



INCIDENT RESPOSE PLAN

If a compromise is suspected, please follow the course of action below

Contact the Incident Response Officer (normally the Treasury & Transactions Manager (k.parks-smith@napier.ac.uk))

If the Treasury & Transactions Manager is unavailable contact the Head of Systems and Assurance (d.breckenridge@napier.ac.uk)

The Incident Response Officer will

- Alert the Network Services and Security Manager
- Conduct an initial investigation of the suspected compromise
- If a compromise of breach of information is confirmed will alert Senior Management and authorised University personnel
- Inform parties that may be affected by the compromise
- Provide advice regarding processing further transactions

If the compromise involves card account numbers the Incident Response Officer will

- Contact Network Services and Security Manager to contain and limit the exposure by shutting down any processes or systems affected by the compromise
- Alert necessary parties (Merchant bank, Visa Fraud Control, Mastercard via Merchant Bankers, the Police (crime reference required))
- Provide compromised or potentially compromised card numbers/details to Merchant Bank/Visa Fraud Control within 24 hours
- For further information see
 - 'Account Data Compromise Master' [PCIDSS SharePoint Site](#) or
 - [PCIDSS page](#) on Treasury and Transactions section on staff Intranet.
- All policies and procedures and further information is available on [PCIDSS SharePoint Site](#)

Incident Analysis

After 7-10 days following the data breach and implementation of the Response Plan, the Incident Response Officer and all affected parties will meet to review;

- Results of any investigation
- Determine root cause of breach/compromise
- Evaluate effectiveness of plan
- Review other security controls to determine appropriateness of current risks
- Identify areas where procedures can be improved, and/or made more effective or efficient.
- Agree policies and procedures to be updated