Payment Card Industry Data Security Standard (PCI DSS)
Incident Response Plan
Required Documentation

Definition: A "cardholder data security incident" is an event in which one or more debit/credit cards has been compromised or appears to have been compromised. This includes incidents involving any known or suspected compromise of a computer, server, register, media (including paper) or other device directly involved with the storage, processing, or transmission of cardholder data.

Incident Response Procedures:

1) Immediately upon experiencing a suspected or confirmed security breach, the staff member will contact the departmental IT Manager and Merchant Owner/Business Manager of the affected unit. If these people cannot be reached, contact Duke's E-Commerce Office or IT Security Office. Refer to contact information noted at the end of this document.

2) The departmental IT manager will immediately contact Duke's IT Security Office and the E-Commerce Office if a confirmed or suspected breach (incident) of cardholder data has occurred.

3) Duke's IT Security Office will conduct a thorough investigation of the incident. The departmental IT manager will immediately contain and limit the exposure to minimize further loss of cardholder data, however, to preserve evidence and facilitate the investigation:
   - Do not access or alter compromised systems (i.e. do not log on to the machine and change passwords, do not log in as ROOT).
   - Do not turn off the compromised machine. Instead, isolate compromised systems from the network (i.e. unplug network cable).
   - Preserve logs and electronic evidence. Log all actions taken.
   - If using a wireless network, change SSID on the AP and other machines that may be using this connection with the exception of any systems believed to be compromised.
   - Be on "high" alert and monitor all systems associated with cardholder data.
   - Take no additional action until directed by either the IT Security Office or the E-Commerce Office.

4) In the event unauthorized wireless devices are detected, merchants must immediately contact Duke's IT Security Office and the E-Commerce Office, even if there is no suspected incident.

5) The departmental IT manager will issue immediate and intervening orders designed to:
   - Follow directives provided by the IT Security Office and E-Commerce Office to further secure the cardholder information and equipment in question.
   - Maintain business operations to the extent that this is safe and possible.
   - Arrange for secure alternative methods of credit card processing with the E-Commerce Office until usual systems can safely be restored.

6) The departmental IT manager will work with the IT Security Office and the E-Commerce Office to assess the incident. Assessment may include the:
   - Number of accounts and the associated data at risk (account number, expiration date, cardholder name, address, CV code, track data, PIN, etc).
   - Attack vector and method; the source of the compromise will be identified.
   - Timeframe of the compromise.

7) The E-Commerce Office will contact Duke's merchant acquiring bank as needed to report any fraud and will coordinate subsequent fraud control steps with issuing card companies. The E-Commerce Office will instruct the merchant departments on any further incident reporting with banks and/or card companies.

Payment Card Industry Data Security Standard (PCI DSS)
Incident Response Plan
Required Documentation

8) If needed, Duke's IT Security Office will contact the local office of the Secret Service and other internal senior officers as appropriate (i.e., Duke University Public Affairs).

9) The departmental IT and Business Managers will coordinate final procedures in the incident recovery with oversight from the IT Security Office and E-Commerce Office.

Departmental Contact Information:

Name	Phone	Email
Technical Contact: Neil Prentice – IT Director	**919-613-9355**	**neil.prentice@duke.edu**
Merchant Owner: Zach Johnson –Associate Dean for Finance and Administration	**919-613-7310**	**zach.johnson@duke.edu**
Additional Departmental Staff: Kirk Bostwick, HelpDesk Manager	**919-681-1740**	**kirk.bostwick@duke.edu**
Additional Departmental Staff: Beverly Harris, Director of Finance	**919-613-7378**	**beverly.s.harris@duke.edu**

Corporate Contact Information:

Office	Phone	Email
E-Commerce Office	919-681-6455 919-681-2446	christa.stilleypoe@duke.edu steve.marciniak@duke.edu james.mccullen@duke.edu ecommerce@duke.edu
University IT Security Office		security@duke.edu
After Hours Emergency Contact: OIT Help Desk *Reference your department name and related details to ensure the proper escalation.*	919-684-2200	Click here to report a CREDIT CARD SECURITY PROBLEM *https://www.dukeonline.duke.edu/invoice/dukepay/DukePayHelp.html*

Payment Card Industry Data Security Standard (PCI DSS)
Incident Response Plan
Required Documentation

Annual Incident Response Plan Test
Merchants should test their incident response plan annually and record results in the following table. An example incident response plan test is provided; your actual tests should reflect your department's unique information.

- Tabletop Exercises: Tabletop exercises are facilitated, discussion-based exercises where personnel meet to discuss roles, responsibilities, coordination, and decision-making of a given scenario. Tabletop exercises provide a good mechanism to ensure personnel with incident response duties understand their roles, responsibilities and procedures.

- Functional Exercises: Functional exercises allow personnel to validate their readiness for emergencies by performing their duties in a simulated environment.

Test Date	Duke Staff Involved	Test Scenario	Test Results	Lessons Learned/ Modifications Needed
10/17/23	David Arrington, Neil Prentice, Stan Paskoff, Zach Johnson, Stephanie Martinek	A potential breach in our Duke Public Policy account has been reported to you. Where is the Incident Response Plan you need to to take action?	All involved were able to locate the Incident Response Plan.	Users found the plan in different locations – keeping it in the shared drive as well as our internal Intranet is essential to ensure everyone can find it if need be.