1. Introduction

This policy provides essential information for everyone tasked with handling credit and debit cards, credit and debit card data and the systems processing such data within YU. It is designed to ensure we can meet the standards required by the Payment Card Industry's Data Security Standard (PCI-DSS), which YU is obliged to meet in order to be able to process credit card payments.

2. Scope

All environments within Yeshiva University where credit and debit cards are handled.

3. Compliance Requirements

Compliance with this policy is mandatory. Failure to follow this policy will be considered as gross misconduct and may result in disciplinary action, up to and including summary dismissal. Compliance with policies is primarily enforced through process and standard documents that need to be developed by each business unit on how they perform their day to day activities in accordance with these policies.

4. Yeshiva University Policies

YU Policies affecting YU IT entirely – not just the YU cardholder data environment – can be found at: http://www.yu.edu/its. Where any contradictions arise within the cardholder data environment, this policy takes precedent.

POLICY

1. General

System users shall not send confidential data, such as credit or debit cardholder data, unencrypted, via end-user messaging technologies such as, e-mail, instant messaging or chat without using an approved encryption solution. Where a solution is not available the data shall not be sent via any of these methods.

All employees, 3rd parties or contractors shall not attach or use within YU cardholder data environments network devices including but not limited to modems, remote-access technologies, wireless technologies, removable electronic media, personal laptops, tablets, PDAs, iPods or personal storage media (e.g. memory sticks).

Users shall not store confidential data, such as credit and debit cardholder data on local hard drives, floppy disks, or other external or mobile media. If anyone must store confidential data on a hard disk that is not in a securely protected environment, they must report this to *Information Security Manager* so that the data can be encrypted with YU approved encryption solutions.

All employees, 3rd parties or contractors are responsible for the YU assets, particularly confidential data, that they use to carry out their function. Any suspicious activity or suspect breach in security must be immediately report to the *Information Security Manager*.

Ensure documents containing credit and debit cardholder data are securely locked away.

2. Credit Card Handling

2.1. Scope

This section provides the minimum mandatory requirements that need to be applied to all employees that handle or come across credit or debit cardholder data, in any format within the YU environment. Furthermore any third party that uses or accesses any of YU's credit cardholder data, either physically or logically must also comply with this section. It is not YU's intention to hold cardholder data, however, this section outlines what to do if such a situation arises.

2.2. Policy Statements

2.2.1. General

Failure to protect card data can lead to large fines from banks, expensive investigations, expensive litigation, loss of reputation and in the worst case scenario, withdrawal of the ability to take payment by credit cards; which would greatly hinder YU's ability to conduct business.

No staff should handle cardholder data unless you have explicit authorization to do so

Cardholder data should only be handled in such a manner as is explicitly authorized by job roles.

2.2.2. Card Data Definitions and Requirements

Credit Card Data' means most of the information on a Credit Card or Debit Card and includes the long 16 digit card number (Primary Account Number - PAN). It also includes the issue and expiry dates and the cardholder's name. The three or four digit security code on the back or front of the card (depending of type of card) is known as the Card Verification Value (CVV). The PAN must always be encrypted when electronically stored and the Cardholder data, if stored with the PAN must be protected.

The CVV should be handled with great care and should never be written down or stored **anywhere**, whether on a piece of paper, a form, in a database, in a spreadsheet or any other electronic format, even if encrypted. The only exception to this is where you are taking a payment and need to store the CVV temporarily (pre-authorization) whilst you arrange to take the payment. After the transaction has been authorized the CVV data *must be destroyed immediately*.

If during the performance of your job you can see, by error or intention, a full card number when it is not required for you to do your job, please report this to Information Security Manager. If however your job requires that you need access to the full credit card number and it is not mentioned in your job description, please report this to your line manager so that they can update your job description and confirm it with HR.

2.2.3. Card Data Handling Requirements

Credit card data should NOT be stored in YU's environment

If for any reason credit card data needs to be stored, then:

- Credit card data is classified as confidential, in accordance with the YU Information Classification Standard. This means that if credit card data is stored for whatever reason it must be protected. If it is stored in systems, it has to be encrypted. If it is stored on paper it must be locked away at all times unless in use. In the first instance, report **any** credit card number storage to the Information Security Manager.
- Do not store credit card data on laptops, desktop computers, file shares, memory sticks, CDs or floppy disks unless these are on approved systems. If in doubt, do not store the data.
- Do not store credit card data in spreadsheets and other office documents, unless specifically required for your work, approved in writing by the Information Security Manager and the document is encrypted to AES-256 bit standard.
- Any card data on YU systems must be reported to the Information Security Manager immediately upon discovery.

2.2.4. Printing of Documents Containing Card Data

There will be no cardholder data within YU and therefore there will be no printing of cardholder data. Should cardholder data exist, printing of it is expressly forbidden.

2.2.5. Handling Documents Containing Card Data

There are numerous cases where card data is legitimately stored on paper, be it a chargeback letter, a fraud document, an exceptions report etc. This data needs to be

retained only until the systems are back up again and card data can be processed electronically.

2.2.6. Vigilance and Awareness

Credit card data can be inadvertently left on printers, fax machines, on a desk, on a screen, in a clear email (although this is against the PCI-DSS Data Management Policy), in the 'trash' or 'recycle bin' file on a computer, in a temporary file, memory swap files etc.

A good example of unusual locations to find credit card data is in call recordings. Occasionally telephone calls are recorded for quality and security purposes. These recorded calls can obviously contain the customer giving us their credit card details. To use these call recordings for training purposes the calls should be edited beforehand to remove any mention of a customer's credit or debit card details. So if you are listening to a call recording for training purposes, you should not hear a credit card number.

If however, as part of your job you are required to listen to complete calls (for example for real-time quality checking) this is acceptable. However, storing such calls for any length of time must be done securely within an approved storage system.

Each employee or contractor is responsible to protect YU assets which include all forms of data. It is therefore important that, should you see any credit card data or other confidential data in a place that is insecure, inappropriate or where you do not expect to see it, even if your role includes the ability to work with credit card data you must:

a. secure the data, e.g. lock it in your desk,

b. report it to your manager and

c. report the incident to the Information Security Manager immediately.

3. PCI-DSS Cardholder Data Management

3.1. Scope

This section provides the minimum mandatory requirements that need to be applied to all data created, transmitted, stored or managed by YU within the Cardholder Data Environment; be that data in hard (e.g. paper) or soft (e.g. hard disk) formats. Furthermore any third party that uses or accesses any of YU's data within the CDE, either physically or logically must also comply with this policy.

3.2. Statements

3.2.1. PCI-DSS Data Retention

Cardholder data must not be retained on any YU system.

Other data referring to the cardholder data environment will be treated as outlined below.

3.2.1.1. Payment Card Data

Payment card data will not be stored within YU.

3.2.1.2. Revenue Protection Correspondence

This refers to all correspondence relating to charge-backs, revenue protection and fraud prevention. These will typically be paper copies and must be destroyed by cross-cut shredding once they have met their retention period.

3.2.2.3. Information Systems and Physical Location Documentation
All documentation relating to Information Systems within the PCI-DSS CDE, including network diagrams, firewall access, system configuration, system passwords and backup documentation must be held securely with privileged access.

3.2.2.4. Audit Logs
There will be no cardholder data in YU, therefore no audit logs fall in scope.

3.2.2. Cardholder Data Security

Within the Cardholder Data Environment:
Confidential data in the cardholder data environment must not be sent to any external party without authorisation from the Division head and the data owner, e.g. 2 separate people.
All data physically sent to an external source must be sent via secure courier or other secure delivery method, as approved in advance by the data owner to ensure it is accurately tracked.
All data must be stored in accordance with its classification regardless of the media it is held on.

All physical backup media must be sent via secure transit.
All data sent externally must be logged and those records retained for a period of 12 months.
All physical (paper) and electronic confidential data, especially if it contains cardholder data, must have physical security controls applied at all times.
All confidential data must be stored securely and all access to be secure and controlled based on a user's "need to know".
Confidential data, especially cardholder data, stored on any form of media, e.g. CD's, backups, hard drives, paper etc, must be inventoried to ensure the secure storage is managed and recorded.
Periodic media inventories must be performed on a minimum of an annual basis. Evidence of media inventories will be retained.
All confidential data, such as cardholder data, access passwords must be encrypted when stored. Stored data includes all logical locations, e.g. databases, servers, log files, debugging files, backups, reports etc.
All system and application passwords are classified as confidential and need to be encrypted in all forms of transmission as well as in storage.

3.2.3. Cardholder Data Storage Locations
YU does not store cardholder data

3.2.4. Cardholder Data Disposal
YU should not hold any cardholder data.

However, should cardholder data exist on any system, the following conditions apply:

All data must be securely disposed of when no longer required regardless of the media or application type on which it is stored.

All hard copies of cardholder data must be manually destroyed as soon as it has reached the end of its retention period. A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.

YU requires that, before they leave YU, all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.

All cardholder information awaiting destruction must be held in lockable storage containers clearly marked “To Be Shredded” - access to these containers must be restricted.

3.2.5. Mobile Data
Cardholder data will NOT be stored on mobile devices.

4. Physical Security

4.1. Device Checking
Devices must be periodically inspected by staff to look for tampering (for example, addition of card skimmers to devices) or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device)

Personnel will be trained to be aware of suspicious behavior and to report tampering or substitution of devices

Any tampering or suspicion that tampering has taken place must be reported to the *Information Security Manager*

4.2. Personnel Checking
Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices

Do not install, replace, or return devices without verification

Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices)

Report suspicious behavior and indications of device tampering or substitution to the *Security Office*

5. Acceptable Use

The information system facilities of YU are provided for business purposes and use of these facilities must be authorized in accordance with the '**Conditions of Use of IT Facilities**' and the **Access Control Policy**.

It is mandatory for all users of systems and equipment within YU's cardholder data environment to adhere to the terms of 'Conditions of Use' and the Access Control Policy.

Employees and other users who deliberately breach the terms of this policy will be subject to disciplinary action up to and including summary dismissal. Serious offenders are liable for prosecution under the applicable laws.

Every user is responsible for the proper use of the equipment they have been assigned and must comply with YU's policies and all applicable laws.

Users must ensure anti-virus is installed, up-to-date and operating on all YU devices**, and report any failure of provision to the IT Help Desk**.

It is prohibited to install and download any software on YU computers within the cardholder data environment, unless authorized by the *Information Security Manager*.

Any IT Systems equipment not belonging to YU should not be installed on the YU network within the cardholder data environment, unless permitted, with the authorization of the *Information Security Manager*. Any such equipment must adhere to the standards within this document.

6. Responsibilities

All users within the cardholder data environment include all permanent (direct hire), temporary and contract staff who use YU computer systems. All users must use the IT systems, information and equipment in accordance with YU security policies and procedures. Users are responsible for:

1. Familiarizing themselves with and adhering to the policies and procedures applicable to their area of responsibility;
2. Protecting YU equipment issued to them against unauthorized access and damage;
3. Using YU equipment for business purposes only;
4. Protecting YU and customer information against unauthorized access and loss;
5. Not disclosing their passwords or sharing user accounts;
6. Ensuring that YU IT systems and facilities (e.g. email or Internet) are used in accordance with the '**Computer Policy Handbooks'** at YU;
7. Clearing desks of all sensitive material and logging off or locking workstations at the end of the day and when leaving their desk;
8. Not removing equipment, information or any other YU property from the organization's premises without authorization;
9. Not connecting personal equipment to YU networks within the cardholder data environment;
10. Not installing, copying or modifying any software on YU equipment without authorization;

11. Immediately reporting security incidents to the information Security team (infosec@yu.edu).

Responsibilities for carrying out specific information security duties will be defined in job descriptions where applicable.