Imperial College London

Payment Security Management System (PSMS)

Payment Information Security Policy

May 2021 | Release 1.0

Contents

Purpose

The purpose of this document is to define the role that Imperial College London's ("Imperial") senior management takes in operating sustainable payment security. This ensures the commitment to payment information security, the development and propagation of the policy, and the assignment of appropriate roles, responsibilities and authorities.

This policy may be used to demonstrate and communicate the level of importance that the organisation places on the protection of cardholder data (CHD), associated with any credit or debit card transaction as part of Imperial's payment security practices.

1 Scope

The policy applies to all staff associated with the cardholder data environment (CDE), including contractors and anyone else who, even on a temporary basis, processes card payments or supports the payment card technical infrastructure.

2 Responsibilities

- The Payment Security Committee is responsible for setting and approving the payment information security policy.
- The Payment Security Committee will nominate an overall Payment Compliance Officer who is responsible for ensuring that roles, responsibilities and authorities are appropriately assigned, maintained and updated as necessary.
- Overall responsibility and accountability for the security of CHD associated with any credit or debit card transaction within Imperial, resides with the managers in areas interacting with CHD.
- All employees are responsible for adhering to the requirements of the payment information security policy and for fulfilling any duties related to assigned roles, responsibilities or authorities.

3 Payment Information Security Policy Statement

- It is Imperial's policy to maintain a level of payment security that at least meets the requirements of the Payment Card Industry Data Security Standard (PCI DSS) for Imperial's payment acceptance activities.

- Imperial aims to provide a level of payment security to the satisfaction of all customers, stakeholders and interested parties, meeting and exceeding expectations.
- Imperial ensures the details of this policy are known to all internal and external parties where appropriate, and determines the need for communication and by what methods. These include, but are not limited to, customers and suppliers and their requirements as documented in contracts and specifications and internal staff who are directly involved in accepting payments or supporting the technical and maintenance aspects of the CDE.
- Imperial employees, third-parties acting on Imperial's behalf and contractors shall not send credit or debit CHD via end-user messaging technologies such as e-mail, instant messaging or chat applications.
- All employees, third-parties and contractors shall not attach or use within Imperial's CDEs, network devices including but not limited to modems, remote-access technologies, wireless technologies, removable electronic media, personal laptops, tablets, smartphones or personal storage media (e.g. memory sticks).
- Users shall not store credit and debit CHD on local hard drives, or external or mobile media.
- Imperial complies with all legislation, regulations, codes of practice and all other requirements applicable to payment security activities.
- Imperial provides all resources inclusive of equipment, trained and competent staff and any other requirements to ensure that all payment security obligations and objectives are met.
- Imperial ensures that all employees are made aware of their individual obligations in respect of this payment information security policy.
- To ensure Imperial maintains its awareness for continuous improvement, payment security within the organisation is regularly reviewed by the Payment Security Committee to ensure it remains relevant and appropriate for the payment activities taking place.
- Imperial's payment security activities will be subject to both internal and/or external audits as appropriate.
- Imperial accepts its responsibility for security as a custodian of CHD associated with any credit or debit card transaction, and will continue to adhere to all applicable payment security controls.

4 Document Management

This policy is the property of Imperial. It is a controlled document which is version

numbered reviewed, maintained and revised as required and updated at least annually. Previous versions of this policy will be retained in archive by Imperial for at least one year. Where this policy is printed and distributed within Imperial, a list is maintained of all recipients to control amendments and recall of subsequent versions.

4.1 Document Owner and Approval

The Payment Compliance Officer is the owner of this document and is responsible for ensuring that it is reviewed in line with Imperial's review requirements.

A current version of this document is available to all relevant members of staff and is published on Imperial's website.

4.2 Change History Record

Issue	Description of Change	Approved by	Date of Issue
1.0	PSMSPaySecPolicy Introduction	Payment Security Committee	12/05/2021