University of San Francisco
Acceptable Use Policy (AUP) & Agreement for POS Devices and PCI Network

1. Purpose

University of San Francisco (USF) provides access to the PCI network for processing CASHNet related credit card payment. This Acceptable Use Policy provides guidance for using related IT Resources and protects the University, users, and PCI network. This is a requirement that aligns with Payment Card Industry Data Security Standard (PCI-DSS).

2. Roles and Responsibilities

Access to Payment Card Industry (PCI) computer systems and networks owned or operated by University of San Francisco imposes certain responsibilities and obligations and is granted subject to University policies, local, state, and federal laws.

Role	Team	Responsibility
PCI Manager	ABS	• Review and approve new user requests, maintain approval documentation • Submit disable request when cashier access is no longer needed (see KB10158, KB11181) • Participate in regular PCI user reviews • Assist in risk assessment for USF PCI environment • Conduct periodic inventory of PCI POS devices • Manage and administer physical inspection of PCI POS devices • Provide security training to new PCI Cashiers and re-train existing users as per PCI-DSS regulations • Review and maintain Information about PCI DSS requirements that are managed by service providers • Submit Self-Assessment Questionnaire (SAQ) and on-site assessment results
NeuLion Manager	Athletics	• Create/remove NeuLion user • Submit requests to PCI Manager for addition/removal of user access on USF PCI Network

IT Security	Information and Security Compliance (ISC)	• Review security logs for PCI Domain Controller, network device • Review IT security configuration for PCI IT environment • Gather and/or provide info related to IT and Information Security for Self-Assessment Questionnaire (SAQ) and on-site assessment • Assist with PCI certification and risk assessment
Server and Cashier Laptop custodian	Client Support Services	• Provide/remove user access to USF PCI network • Provide USF PCI Point of Sale devices as requested by ABS • Maintain list of servers/laptop/iPad devices • Manage/deploy Server and Cashier laptop/iPad environment • Manage and monitor Sophos Anti-Virus for PCI Server and laptops • Apply patches to fix vulnerabilities for Servers and Cashier laptops / iPads
IT Infrastructure custodian	Infrastructure Team (Network and Server)	• Manage ESXi Server and PCI related network devices (switches, routers, firewalls and load balancers) • Apply patches to fix vulnerabilities for ESXi Server and PCI related network devices
Cashier	Cashiers approved by ABS	• Perform hardware inspections according to USF PCI POS Hardware Inspection Guidelines • Report and submit results according to above mentioned guidelines • Process credit card payments according to this Policy
Supervisor of Cashier	Request access from ABS	• Submit new cashier requests to PCI Manager • Inform PCI Manager when user no longer needs CASHNet cashier access • Ensure that Cashier performs hardware inspections according to USF PCI POS Hardware Inspection Guidelines

3. Roles & Privileges

Acceptable use is established and maintained by cautiously exhibiting ethical choices that reflects academic honesty.

USF utilizes the security industry standard practice of 'least privileged' to restrict rights to only those individuals requiring access. That said, privileges are assigned to users based on required job functions. The PCI Manager (ABS) is responsible for reviewing and granting access to appropriate personnel.

Role	Team	Privilege
CASHNet Admin	ABS	• Full access to CASHNet application • View full details for all CASHNet transactions
NeuLion Admin	Athletics	• Full access to NeuLion application • View full transaction details of payments made via NeuLion-CASHNet integration
IT Security	Information and Security Compliance (ISC)	• Full Access to log data on server and OS environment
IT Infrastructure Custodian	Infrastructure Team (Network and Server)	• Privileged user access to ESXi server and network device for daily operation and maintenance
Server and Cashier Laptop Custodian	Client Support Services	• Privileged user access to server and OS environment for daily operation and maintenance
Cashier	Cashier approved by ABS	• Normal user access to PCI laptop and CASHNet or NeuLion applications to process credit card payments

4. Do's and Don'ts

Departments approved to access CASHNet must ensure that their employees using the system comply with the acceptable use standards set forth in this Policy. These standards include, but are not limited to, the following examples of acceptable and unacceptable uses:

Acceptable use means that you MUST:

- Use CASHNet and POS devices only for authorized purposes.
- Protect user identification and system from unauthorized use.
- Access information only authorized for the user to access.
- Restrict access to cardholder data to individuals with a business need-to-know.

- Redact credit card numbers on all documents after the transaction has been processed.
- Retain redacted cardholder data only if it is absolutely necessary, e.g., to reconcile payments.
- Shred all documents containing credit card information when it is no longer needed for business or legal reasons.
- Process credit card transactions only on University-provided point-of-sale (POS) devices.
- Use strong passwords and update them when prompted.
- Maintain and update security software on all POS devices.
- Always lock computers, electronic devices, files, and storage areas when unattended.
- Periodically inspect POS devices for signs of damage or tampering.
- Report suspicious activities or suspected security breaches immediately.
- Immediately report lost or stolen POS devices to ITS.
- Protect computer networks with firewalls and intrusion detection systems.
- Continuously monitor the network for intrusion and anomalies.

Unacceptable use means that you MUST NOT:

- Use another person's system access, user identification, password, files, or data.
- Leave POS devices unattended in public areas.
- Transmit cardholder data via email or on the Internet.
- Store credit card data electronically unless it is encrypted and secured by firewalls.
- Use software or other technology to access CASHNet control information.
- Attempt to circumvent or subvert system or network security measures.
- Engage in any activity that might be harmful to University systems or data, such as creating or propagating viruses, disrupting services, damaging files, or making unauthorized modifications to data.
- Make or use illegal copies of cardholder information or transmit such copies over University networks.
- Use public wireless networks for processing credit card transactions.
- Use University computing or network resources for nonbusiness purposes or personal gain.
- Engage in any other activity that does not comply with this Policy and the **Technology Resources Appropriate Use Policy.**

5. Point of Sale Device Protection

Device Listing

USF ITS maintains a complete list of the point of sale (POS) devices at all merchant locations, and includes the manufacturer, model number, serial number and the location of the devices. The Desktop Engineering Team updates the list when devices are added, relocated, decommissioned, etc.

The device list is updated at least semi-annually, where upon Information and Security Compliance (ISC) will notify ABS to conduct an inventory verification. ABS will document findings and provide them to ISC.

Periodic Inspection of POS Devices

Cashiers must inspect POS devices for tampering and substitution periodically according to the procedures specified in the inspection guide. *(See: USF Physical Inspection Guide for PCI POS Devices SOP.pdf).* This process is aimed at ensuring that an unauthorized card skimmer has not been added to the card swipe device, and that the manufacturer, model number, serial number, asset tag number, and location of the device is accurate.

Standard Operating Procedure (SOP) requires the Cashier to perform weekly physical inspections and report the completion via shared Google sheet.

Personnel

Cashiers must also verify that any maintenance or repair attempts are done only by identifiable ITS personnel. If the identity of ITS member cannot be verified Cashier should not allow that individual to access the machine and should contact ITS Help Desk to verify. The same process applies for any third-parties claiming to repair, troubleshoot, or provide maintenance to the machine. USF does not install, replace, or return devices without prior authorization from ABS and/or ITS Desktop Engineering Team.

Any suspicious individuals or behaviors must be reported to ABS, ITS ISC and Public Safety immediately in accordance with System Life Cycle Management (SLCM) Security Change and Incident Response Procedures.

Session Timeout

If a session has been idle for more than 15 minutes, the user will need to re-authenticate and re-activate the terminal and/or session.

6. Training

Approved cashiers must attend annual PCI training which covers credit card data security, PCI POS device inspection, as well as all the topics mentioned in this Policy

Acceptable Use Agreement

I have read the above requirements regarding use of the University's payment card-processing system. I understand my responsibilities regarding these systems and information contained therein.

The University considers any violation of acceptable use principles to be a serious offense and reserves the right to copy and examine any files or information residing on University systems allegedly related to unacceptable use, and to protect its network from systems and events that threaten or degrade operations. Violators are subject to disciplinary actions

Individuals using computer systems owned by the University of San Francisco are subject to applicable laws and University policies. Offenders also may be prosecuted under laws including (but not limited to) the Communications Act of 1934 (amended), the Family Educational Rights and Privacy Act of 1974, the Computer Fraud and Abuse Act of 1986, The Computer Virus Eradication Act of 1989.

Employee Signature	Print Name	Date