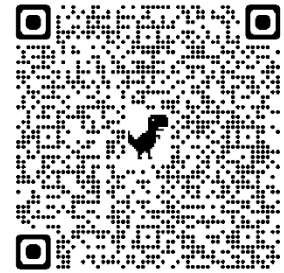


Cardholder Data Security Incident Response Plan



E-Commerce & Virtual Terminal

Business Name: _____
Incident Response Lead: _____
Incident Response Deputy: _____
Manager/Director to Notify _____



THREAT INDICATORS

E-Commerce

- QR code tampering
- A third-party partner reports a breach
- Suspicious financial transactions
- Suspicious activity on the Application
- Unauthorized access to a system or network
- Gateway and application's daily financial reports don't reconcile

Virtual Terminal and Gateway Access

- Suspected malware:
 - Frequent random pop-up windows
 - Passwords no longer working
 - Anti-virus alerts or anti-virus shutting down
 - Frequent crashes or unusually slow performance
 - Hung process
- Customer reports compromised credit/debit card
- Hidden camera recording entry of credentials



STOP processing transactions immediately



DO NOT unplug power



If Virtual Terminal - **unplug network cable**



DO NOT alter or access the compromised system (e.g., do not log in to change passwords)



Preserve electronic evidence



Report the incident indicating **urgency, PCI & credit card breach** to the ITSServiceDesk@cunet.carleton.ca or call **613-520-3700**



Notify your supervisor and the designated incident response lead/delegate



Notify PCICompliance@Carleton.ca



Log all actions taken