewall product if computer is connected via VPN or other high-speed connection, to secure these "always-on" connections, per PCI Data Security Standard 1.3.10.

10.1 Compliance Status: In Place

- Software updates are not delivered via remote access into customer's systems.

10.1 Planned Improvements:

- Review how updates are delivered to increase reliability and security through signed packages.

11. Facilitate secure remote access to application

- 11.1 If employees, administrators, or vendors can access the application remotely, access should be authenticated using a 2-factor authentication mechanism. The application should allow for technologies such as RADIUS or TACACS with tokens, or VPN with individual certificates.
PCI Data Security Standard 8.3.
- 11.1.a If customer can access the application remotely, examine CISP Implementation Documentation (B) prepared by the software vendor, and verify it contains instructions regarding secure remote access to the network, including the use of two-factor authentication (username/password and an additional authentication item such as a token or certificate).
- 11.1.b If vendor accesses customers' sites remotely for application support, etc., verify the vendor has processes implemented to:
- Restrict access to passwords to authorized vendor personnel,
 - Protect customers' passwords from unauthorized use,
 - Establish customer passwords according to Best Practice 3, above, and PCI Data Security Standard 8.1, 8.2, 8.4, 8.5 (or that the vendor provides such instruction to the customer in the CISP Implementation Documentation (B)).
- 11.1.c If the application requires, or supports use of, a remote access product for remote vendor or customer access (e.g., pcAnywhere), examine CISP Implementation Documentation (B) prepared by the software vendor, and verify that customers are instructed to use and implement all security features of the remote access software. See (E) for more details.
- 11.1 Compliance Status: In Place**
- Application includes a Remote Console that connects to the application using AES encrypted communications channel.
 - Transactions cannot be accessed via the remote console.

12. Encrypt sensitive traffic over public networks.

- 12.1 Use strong cryptography and encryption techniques (at least 128 bit) such as Secure Sockets Layer (SSL), Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPSEC) to safeguard sensitive cardholder data during transmission over public networks. PCI Data Security Standard 4.1.

If the application allows data transmission over the Internet, examine CISP Implementation Documentation (B): prepared by the vendor, and verify the vendor recommends use of SSL for secure data transmission.

12.1 Compliance Status: In Place

- Auric Software complies with each processor's best practices for communications. Compliance of communication channel rests with processor providing the channel. Please contact your payment processor for details.

- 12.2 The application should never send cardholder information via unencrypted e-mail.

PCI Data Security Standard 4.2^(A)

- 12.2.a If the application allows and/or facilitates sending of email, verify that email encryption features are provided.

- 12.2.b If the application allows and/or facilitates the sending of email, examine CISP Implementation Documentation (B) prepared by the vendor, and verify the vendor recommends use of email encryption for sending sensitive emails (with cardholder data).

12.2 Compliance Status: In Place

- Application does not send email.

13. Encrypt all non-console administrative access.

13. Use technologies such as SSH, or SSL/TLS for web-based management and other non-console administrative access. Telnet or rlogin must never be used for administration.

PCI Data Security Standard 2.3.

If application or server allows non-console administration, examine CISP Implementation Documentation (B): prepared by vendor, and verify vendor recommends use of SSH or SSL/TLS for secure administrative access.

13 Compliance Status: Not In Place

- Write CISP Implementation Documentation.

References

For references to PCI Data Security Standard, see <http://www.visa.com/cisp>

For references to CISP Implementation Documentation, Visa suggests vendors document the configuration specifics in this document and strongly advise their customers that the application has to be configured as stated. Vendors may tell customers something similar to “this application, when implemented according to CISP Implementation Documentation, and when implemented into a secure environment, will not keep the customer from being CISP compliant”.

<http://www.owasp.org>, “The Ten Most Critical Web Application Security Vulnerabilities,” 2004 Update, January 27, 2004

See Visa CISP web site at <http://www.visa.com/cisp> for definitions of merchant levels and other program details.

For example, features like usernames with complex passwords, password protection for dial-in and dial-out files, automatic log off when call is completed, encrypting session traffic, limiting logon attempts, and logging failed attempts are features available in most remote access software, but not enabled by default.

###