9/12/13	8/5/09	1 of 7	2.65
(Effective)	*(Supersedes)*	*(Page)*	*(Number)*

SUBJECT: **PAYMENT CARD INFORMATION POLICY**

SCOPE: All Companies

PURPOSE: To establish guidelines for managing Payment Card Information.

1.0 Introduction

The Payment Card Industry Data Security Standard and state and federal statutes require companies to: (i) protect Payment Card Information and secure computer systems, software, and networks where this information resides against theft, loss, damage, and unauthorized access and use; (ii) conduct an annual assessment of how such information is managed, stored and processed; and (iii) issue a Policy that memorializes how the Company complies with the Standard. This Policy is designed to ensure that the Company complies with these requirements.

2.0 Definitions

For purposes of this Policy:

2.1. "Payment Cards" are cards that are presented to make a payment to the Company, including credit cards, debit cards, charge cards, smart cards, NFC cards/device and similar devices.

2.2 "Payment Card Industry Data Security Standard" (PCI DSS) is a standard created by the Payment Card Industry Security Standards Council[1] to establish security requirements for members, merchants and service providers that store, process or transmit cardholder data.

2.3 "Payment Card Information" includes the following information collected by the Company relating to Payment Cards: Payment cardholder names; Payment Card numbers, expiration dates, card validation values or codes (the three or four-digit numbers on the front or back of a Payment Card), personal identification numbers ("PINs"), and other data stored on Payment Cards.

[1] The Payment Card Industry Security Standards Council is an organization developed by the major credit card companies (e.g., MasterCard, Visa, American Express, etc.).

3.0 Disclosure of Payment Card Information

Employees must protect Payment Card Information in accordance with this Policy and other Company policies.[2] An employee may not disclose Payment Card Information to anyone **outside** the Company unless the employee has a legitimate business purpose and the disclosure is approved by an appropriate person in the Business Unit (who is at least an SVP or above), and after prior consultation with either the VP of Compliance Support or the applicable Business Unit attorney. All such disclosures must be documented. (See also Section 10.0, which discusses sharing Payment Card Information with vendors.) A Business Unit employee may also release Payment Card Information as required by law (e.g., in response to a subpoena; to comply with contractual obligations), but must first consult with either the VP of Compliance Support or the applicable Business Unit attorney, unless the disclosure has already been approved by the Legal Department (e.g., approved disclosures in response to law enforcement legal process). Employees must also limit the distribution of Payment Card Information **within** the Company to only those employees who have a need to know such information in order to conduct Company business, and must distribute such information in accordance with the direction provided in Sections 6.0 and 7.0.

4.0 Reporting Data Security Incidents.

Further, employees must report any actual or suspected incidents where the Company has lost control or possession of customer or employee Payment Card Information (whether reported by another employee, a customer, third party, or otherwise), and any data breaches, suspected data breaches, or other data security incidents to his or her manager, who must report the incident or breach to either the VP of Compliance Support or the applicable Business Unit attorney. The employee and/or manager may choose to notify the Legal Department by sending an email explaining the incident to **databreach@cablevision.com** (but note that any such email must not contain Payment Card Information, see Section 6.0 for more information), but in any event must make sure that the Legal Department is aware of the breach as soon as possible. See the Data Breach Notification Policy for a definition of what constitutes a data breach. The Company's Security Incident Response Team will be notified, and the Computer Security Incident Response Plan implemented, if appropriate.

[2] See the Confidential Information Policy; the Data Breach Notification Policy; the Computer Security Incident Response Plan; and the Record Management Policy.

9/12/13	8/5/09	3 of 7	2.65
(Effective)	*(Supersedes)*	*(Page)*	*(Number)*

SUBJECT: PAYMENT CARD INFORMATION POLICY

5.0 Storing Payment Card Information

Employees should retain electronic and hard copy records containing Payment Card Information in accordance with this Policy, the Company's Record Management Policy and Record Retention Schedule. In any event, employees must **never** store the following information on Company or vendor systems, or in hard copy format:

- Full magnetic stripe data
- Payment Card Validation Values/Codes
- PINs

*Employees may store payment card numbers, cardholders' names and expiration dates, but all payment Card numbers that are stored electronically **must** be encrypted, truncated, or otherwise rendered unreadable*. If a software application is not capable of encrypting or truncating payment card numbers, then in those limited circumstances the business must consult with the SVP of EIT, with input from the VP of Compliance Support or the applicable Business Unit attorney, to determine how to proceed.

5.1 Storing Electronic Payment Card Information

Employees must store electronic Payment Card Information only in applications, databases, and other electronic forms that have been approved by the SVP of EIT, and that are located on Company-owned servers, or by a vendor specifically authorized by the Company to store Payment Card Information. Employees and vendors must **never** store Payment Card Information on laptops, PDAs, CDs, portable hard drives, USB drives, or any other removable media, *except* on media (e.g., tapes, disks, etc.) used by Enterprise IT to back up Company-approved applications. Employees with a legitimate business need to store Payment Card Information on a portable device should first discuss with an SVP or above in their Business Unit or Corporate Department, and obtain prior approval from the SVP of EIT, and either the VP of Compliance Support or the applicable Business Unit attorney. Employees may not store Payment Card Information on any computer or other media that is **not** Company-owned.

5.2 Storing Hard Copy Payment Card Information

When handling and storing Payment Card Information in hard copy form, employees must:

- Never leave Payment Card Information in an insecure location, such as on a desk top, while away from their work spaces; and
- Ensure that hard copy records containing Payment Card Information are stored in locked file cabinets or other secure locations when not in use.

9/12/13	8/5/09	4 of 7	2.65
(Effective)	*(Supersedes)*	*(Page)*	*(Number)*

SUBJECT: PAYMENT CARD INFORMATION POLICY

6.0 Electronic Transmissions of Payment Card Information

Employees may not transmit Payment Card Information electronically, whether through emails, instant messages, text messages or file transfer protocols, including transmissions that are made within the Company's computer systems or network. Employees with a legitimate business need to send Payment Card Information electronically, *and* where other methods of transmission will be ineffective, must obtain prior approval from an SVP or above in their Business Unit or Department, and then consult with EIT and either the VP of Compliance Support or the applicable Business Unit attorney, about how to do that in a secure fashion. An employee who receives Payment Card Information electronically (regardless of whether the information was sent via an encrypted message), should immediately print the message, delete it from the system, and refer to Sections 5.2 and 8.0 of this Policy for guidance on proper storage and disposal.

7.0 Physical Removal of Payment Card Information.

Employees should not remove any tangible items that contain Payment Card Information from Company premises unless they need to do so in order to perform their job for the Company. In that case, employees must obtain prior approval from an SVP or above with the relevant Business Unit or Department and consult with either the VP of Compliance Support or the applicable Business Unit attorney as needed.

8.0 Printing and Disposing of Payment Card Information.

Employees should avoid printing any documents containing Payment Card Information unless absolutely necessary (or to comply with Section 6.0). If it is necessary to print documents containing Payment Card Information, employees should manage such documents securely (e.g., placing the document in a locked drawer or file cabinet), and should properly dispose of the document as soon as it is no longer needed. Proper disposal requires employees to shred hard copy records (or use a Company-approved vendor who provides secure shredding), and delete or erase electronic Payment Card Information once it is no longer needed.

9.0 Remote Access to Electronic Payment Card Information

Remote access to electronic Payment Card Information is limited to employees and vendors specifically authorized by the SVP of EIT (see Section 11.1), who should consult with either the VP of Compliance Support or the applicable Business Unit attorney as needed. The SVP of EIT will maintain a list of employees and vendors who have remote access and update the list as needed. In any event, employees and vendors remotely accessing databases with electronically stored Payment Card Information must not copy and paste or otherwise store Payment Card Information on any device or in any software or other application that is not authorized by the Company to store Payment Card Information.

10.0 Vendors Who Manage Payment Card Information

Employees should not permit vendors to have access to Payment Card Information, or be connected to Company systems that store, process or transmit Payment Card Information, until they take the following steps: (1) obtain prior approval from an SVP or above within the relevant Business Unit or Department, with consultation from either the VP of Compliance Support or the applicable Business Unit attorney; and (2) work with the applicable Business Unit attorney to have the vendor verify in writing that they are PCI DSS compliant, (as well as compliant with any other applicable laws, regulations and industry standards). Best practice is to obtain a contractual commitment that the vendor is and will continue to ensure that they remain PCI DSS compliant. Additionally, the vendor must sign an annual Vendor Statement of Compliance with Data Protection Requirements Form. Please consult with the VP of Compliance Support or the applicable Business Unit attorney to learn more.

11.0 Compliance. Various Corporate Departments and/or Business Units have an obligation to assist the Company in complying with this Policy and the PCI-DSS. Specifically:

11.1 Compliance Support is responsible for:

11.1.1 Advising the relevant Corporate Departments (including Enterprise IT) and Business Units regarding changes in laws, standards, regulations, or other mandates that address Payment Card Information;

11.1.2 Revising this Policy, with the support of EIT and the relevant Business Unit(s);

11.1.3 Providing Legal guidance with reference to the annual review explained in Section 11.3.5;

11.1.4 Participating in and/or overseeing internal investigations regarding actual or potential breaches of Payment Card Information, in compliance with the Company's Security Incident Response Plan (CSIRP) as needed**,** and managing any resulting communications with law enforcement agencies**;** and

11.1.5 Developing and issuing periodic communications and/or trainings regarding the proper management of Payment Card Information, with the support of EIT, Human Resources and others as needed.

11.2 The SVP of Internal Audit and/or his or her designee will be responsible for monitoring the annual review process, as explained further in Section 11.3.5.

11.3 The Company's Chief Information Officer, and/or his or her designee is responsible for:

11.3.1 Ensuring the Company's computer systems, software, and networks where Payment Card Information resides are protected against theft, loss, damage, and unauthorized access and use;

11.3.2 Implementing technical and/or procedural controls to mitigate threats and risks to Payment Card Information, and the systems that store, process or transmit Payment Card Information (e.g., quarterly security scans, annual penetration tests and other procedures require by PCI DSS);

11.3.3 Notifying Compliance Support of any changes in the Company's systems that affect any aspects of how Payment Card Information is processed, managed, or stored;

11.3.4 Conducting periodic reviews as necessary of information security controls (e.g., policies, procedures, or technical controls, etc.) and information systems to ensure that new threats and risks to the Payment Card Information and systems that store, process or transmit Payment Card Information, are identified;

11.3.5 Designating EIT employees to assist in an annual review to ensure that the Company complies with this Policy and the PCI-DSS (e.g., attending periodic meetings to review the relevant Self-Assessment Questionnaire and associated standards; reviewing and revising (as needed) the relevant computer systems; etc.), with support from relevant Business Unit employees and Compliance Support; and

11.3.6 Assisting Compliance Support in updating this Policy, as determined necessary by Compliance Support.

11.4 An SVP or above (or their designee) from the relevant Business Unit that owns the merchant number/merchant relationship (e.g., Billings and Collections) is responsible for:

11.4.1 Designating employees to assist in an annual review to ensure that the Company complies with this Policy and the PCI-DSS (e.g., attending periodic meetings to review the relevant Self-Assessment Questionnaire and associated standards, etc.), including documenting the review and communicating with the relevant acquirer bank or card association, with support from EIT and Compliance Support; and

11.4.2 Notifying Compliance Support of any changes in the Company's systems that affect any aspects of how Payment Card Information is processed, managed, or stored.

12.0 Reporting Non-Compliance. All employees with any information that the Company is not complying with this Policy must report such non-compliance to the Legal Department, Compliance

9/12/13	8/5/09	7 of 7	2.65
(Effective)	*(Supersedes)*	*(Page)*	*(Number)*

SUBJECT: PAYMENT CARD INFORMATION POLICY

Support and/or the Internal Audit Department. Employees may also report non-compliance to the Company's Integrity Hotline at 1-888-310-6742.

13.0 Enforcement

The Company may take steps to monitor and ensure that employees and vendors that handle, process, store, and dispose of Payment Card Information, and the computer systems, software and networks where this information resides, are in compliance with this Policy. Enforcement may include:

- Reviewing the systems that store, process or transmit Payment Card Information and the information that is stored, processed or transmitted on such systems;
- Investigating allegations of abuse or misuse of systems and Payment Card Information; and
- Taking all necessary actions permissible under the law to prevent theft or misuse of Payment Card Information.

Employees and vendors shall not use any unauthorized codes or encryption techniques in an effort to circumvent or bypass such monitoring procedures. Employees that violate this Policy may be subject to corrective action, including separation from the Company.