Building a PCI DSS incident response plan

To meet the requirements of the Payment Card Industry Data Security Standard (PCI DSS), you must have an incident response plan. This guide tells you how to build a plan and outlines the actions you need to take if the security of your cardholder data is ever threatened.

By making a plan, you'll have all this information in one place and be able to act quickly.

Please note – this document doesn't include the regulations you need to follow when non-cardholder data is lost.

What is an incident response plan?

It's a checklist of processes and procedures your business needs to have, so you can act quickly and effectively if a data breach happens. You can use it if you know or even suspect your customers' cardholder details have been threatened.

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

Part of Requirement 12 asks that you show;

An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The 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

The security incident response plan includes 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 unauthorised wireless access points.

More important information over the page

Seven processes to include in your plan

These processes cover each stage of an incident – from the moment it's picked up to when it's safe to restart trading.

1) Alert
Spot that there's an incident taking place that could threaten the security of cardholder data.

2) Activate
Put your PCI DSS 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.

7) Normal trading
Return to normal trading 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?

- Make sure your business has staff who 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
- Test their knowledge of the plan (at least every year)

Recording your key contacts and PCI DSS status

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

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/Responsibly	Contact number	Email

List your acquirer/card processer contact
This is the business that provides the merchant account(s) which enable your business to accept card payments.

Name (if known)	Company	Contact number	Email (if known)
Contact Centre	Barclaycard Payments	0800 161 5343	N/A

Include Third party contacts
This means those who offer support or services, including (but not limited to) ecommerce payment gateways, hosting, web developers, call centre services and point of sale.

More important information over the page

Name	Company	Role	Contact	Email

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

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
- Cut 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.

More important information over the page

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 security incident response plan should be:

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

Request this information in large print, Braille or audio.
Just call 0800 1615 350 (Barclaycard Payments) or 1800 812 700 (Barclaycard International Payments).