PCI Compliance Guide

As company that deals with cardholder data, it's particularly important for you to maintain strong security standards. CenterEdge Software is here to help.

Working with our payment partners, we are offering a free PCI Compliance program to help you keep cardholder data secure.

This service is free and upon completion of a brief questionnaire provided via SecurityMetrics, it includes $100,000 in breach assistance.

To help you complete the 26-question survey, we've prepared this PCI Compliance Guide. Following are the questions you'll see, the needed response, and guidance to help you with the process.

Policy Section

Q#	PCI Question	PCI Question	Response Needed	CenterEdge Explanation
1	12.1	Do you have a written policy which is kept up to date and disseminated to all relevant employees?	**Yes**	If you do not yet have a security policy, you can use the template here as a starting point. Instructions are also provided.
2	12.1.1	Your policy should be reviewed at least once a year or whenever changes in business environment require, such as hiring new employees, changes in your business or risk environment or using new technologies. Is your policy reviewed appropriately?	**Yes**	CenterEdge will review and update the provided template yearly.
3	12.4	Does your policy explain each employee's role in cardholder security?	**Yes**	See page 12 of the recommended policy template referenced above to verify or update roles.
4	12.5.3-12.6.a	A security awareness program should be in place to inform employees regarding cardholder data security. Included in this program should be a documented procedure for an effective handling of an escalated situation. Do you have this in place?	**Yes**	See page 12 of the recommended policy template referenced above to verify or update roles.

Service Providers

Q#	PCI Question	PCI Question	Response Needed	CenterEdge Explanation
5	12.8.1	Is a list of service providers maintained, including a description of the service(s) provided?	**Yes**	Note that this is specifically related to partners that you share cardholder data with or that could affect the security of your cardholder data, such as an accountant, managed IT provider, shredding company, attorney or other business partners. If that is not applicable for you, just select 'yes'. If it is applicable, make sure you keep an updated list of such partners. (CenterEdge is one such partner.)
6	12.8.2	You should have a written agreement with your providers that acknowledges their responsibility for the cardholder data they possess. Do you have such an agreement?	**Yes**	CenterEdge acknowledges its responsibility for cardholder data. If you have other service providers that work with cardholder data, be sure they acknowledge their responsibility for managing such data.
7	12.8.3	Do you have an established process for selecting a service provider, including proper due diligence?	**Yes**	Again, this applies just to service providers who work with cardholder data.
8	12.8.4	Do you verify that all your providers are PCI compliant themselves at least once a year? Do you personally verify their compliance annually?	**Yes**	Again, this applies just to service providers who work with cardholder data. CenterEdge will verify its compliance annually.
10	12.8.5	If you have multiple third party providers, you should maintain records showing what data is shared with which provider. Do you maintain this data?	**Yes**	CenterEdge may be your only such partner. If you have more, you should track what data is shared with each.
11	12.10.1.a	Do you have an incident response plan in the event that cardholder data has been compromised?	**Yes**	This Data Breach Response: A Guide for Business - authored by the US Federal Trade Commission, may be a helpful incident response plan for your company.

Physical Access

Q#	PCI Question	PCI Question	Response Needed	CenterEdge Explanation
12	9.5	Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)?	**Yes or N/A**	“For purposes of this section (connected to PCI Requirement 9), “”media”” refers to all paper and electronic media containing cardholder data. You can select N/A if you don’t store cardholder data.”
13	9.8.a-9.8.1.a	All media should be destroyed when it is no longer needed for business or legal reasons. Acceptable methods to destroy paper media include cross-cut shredding, burning and/or pulping. Do you properly dispose of media to make sure that the data cannot be reconstructed?	**Yes or N/A**	Same. You can select N/A if you don’t store cardholder data.
14	9.8.1.b	Is your media stored appropriately?	**Yes or N/A**	Containers that hold media waiting to be destroyed should be secured and labeled. For example, a label of “To be shredded” on a locked container would satisfy this requirement.
15	9.9.1.a-9.9.1.c	Your list of devices should detail the make and model, where the devices are kept, and unique IDs (like serial numbers.) This list should be updated whenever a device is added, moved or retired. Is your policy and device list up to date?	**Yes or N/A**	This is related to any devices that are used in the management of cardholder data.
16	9.9.2.a-9.9.2.b	Devices need to be regularly inspected for tampering. Common methods of tampering are adding card skimmer hardware to a swipe machine or to replace devices with a new device. Checking the serial number of the device against your recorded numbers will detect fraudulent devices. Do you have documentation indicating when inspections have occurred?	**Yes or N/A**	This is related to any devices that are used in the management of cardholder data.

Physical Access - Cont'd

Q#	PCI Question	PCI Question	Response Needed	CenterEdge Explanation
17	9.9.3.a-9.9.3.b	Personnel must be trained regarding tampered devices. Training should cover: • Verifying anyone claiming to be a service or repair person before allowing them access to processing or swiping devices • Not installing or replacing devices without verification • Being wary of suspicious behavior such as unknown persons unplugging or opening devices • Reporting suspicious behavior or device tampering to the correct personnel • Have your employees been trained to detect suspicious activity and device tampering?	**Yes or N/A**	This is related to any devices that are used in the managament of cardholder data.
18	9.9-9.9.c	Devices used to swipe or dip payment cards need to be protected against tampering. You should maintain a list of all your devices used to swipe cards, manually inspect them for tampering periodically and train your personnel to inspect them. You should also work with employees to report suspicious behavior or unexpected device replacement. Do your policies address this?	**Yes or N/A**	This is tied to the devices listed in #15 above.
19	9.10	Are security policies and operational procedures for restricting physical access to cardholder data: • Documented • In use • Known to affected parties	**Yes**	

Stored Data

Q#	PCI Question	PCI Question	Response Needed	CenterEdge Explanation
20	3.1.a	Is data storage amount and retention time limited to that required for legal, regulatory, and business requirements?	Yes	
21	3.1.b	Are there defined processes in place for securely deleting cardholder data when no longer needed for legal, regulatory, or business reasons?	Yes	
22	3.1.c	Do you have specific requirements for the retention of data?	Yes	For example, cardholder data needs to be held for X period for Y business reasons.
23	3.1.d	Is there a quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements?	Yes	
24	3.1.e	Does all stored cardholder data meet the requirements defined in the data-retention policy?	Yes	Data retention is included in the sample policy, (Section 3) linked at the top of this document.
25	3.2.2	The card verification code (the three or four digit number from the back of the card) cannot be stored. Do you agree that you do not and will not store this information?	Yes	This data is not stored in your relationship with CenterEdge
26	3.7	Are security policies and operational procedures for protecting stored cardholder data documented, in use and known to all parties?	Yes	Data retention is included in the sample policy, (Section 3) linked at the top of this document.

How Do You Accept Cards

Q#	PCI Question	PCI Question	Response Needed	CenterEdge Explanation
27		Please enter the details of your card processing methods. At least one third party provider must be filled out to proceed.	**(Complete the open field.)**	Enter Element triPOS, Datacap NETePay, or authorize.net, depending on which is your online payment processing method via CenterEdge. Reach out to Support if you need help determining this. You may also have a POS pin pad device through CenterEdge. If you conduct payment processing outside of CenterEdge, be sure to enter that info as well.”