University of Warwick Incident Response Plan

1. Scope

The University is required to implement an Incident Response Plan which should be followed in the event of a system breach. This is a mandatory part of the PCI DSS Standard (requirement 12.10).

An "incident" is defined as a suspected or confirmed "data compromise". A "data compromise" is any situation where there has been unauthorised access to a system or network where cardholder data is collected, processed, stored, or transmitted. For the purposes of PCI DSS, a data compromise can also involve the suspected or confirmed loss or theft of any material or records that contain cardholder data.

Some examples of data compromise incidents in relation to card holder data that an employee might recognise in their day to day activities include, but are not limited to:

- Theft, damage, or unauthorised access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorised physical entry)
- Fraud
- Inaccurate information within databases, logs, files or paper records
- Card terminals that have been tampered with or substituted
- Computers that have had a suspect device installed to the USB port

Staff in the context of this document refers to all individuals employed by the University of Warwick or paid by the University of Warwick to perform duties that require the individual to process card payments.

The Incident Response Plan is reviewed at least annually and updated if required.

2. Identifying Security Breaches

Security breaches come in many different forms and, while detecting them may be challenging, there are certain signs that tend to appear when a security breach has occurred.

- Unexpected outgoing internet network traffic from the payment card environment.
- Presence of unexpected IP addresses on the network.
- Unknown or unexpected services and applications configured to launch automatically on system boot.
- Unknown files, software and devices installed on systems.
- Anti-virus programmes malfunctioning or becoming disabled for unknown reasons.
- Failed login attempts in system authentication and event logs.

- Vendor or third party connections made to the cardholder environment without prior consent and/or a trouble ticket.
- SQL Injection attempts in web server event logs.
- Authentication event log modifications.
- Suspicious after-hours file system activity.
- Presence of .zip, .rar, .tar, and other types of unidentified compressed files containing cardholder data.
- System rebooting or shutting down for unknown reasons.
- Malicious code hidden in windows registry.

It is most likely that any breach would be detected by the University's acquirer, currently Global Payments, and/or a card brand, and reported to the University directly from the acquirer. The primary contacts for reports in this manner are the Deputy Finance Director and the Financial Controller.

3. Reporting an Incident

Staff are responsible for reporting any incidents identified in their area immediately to their Line Manager and the PCI DSS Incident Response Team. If you become aware of a suspected or real security incident relating to cardholder data, or a failure in procedure, then you must act immediately, identifying your concerns with your line Manager who will log with IT support, via the helpdesk. The Helpdesk will notify the PCI DSS Incident Response Team. See section 4 for response team members.

If the compromise is in relation to a terminal, device or PC, in addition to notifying the incident response team, the following steps must be immediately followed:

- Disconnect the terminal/device/PC's network cable / telephone line (but DO NOT switch the device off);
- Put a note on the terminal/device/PC stating that it is 'not in use';
- Do not access or alter the suspected or confirmed compromised device or system;
- Keep a watchful eye over the device or system until further information is given;
- Document all steps taken. Include the date, time, location(s), person(s) involved and action taken for each step. See appendix 1 Incident Response Form.

For PCI DSS queries in relation to different payment card processes please use the following table:

Type of Payment Process	**Primary Contact**	**Secondary Contact**	**Out of hours contact**
Tills / Interfaced PDQ	Atia Chaudry		IT Helpdesk
PDQ	Atia Chaudry		IT Helpdesk
PC / Laptop	Neal Welland	Bendra Ojameruaye	IT Helpdesk
Website	Des Butcher	Paul Strapps	IT Helpdesk
Other	Catherine Wallis		IT Helpdesk

If the incident is in relation to the loss of hard copy data it is still important to document all steps taken and all persons involved or suspected to be involved again using appendix 1 Incident Response Form.

4. Incident Response Team

The initial Incident Response Team will include the following University team members.

Neal Welland – IT Security Specialist, Information Technology Services
Bendra Ojameruaye – IT Security Analyst, Information Technology Services
Debbie Jay – Deputy Finance Director
Catherine Wallis – Financial Controller
Atia Chaudry – IT Systems Manager/Business Analyst Commercial Directorate
Graham Yarrow – Application Management Specialist, IT Services

The above team will nominate an Incident Lead, who will co-ordinate actions and ensure other key members of the University are kept updated as the investigation unfolds.

Please note that all communications with law enforcement will be dealt with via Head of Campus Security – Mark Kennell and the Press and Media Relations Team, will coordinate any communications with the press or public.

5. Incident Response Team Actions

The incident may proceed through the following stages, this will be determined by the Incident Lead:

- Call an emergency meeting of the Incident Response Team to review the completed incident response form and allocate actions to the team. All actions to be logged using appendix 2 – Action Log.
- Inform additional Key University Team members and brief them on the situation. Executive Team, Head of Campus Security – Mark Kennell and Senior Press and Media Relations Manager – Tom Frew
- Identify all relevant parties to be alerted and agree how this will be done. See appendix 3 for list of relevant parties. All communications should be treated as confidential, with the majority of these communications coming via the Senior Press and Media Relations Manager's team.
- Collect and protect information associated with the intrusion;
- In the event that forensic investigation is required, the Incident Response Team will work with legal representatives and management to identify appropriate forensic specialists; An up to date list of qualified PCI Forensic Investigators (PFI's) is held on the PCI Security Council website at https://www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators
- Where a PFI is requested by the University's Acquirer, the contract must be signed within 10 calendar days and they must be on site within 5 calendar days of the contract being signed.
- Eliminate the intruder's means of access and any related vulnerabilities;

- Research potential risks related to or damage caused by intrusion method used;
- Provide all compromised Visa, Interlink and Plus accounts to the Visa Europe acquiring bank or to Visa Europe **within 5 business days** via the University's Acquirer. All potentially compromised accounts must be provided and transmitted as instructed by the Visa Europe Acquiring bank and Visa Europe. Visa Europe will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information.
- Also **within 5 business days** of the reported compromise, provide a Compromised Entity Details Report to the Visa Europe member or to Visa Europe via the University's Acquirer. See Visa Europe guidance for further details and the report.
- Assist the PFI where necessary. The PFI will most likely require access to data, facilities and people. They might also require access to third-party service providers who store, process, or transmit cardholder data on behalf of the University. The PFI is not appointed to apportion blame, but instead to find out what has happened in order to help the University to recover quickly. It is therefore essential that appropriate employees are available to assist with the PFI's investigations, and that they are open and honest, understanding the importance of the PFI's role.
- Maintain ongoing communications with the University's Acquirer who will support and advise on timelines and requirements for reporting.

6. Post Incident Response Actions

Within a week of the incident being reported the Response Team will meet to evaluate the effectiveness of the Incident Response Plan. Depending on the size and complexity of the incident the investigation may still be ongoing at this time. Where the root cause of the compromise has been identified, the response team will ensure all areas in which the policy or security control can be made more effective or efficient, are updated accordingly. Where applicable additional staff training will be identified and followed up with departments.

Appendix 1 - Incident Response Form – Cardholder data breach

On completion, send to the officers recorded below*

Requirement	**Response**	**Follow up actions**
Note: Any suspected breach should be notified immediately to the PCI DSS Incident Response Team via the IT Services Helpdesk.		
Date and Time of Report:		
Name, job title and contact details of person writing report		
Confirmed or Suspected Incident?		
How did you become aware of the Incident?		
Date/time of Incident (if known)		
Nature of Incident		

Areas / systems affected		
Any other information surrounding the Incident?		

*** Reporting and decisions made**		
Name / Job Title reported to	**Date reported**	**Decision of action to take**
Line Manager		
Income Office Manager		
Data Protection Liaiosn/Compliance Officer		
PCI DSS Team		

Appendix 2 - Action Log

Response coordinated by: [insert full name]

Action Log maintained by: [insert full name]

Action / Decision No.	Date / Time	Action/Decision Description	Person Responsible	Completed (Date / Time)	Outcome / Comments
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					

Appendix 3 – Relevant Parties to be contacted in the event of a breach.

University's Acquirer	Global Payments, Grahame Vincent, Corporate Relationship Manager (Global Payments will report to the Card Companies ie Visa and Mastercard) Initial contact required within 24 hours of suspected compromise
University's Executive Team	
University Staff and Students if breach prevents business as usual (Internal Communications Team)	
National Crime Agency	0370 496 7622. Initial contact required within 48 hours of suspected compromise
Office for Students	via Governance Team, if the breach results in a loss >£25,000
Information Commissioner	via the IDC Team