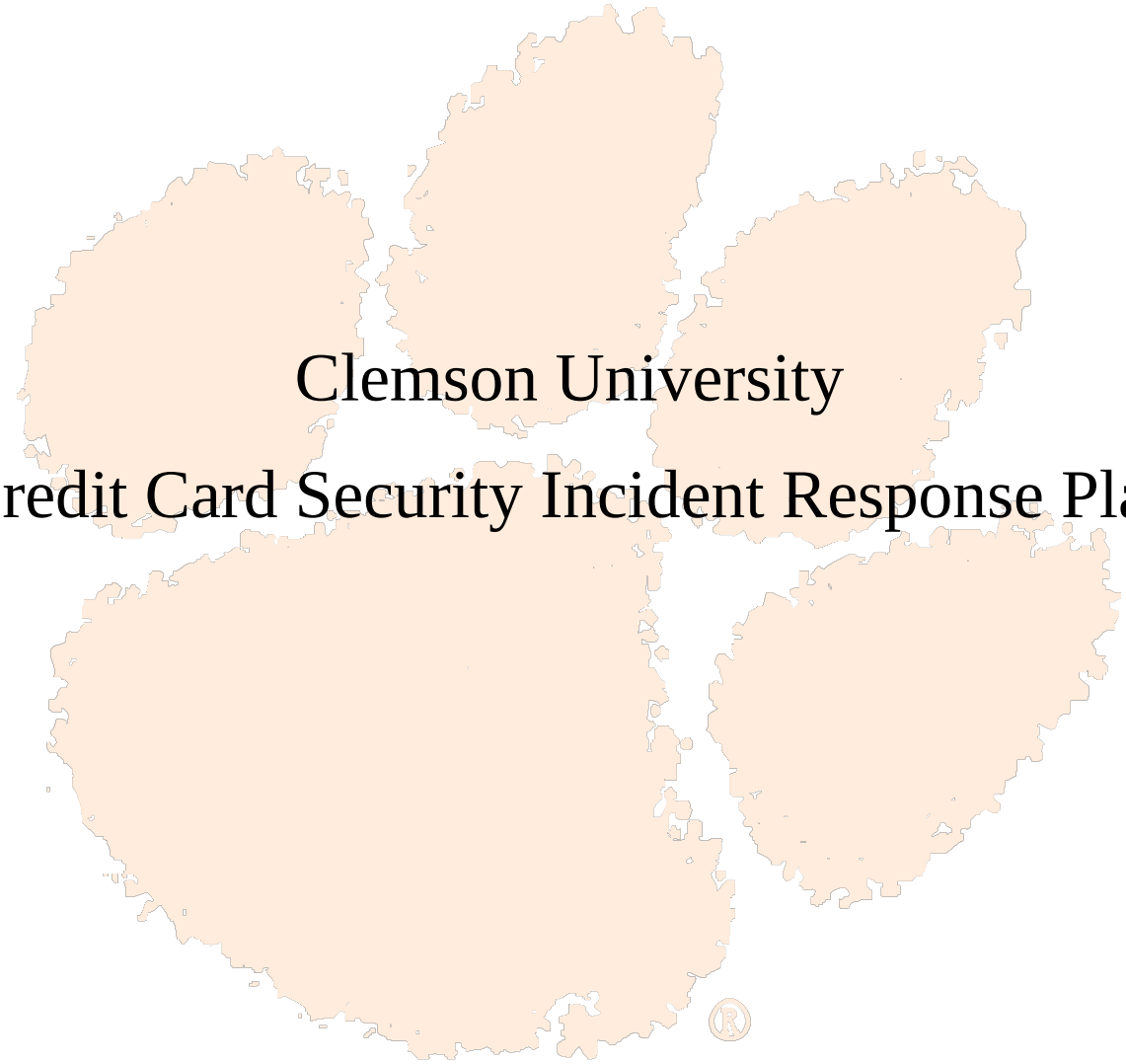


Clemson University

Credit Card Security Incident Response Plan

To address credit cardholder security, the major card brands (Visa, MasterCard, Discover, American Express and JCB) jointly established the PCI Security Standards Council to administer the Payment Card Industry Data Security Standards (PCI DSS) that provide specific guidelines for safeguarding cardholder information. One of these guidelines requires that merchants create a security incident response team and document an incident response plan. The Clemson University Credit Card Security Incident Response Team (Response Team) is comprised of CCIT Security and Privacy and Cash and Treasury Services. (see below for names and contact information).

The Chief Information Security Officer (CISO) and the Office of Cash and Treasury Services lead the response team when an incident occurs. The CISO will determine if other University staff should be notified of the breach. The team also includes representatives from:

- Controller's Office
- CU Media Relations
- Internal Audit
- Office of General Council
- Risk Management

1. All incidents must be immediately reported by completing the form located at http://www.clemson.edu/ccit/help_support/safe_computing/report/index.html
2. The CCIT Incident Report will notify all members of the Incident Response Team.
3. The Response Team, along with other University staff, will investigate the incident and assist the compromised department in limiting the exposure of cardholder data.
4. The Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary.
5. The Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future.

Position Title	Name	Office Phone Number	Email Address
Chief Information Security Officer (Interim)	Hal Stone	864-656-7132	hastone@clemson.edu
Associate Director of Cash and Treasury Services	Stephanie Barker	864-656-5271	wald2@clemson.edu
Payment Card Coordinator	Cathy Freeman	864-656-0530	cdorfne@clemson.edu

Incident Response Plan

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

In the event of a *suspected or confirmed* incident:

1. All incidents must be immediately reported upon discovery to members of the Response Team. Contact the Response Team by completing the form located at http://www.clemson.edu/ccit/help_support/safe_computing/report/index.html
2. Immediately contain and limit the exposure and preserve evidence by taking the following steps:
    a. Do not access or alter compromised systems (i.e., don't log on to the machine and change passwords, do not log in as ROOT).
    b. Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug Ethernet cable, disable wireless).
    c. Preserve logs and electronic evidence.
    d. Log all actions taken.
    e. If using a wireless network, immediately contact the Payment Card Coordinator in the Office of Cash and Treasury Services at 864-656-0530 or cdorfne@clemson.edu to deactivate the Wi-Fi.
    f. Be on "high alert" and monitor all systems with cardholder data.
3. Document any steps taken until the Response Team has arrived. Include the date, time, person/persons involved and action taken for each step.
4. Assist the Response Team as they investigate the incident.
5. If an incident of *unauthorized access* is **confirmed** and card holder data was potentially compromised, the Payment Card Coordinator with the Office of Cash and Treasury Services will contact the System's acquiring bank as follows:

    a. For incidents involving Visa, MasterCard or Discover network cards, contact FirstData Merchant Services Account Manager at 301-766-5789 or sc.gov@firstdata.com within 72 hours of the reported incident.
    See Appendix A – FirstData Merchant Services – Responding to a Breach
    b. For incident's involving American Express cards, contact American Express Enterprise Incident Response Program (EIRP) within 24 hours after the reported incident at (888)-732-3750 or email EIRP@aexp.com.
    See Appendix A – American Express – Responding to a Breach

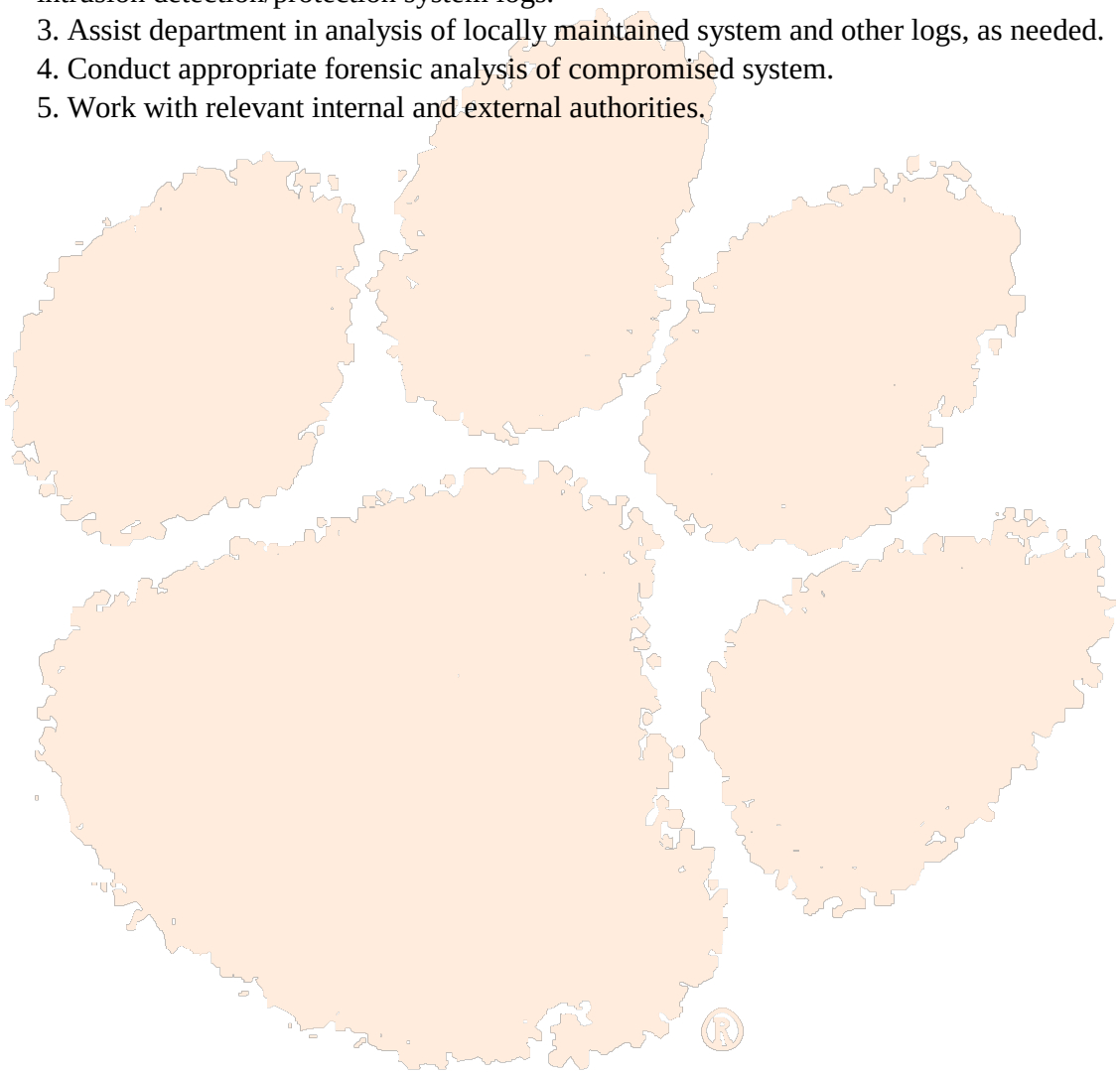
6. If an incident of *unauthorized access* is confirmed and card holder data was potentially compromised, the Payment Card Coordinator will coordinate with the Response Team to proceed as indicated in Appendix A.

IT Security Incident Response Procedures

The Clemson University Credit Card Security Incident Response Team must be contacted by a department in the event of a system compromise or a suspected system compromise. After being notified of a compromise, the Response Team will implement their incident response plan to assist and augment departments' response plans.

In response to a system compromise, the Response Team will:

1. Ensure compromised system is isolated on/from the network.
2. Gather, review and analyze all centrally maintained system, firewall, file integrity and intrusion detection/protection system logs.
3. Assist department in analysis of locally maintained system and other logs, as needed.
4. Conduct appropriate forensic analysis of compromised system.
5. Work with relevant internal and external authorities.



The credit card companies have specific requirements the Response Team must address in reporting suspected or confirmed breaches of cardholder data. See Appendix A for these requirements.

APPENDIX A

FirstData Merchant Services – Responding to a Breach
https://www.firstdata.com/downloads/thought-leadership/13405_0714_Payment_Card_Data_Breach.pdf

MasterCard – Responding to a Breach
https://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf

Visa – Responding to a Breach
https://usa.visa.com/support/small-business/data-security.html/merchant-pci-dss-compliance.jsp

American Express – Responding to a Breach
https://www209.americanexpress.com/merchant/services/en_US/data-security