Self-Assessment Questionnaire B (SAQ B)

For UCSD departments that use standalone dial out terminals only.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

		Yes	No
3.2	(c) Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?	☒	☐
	(d) Do all systems adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted)?		
	3.2.1 The full contents of any track from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere)are not stored under any circumstance? This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. *In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* *♣The cardholder's name,* *♣Primary account number (PAN),* *♣Expiration date, and* *♣Service code* *To minimize risk, store only these data elements as needed for business*	☒	☐
	3.2.2 The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored after authorization?	☒	☐
	3.2.3 The personal identification number (PIN) or the encrypted PIN block is not stored after authorization?	☒	☐
3.3	Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed)? *Note:* *♣This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.*	☒	☐

Requirement 4: Encrypt transmission of cardholder data across open, public networks

		Yes	No
4.2	(b) Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies?	☒	☐

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

		Yes	No
7.1	Is access to system components and cardholder data limited to only those individuals whose jobs require such access as follows:		
	7.1.2 Is access to privileged user IDs restricted as follows: • To least privileges necessary to perform job responsibilities? • Assigned only to roles that specifically require that privileged access?	☒	☐
	7.1.3 Are access assigned based on individual personnel's job classification and function?	☒	☐

Requirement 9: Restrict physical access to cardholder data

		Yes	No
9.5	Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? *For purposes of Requirement 9,"media" refers to all paper and electronic media containing cardholder data.*	☒	☐
9.6	(a) Is strict control maintained over the internal or external distribution of any kind of media?	☒	☐
	(b) Do controls include the following:		
	9.6.1 Is media classified so the sensitivity of the data can be determined?	☒	☐
	9.6.2 Is media sent by secured courier or other delivery method that can be accurately tracked?	☒	☐
	9.6.3 Is management approval obtained prior to moving the media (especially when media is distributed to individuals)?	☒	☐
9.7	Is strict control maintained over the storage and accessibility of media?	☒	☐
9.8	(a) Is all media destroyed when it is no longer needed for business or legal reasons?	☒	☐
	(c) Is destruction performed as follows:		
	9.8.1 (a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?	☒	☐
	(b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?	☒	☐
9.9	Are devices that capture payment card data via direct physical interaction with the card protected against tampering and substitution as follows? ***Note:*** *This requirement applies to card-reading devices used in card-present transactions (that is, card swipe or dip at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.*		
	(a) Do policies and procedures require that a list of such devices be maintained?	☒	☐
	(b) Do policies and procedures require that devices are periodically inspected to look for tampering or substitution?	☒	☐

	(c) Do policies and procedures require that personnel are trained to be aware of suspicious behavior and to report tampering or substitution of devices?	☒	☐
9.9.1	(a) Does the list of devices include the following? • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification	☒	☐
	(b) Is the list accurate and up to date?	☒	☐
	(d) Is the list of devices updated when devices are added, relocated, decommissioned, etc?	☒	☐
9.9.2	(a) Are device surfaces periodically inspected to detect 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) as follows? ***Note:*** *Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.*	☒	☐
	(b) Are personnel aware of procedures for inspecting devices?	☒	☐
9.9.3	Are personnel trained to be aware of attempted tampering or replacement of devices, to include the following?		
	(a) Do training materials for personnel at point-of-sale locations include the following? • 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 appropriate personnel (for example, to a manager or security officer).	☒	☐
	(b) Have personnel at point-of-sale locations received training, and are they aware of procedures to detect and report attempted tampering or replacement devices?	☒	☐

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

		Yes	No
12.1	Is a security policy established, published, maintained, and disseminated to all relevant personnel?	☒	☐
	12.1.1 Is the security policy reviewed at least annually and updated when the environment changes?	☒	☐
12.3	Are usage policies for critical technologies developed to define proper use of these technologies for all personnel, and require the following:		

	Note: *Examples of critical technologies include, but are not limited to, remote-access and wireless technologies, removable electronic media, laptops, tablets, e-mail, and Internet usage.*		
	12.3.1 Explicit approval by authorized parties to use the technologies?	☒	☐
	12.3.3 A list of all such devices and personnel with access?	☒	☐
	12.3.5 Acceptable uses of the technologies?	☒	☐
12.4	Do the security policy and procedures clearly define information security responsibilities for all personnel?	☒	☐
12.5	(a) Are the following information security management responsibilities formally assigned to an individual or team:		
	12.5.3 Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?	☒	☐
12.6	(a) Is a formal security awareness program in place to make all personnel aware of the importance of cardholder data security?	☒	☐
12.8	Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:		
	12.8.1 Is a list of service providers maintained?	☒	☐
	12.8.2 Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment? ***Note:*** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*	☒	☐
	12.8.3 Is there an established process for engaging service providers, including proper due diligence prior to engagement?	☒	☐
	12.8.4 Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?	☒	☐
	12.8.5 Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?	☒	☐
	12.10.1 (a) Has an incident response plan been created to be implemented in the event of system breach?	☒	☐