**WCU Payment Card Security Incident Response Plan**

PCI DSS requires that merchants create and document an incident response plan and test the plan annually. The WCU PCI Security Incident Response Team (PCI Response Team) is comprised of the University Controller, the Bursar, the Information Security Officer, the Chief Information Officer, an investigator from the University Police Department, and a representative from Communications and Public Relations, Legal Counsel and Internal Audit. The WCU PCI security incident response plan is as follows:

1. WCU Payment Card Processing Policy dictates that each merchant department must report suspicious activities, evidence of tampering or security incidents first to the WCU Police Department and then the Controller’s Office.
2. Incidents affecting the cardholder data environment detected by the IT Division will be reported to the Information Security Officer or the Chief Information Officer. The person receiving the report will advise the PCI Response Team of the incident.
3. The PCI Response Team will investigate the incident, assess the threat and assist the potentially compromised department in limiting the exposure of cardholder data and in mitigating the risks and impacts associated with the incident.
4. The PCI Response Team will determine if an account compromise event has occurred or a security breach has occurred wherein there is a suspected or confirmed loss or theft of any material or records that contain cardholder data.
5. The PCI Response Team will notify the Office of State Controller within 24-hours of the report and with their help resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (card brands, merchant card processors, etc.) as necessary.
6. If business recovery and continuity is a concern for the merchant department(s) then the Controller’s Office should be contacted for advice and possible rental of their cellular point-of-sale terminal.
7. The PCI Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.
8. If it is determined that a security breach has occurred that may have compromised cardholder data then a formal PCI Incident Response Report may need to be completed.

# WCU PCI Response Team Contact Information

|  |  |
| --- | --- |
|  |  |

University Police - 828-227-8911

Controller - 828-227-3112 David Steinbicker [bdsteinbicker@wcu.edu](mailto:bdsteinbicker@wcu.edu)

Bursar - 828-227-3102 Brady Proffitt [bproffitt@wcu.edu](mailto:bproffitt@wcu.edu)

CISPO - 828-227-2667 Joel McKenzie [mckenzie@wcu.edu](mailto:mckenzie@wcu.edu)

CIO - 828-227-7282 Craig Fowler [cfowler@wcu.edu](mailto:cfowler@wcu.edu)

Office of the State Controller Risk Mitigation Services - 919-707-0757 [ben.mclawhorn@osc.nc.gov](mailto:ben.mclawhorn@osc.nc.gov)

Coalfire Forensic Services -

Kyesha Moultrie (O) 678-808-3808 (M) 856-275-0513 [kyesha.moultrie@coalfire.com](mailto:kyesha.moultrie@coalfire.com)

Jim Fish 877-224-8077 x7501 [jim.fish@coalfire.com](mailto:jim.fish@coalfire.com)

Jon Bonham 877-224-8077 x7526 [jon.bonham@coalfire.com](mailto:jon.bonham@coalfire.com)

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

**Payment Card Security Incident Response Procedures**

As a participant in the State Controller’s Master Services Agreement for Merchant Card Services, the participant is to consult first with the Office of the State Controller (OSC), and the OSC shall make the appropriate notifications on the agency’s behalf, or advise otherwise.

1. The WCU Controller’s Office shall notify the Office of the State Controller within 24 hours of a known or suspected security breach.
2. When reporting a security incident to the OSC, all pertinent details of the incident are to be provided to assist the OSC in making an assessment of the seriousness and extent of the incident. Any credit card data provided to the OSC as part of the assessment process shall be transmitted in a secure encrypted manner.
3. Whenever a press release regarding the occurrence of a security breach is warranted, the OSC should be consulted first, in order to coordinate the timing of the release with any other notifications that may be required.
4. In cases where a security incident is required to be reported to the card brands, they may require a forensic investigation to be performed by a Qualified Security Accessor (QSA). WCU will first use the QSA that the OSC has a contract with to provide such services. WCU is responsible for the costs of any forensic services provided.

Additionally, in response to a systems compromise, the PCI Response Team and designees will:

1. Ensure compromised system/s is isolated on/from the network;
2. Gather, review and analyze the logs and related information from various central and local safeguards and security controls;
3. Assist the QSA in conducting appropriate forensic analysis of compromised system;
4. Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required;
5. Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.

Response to incidents detected by the IT Division:

1. Detection of unauthorized wireless access points: The Networking Department of the IT Division will investigate the alert by tracking down the location of the access point and logging the time it first appeared on the network and the duration if applicable. They will disable the access point once enough information has been gathered from the device. Once the information has been reported to the PCI Response Team they will investigate the incident with the department where the access point was located.
2. Alerts generated by the change-detection systems or log monitoring systems: Depending on the nature of the alert a team within the IT Division will investigate the details and assess the threat to the cardholder data environment. If the alerts indicate a security incident has occurred they will report the findings to the PCI Response Team and assist with further investigation and mitigation of the risk.