HEALTH SERVICES UNION
Payment Card Industry Data Security Standard (PCI-DSS) Policy

Purpose

The Payment Card Industry Data Security Standard (PCI-DSS) is the global data security standard established by the major credit card companies which their clients must adhere to accept payment by cards, and to store, process, and/or transmit cardholder data regardless of their size and/or the volume of payment card transactions.

The PCI-DSS thus acts as a guideline for operational and technical compliance requirements to manage security concerns associated with the widespread use of payment cards and protect cardholder data.

While PCI-DSS compliance is not legally mandated, there are repercussions for non-adherence such as significant financial and reputational risks. Failure to comply with PCI-DSS can result in i.) fines and penalties imposed by payment card institutions and banks; ii.) monetary costs associated with legal proceedings, settlements, and judgements; iii.) inability to accept payment cards for payment.

The purpose of this document is to advise of actions the HSU can take to maintain PCI-DSS compliance and expand on the justifications for doing so as mentioned above.

Policy Statement

The HSU has entered into a merchant agreement with credit card providers and is obligated to protect cardholder information received with any payment transaction.

To ensure the HSU maintains compliance with the PCI-DSS, a set of controls are enforced to safeguard the processing, transmission, storage, and disposal of cardholder data of all payment card transactions with the aim of preventing payment card fraud.

Controls required include:

a. Acceptable use of computer equipment within the HSU
b. Physical constraints to protect data and facilities in the Card Data Environment (CDE)
c. A security configuration policy for all payment CDEs owned, operated, or managed by the HSU
d. Security requirements for the development of any payment application software or web-based applications that transmit, process, or store payment card information
e. A storage and disposal procedure for all confidential or sensitive data after payment card details are processed
f. Control of all backup subsystems and data therein of the CDE
g. An operational and contractual procedure for sharing confidential or sensitive data with third parties
h. Requirements for the use of wireless communications to transmit sensitive credit card information
i. Ensuring encryption techniques are approved and used to protect confidential or sensitive electronic data within the CDE

General Requirements and Procedures

- **Storage of Sensitive Authentication Data (SAD) and Cardholder Data (CHD)**

Storage of electronic and/or physical CHD or SAD poses significant risks and increases requirements that must be satisfied to be PCI-DSS compliant.

PCI-DSS prohibits the storage of SAD even if the data is encrypted. This includes any data on a card's magnetic stripe, verification or CVC/CVV and PIN. CHD is not to be stored, processed, or transmitted on HSU computers and/or mobile devices in any form.

- **Receipt of CHD via End-User Messaging Technologies**

Receipt or transmission of end-user messaging such as email, text messages, and instant messages containing CHD is prohibited. If end-user messages containing CHD are received, they are not to be printed or saved and no transactions should be processed. The recipient is to immediately delete the email from the inbox and trash folder and draft a new email advising that the HSU does not accept any payment details via the end-user messaging method and specify alternative options for payment.

Receipt or transmission of end-user messaging such as phone call containing the CHD must not be recorded and/or stored in any server/local machine. It also must not be written down on any paper or entered on a computer other than into the secured payment gateway.

- **Paper Forms**

CHD found on paper forms must be destroyed by close of business after the payment has been authorised. Documents containing CHD destined for destruction must always be stored securely. Appropriate methods to destroy CHD are cross-shredding and incineration. Shredders must be kept in a secure room with limited access.

In circumstances where CHD must be retained based on a justified business need, the documents containing the CHD must be stored in a secure location such as a safe, or a locked filing cabinet in a locked office.

Concealing CHD using a permanent marker does not meet the minimum requirements for destroying CHD.

- **Fax Machine**

If faxing is an option for receipt of CHD, a dedicated fax machine should be used for receipt of payment details. It must be set up in a method that ensures no incoming faxes are displayed or must be locked with a pin. Only staff members authorised for receipt of CHD should know the pin. The fax must not convert or forward the data received in/to an email.

- **Recording CHD**

Typing of the full Primary Account Number (PAN) in HSU documents or spreadsheets is strictly prohibited. PAN must not be recorded in any HSU cloud and/or local servers. If any CHDs are found on digital storage media, they must be securely overwritten or physically destroyed to prevent unauthorised disclosure.

- **Card Security Codes**

SAD includes the magnetic stripe, card validation code or value (CCV2, CVC), PIN data cannot be stored or recorded under any circumstances once a transaction has been processed.

- **Self-Assessment Questionnaire (SAQ)**

The HSU will complete an SAQ annually to demonstrate compliance with PCI-DSS. The SAQ is issued by the Payment Card Industry Security Standards Council. Upon completion, a compliance certificate will be issued and will be valid for one year.

- **Third-Party Vendor and Service Provider Compliance**

Third-party vendors and/or service providers that store, process, or transmit CHD on behalf of the HSU must also be PCI-DSS compliant as they have a direct impact on the security of this information. A process will be created and implemented for engaging third-party vendors and/or service providers, which will require confirmation of the party's PCI compliance status by consulting an appropriate database such as the VISA Global Registry.

As PCI standards evolve, the HSU will verify the PCI compliance status of third parties by requesting and reviewing a Certificate of Compliance annually.

- **Access to System Components containing CHD**

The HSU utilises a system that assigns a unique ID or username for each person accessing the HSU Servers and any files and/or media including sensitive data. Access is monitored such that each user only accesses data applicable to their role, minimising ease of access to sensitive data. All users who no longer work for the HSU have access revoked and removed immediately. The HSU ensures all users secure their accounts with strong passwords and requires them to be changed annually. The passwords must meet the PCI-DSS requirements:

1. Minimum password length of at least seven characters.
2. Contain both numeric and alphabetic characters

Generic usernames and shared passwords are strictly prohibited within the HSU.

- **Protection of HSU Networks and Systems**

The HSU will continue to implement methods required by PCI-DSS to ensure the network and systems used to process, store, or transmit CHD and member confidential information is protected. This involves ensuring anti-virus programs are the most current available, in addition to strict firewall configuration and constant updates relating to security patches.

- **Suspected/Real breach of data compromise incident**

All HSU employees who have handled debit/credit card transactions have a responsibility in detecting security breaches and assisting with incident response procedures within their operational areas.

Security issues that may arise include but are not limited to:

- Theft, damage, or unauthorised access (e.g., papers missing from desks, breach of access into membership portal, broken locks, etc.)
- Fraudulent misuse of sensitive or confidential information such as card payment details stored in databases, files, or CHD paper records etc.

Breaches

Disciplinary action will be taken against a person who breaches the HSU PCI-DSS Policy. Discipline may involve a warning, counselling or dismissal, depending on the circumstances.

Policy Version Control

Policy Approval Date:	1 July 2022
Approved by:	Union Council under Rule 40
Approval Resolution No:	UC 17/2022
Version No:	V1
Replaced Version No & Date:	NA