IntelliPay®

PCI DSS Incident Response and Information Security Plan Guidelines

September 2024

PCI DSS Incident Response and Informaiton Security Plans

To meet the Payment Card Industry Data Security Standard (PCI DSS) requirements, which apply to any organization that stores, processes, or transmits cardholder data. This includes merchants, payment processors, issuers, acquirers, and service providers. Your organization must create and maintain an information security policy and incident response plan:

An incident response plan, puts all the information your organization will need in one place enabling you to act quickly in the event of a cardholder data breach. Please note that this document doesn't include the regulations you must follow when non-cardholder data is lost.

What is an incident response plan?

It's a critical checklist of processes and procedures your business must have so that you can act swiftly and effectively in the event of a data breach. Whether you have confirmed or suspected a threat to your customers' cardholder details, this plan is essential.

Your incident response plan should be shared with everyone in your business so they understand their role in the event of an incident.

An incident response plan includes, but is not limited to:

- Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum
- Incident response procedures with specific containment and mitigation activities for different types of incidents
- Business recovery and continuity procedures
- Data backup processes
- Analysis of legal requirements for reporting compromises
- Coverage and responses of all critical system components
- Reference or inclusion of incident response procedures from the payment brands

Information Security Plan

This information security plan should include procedures for responding to information security incidents, as well as guidelines for the proper use of systems and networks. The plan should also address the acceptable use of software and hardware. The plan provides for monitoring and responding to alerts from security monitoring systems, including but not limited to:

- Intrusion-detection and intrusion-prevention systems
- Network security control
- Change-detection mechanisms for critical files
- The change- and tamper-detection mechanism for payment pages
- Detection of unauthorized wireless access points.

Testing
The plans should be tested at least annually to ensure it works as intended.

Seven Processes to include

These processes cover each stage of an incident – from the moment an incident is discovered to when resumption of normal operations.

1) Alert - The moment you discover an incident taking place that could threaten the security of cardholder data.

2) Activate - Put your incident response plan into action.

3) Engage - Speak with staff, your acquirer and third-party contacts, such as hosting providers, web developers and any businesses that may be affected or involved in the incident.

4) Investigate - Look into the incident to find out where and how it occurred. Do this with support from industry accredited forensic companies.

5) Containment -Take actions to make sure the incident doesn't get worse. Do this with support from industry accredited forensic companies.

6) Remediation - Find the place affected by the incident and secure it. Do this with support from industry accredited forensic companies. Address system or plan weakness and correct.

7) Normal operations - Return to normal operations and learn lessons from the incident. Make sure the security of cardholder data is documented by reporting your PCI DSS status. You may need to complete this within 180 days.

Who should respond to a suspected or confirmed security incident?

Company designated leader or spokesperson following consultation with your lawyer and other experts which could include a crisis management public relations firm.

- Make sure your designated individual(s) are ready to respond. They'll need to be available on a 24/7 basis
- Make sure they're properly and regularly trained so they know what they need to do and what they can say.
- Conduct a drill to assess their knowledge of the plan (at least every year) and preparedness.

Recording your key contacts and PCI DSS status

Keep records of the contact details for everyone in your business' incident response team, your acquirer/card processor contact, and any third parties. You should also keep track of your PCI DSS status.

A business keeps track of their PCI DSS status by completing a Self-Assessment Questionnaire (SAQ) or undergoing a formal audit by a Qualified Security Assessor (QSA), which results in an "Attestation of Compliance" (AOC) document, essentially proving their compliance with PCI DSS requirements and allowing them to monitor their ongoing status; this document is typically submitted to their payment processor or acquiring bank to demonstrate compliance.

Managing your incident response team

Ideally, you should have a primary contact who owns the plan and takes charge of any actions that need to be taken. You should also list other staff who will be responsible.

Name	Role/Responsibilty	Contact Number	Email

List you acquirer/card processor contact

This is the business that provides the merchant account(s) which enable your business to accept card payments.

Name	Role/Responsibilty	Contact Number	Email

Include third party contacts

This means those who offer support or services, including (but not limited to) ecommerce payment gateways, hosting, web developers, call center services, etc.

Name	Role/Responsibilty	Contact Number	Email

Include the key details that show your business is meeting the PCI DSS requirements.

Meeting the standard? (Y/N)	Attestation type (e.g. SAQ A)	Date when you last reported meeting the PCI DSS	Date when you next need to report meeting the PCI DSS	Date of quarterly ASV scans being performed (if needed)

Your incident checklist

These are the main points your plan should cover and the actions your incident team should take:

- Make sure staff know how to report any potential incident
- If an incident happens, contact all staff with incident response duties immediately
- Make sure all staff with incident response duties know the actions they need to take
- Keep a record of all actions that are taken
- Update everyone in your business on the actions that have been taken and the outcome
- Report the incident to your acquirer immediately. They will tell you what steps you need to take
- Talk to any external companies that your acquirer says can help look into the incident
- Make sure you can quickly pay invoices for any external companies that you get involved
- Your business and any third party providers must give support to any external companies involved
- Reduce the risk of tampering with potential evidence by limiting access to the equipment or environment affected by the incident
- Remove the equipment, system or environment affected by the incident off from your network. Do this without turning the device, system or environment off. This will limit the impact on your customers' card data
- Keep copies of any malware or code that could be a threat to help the investigation
- Check that all system and security logs are secured. (Audit logs should be kept for 12 months as per PCI DSS requirement 10.5.)
- If equipment or media (such as USB, laptop) has been lost or stolen, find out what card details data has been affected
- Log the details of all lost or stolen equipment such as make or model, location of loss or theft
- Keep copies of CCTV footage, if appropriate
- Get in contact with third party providers
- Review how the incident was handled to help cut down the risk of it being repeated in future. Pinpoint any areas that could be improved.

What your acquirer/card processer expects when an incident happens

- To be contacted as soon as an incident that could place cardholder data at risk is found
- For you to arrange support from an external accredited forensic investigation company who will confirm that any risks to cardholder data are being handled and controlled
- Support of any third-party providers who may be included in the acceptance or processing of cardholder data.

Testing your plan

At least once every 12 months, your plans should be:

- Reviewed and updated as needed
- Tested, including all elements listed in Requirement 12.10.1 of the PCI DSS standard.