University of San Francisco

Acceptable Use Policy (AUP) & Agreement for Point of Sale (POS) Devices

1. Purpose

This Acceptable Use Policy provides guidance on using related IT Resources and protects the University, its users, and the PCI network. This requirement aligns with the Payment Card Industry Data Security Standards (PCI-DSS).

2. Roles and Responsibilities

Access to payment processing equipment, applications, and networks owned, supported, or operated by the 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 ▪ Disable the user when the cashier access is no longer needed ▪ Maintain inventory of PCI POS devices ▪ Manage physical inspection of POS PCI devices ▪ Provide security training to new PCI Cashiers and re-train existing users as per PCI-DSS regulations ▪ Participate in regular PCI user reviews ▪ Assist in risk assessment for USF PCI environment ▪ Submit Self-Assessment Questionnaire (SAQ) and on-site assessment results as needed
Paciolan Manager	Athletics	▪ Create or remove Paciolan user access ▪ Maintain inventory of POS devices used for Paciolan ▪ Conduct a physical inspection of POS devices ▪ Participate in regular PCI user reviews ▪ Assist in risk assessment for the USF PCI environment

Role	Team	Responsibility
Cvent & Cybersource Administrators	Development	▪ Review and grant access to new users ▪ Disable the user when cashier access is no longer needed ▪ Maintain inventory of PCI POS devices ▪ Manage physical inspection of POS PCI devices ▪ Participate in regular PCI user reviews ▪ Assist in risk assessment for the USF PCI environment
IT Security	Information Security & Compliance (ISC)	▪ Review IT security configuration for the 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 ▪ Ensure that cardholder data is not stored electronically
POS iPad Administrator	Desktop Engineering (DE)	▪ Maintain/update the required software on PCI POS devices to enable secure processing ▪ Manage/deploy the PCI iPad environment ▪ Apply patches for PCI iPads
Cashier	ABS, Athletics, Development	▪ Process credit card payments according to this Policy ▪ Perform inspections according to the Physical Inspection Guide for POS Devices ▪ Report and submit results according to above mentioned guidelines
Cashier Supervisor	ABS, Athletics, Development	▪ Submit new cashier requests to the appropriate admin for the application ▪ Inform the PCI Manager when the user no longer needs access in Transact/CASHNet ▪ Inform Cvent Admin when the user no longer needs access in Cvent ▪ Inform the Paciolan Manager when the user no longer needs access in Paciolan ▪ Ensure that the Cashier performs POS device inspections ▪ Ensure that cardholder data is not stored physically or electronically ▪ Participate in regular PCI user reviews

3. Roles & Privileges

Acceptable use is established and maintained by cautiously exhibiting ethical choices that reflect 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.

Role	Team	Privilege
Transact Administrator	ABS	▪ Full access to Transact application ▪ View full details for all Transact transactions ▪ Maintain user access
Paciolan Administrator	Athletics	▪ Full access to Paciolan application ▪ View full details for all Paciolan transactions ▪ Maintain user access
Cvent, Cybersource, & GiveCampus Administrator	Development	▪ Full access to Cvent, Cybersource, and/or GiveCampus applications ▪ View full details for all transactions in Cvent, Cybersource, and/or GiveCampus ▪ Maintain user access
IT Security	Information Security & Compliance (ISC)	▪ Full access to log data from the mobile device management (MDM) solution
POS iPad Administrator	Desktop Engineering (DE)	▪ Full access to MDM solution and PCI POS configuration profiles
Cashier	Transact Paciolan Cvent Cybersource	▪ Cashier access to Transact, Paciolan, Cvent, and/or Cybersource applications to process credit card payments

4. Do’s and Don’ts

Departments that are approved to access payment applications 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 POS devices only for authorized purposes.
- Protect user identification and the 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.
- Inspect POS devices for signs of damage or tampering in accordance with the Physical Inspection Guide.
- Report suspicious activities or suspected security breaches immediately.
- Immediately report lost or stolen POS devices to ITS.

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.
- Collect credit card data over USF telephone (VoIP) systems.
- Process credit card transactions over any USF network (wired or wireless) unless using a PCI-validated Point-to-Point Encryption (P2PE) solution.
- Store credit card data in hard copies or electronically unless it is encrypted and secured by firewalls.

- Use software or other technology to access payment applications.
- 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 non-business 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 for 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, whereupon ISC will notify ABS to conduct an inventory verification. ABS will document findings and provide them to ISC.

Inspection of POS Devices

Cashiers must inspect POS devices for tampering and substitution prior to use before each event according to the procedures specified in the inspection guide below. Department must also maintain an inspection log that includes inspection date, device tag number, name of inspector and device condition. *(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.

Personnel

Cashiers must also verify that any maintenance or repair attempts are done only by authorized 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 session.

6. Training

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

Acceptable Use Agreement

I have read the above requirements regarding the 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