Cardholder Data Security Incident Response Plan

Carleton University

Standalone Cellular (wireless) and Network-Connected Terminals

SCAN ME

MID: ______________________________

Business Name: ______________________________

Incident Response Lead: ______________________________

Incident Response Deputy: ______________________________

Manager/Director to Notify ______________________________

THREAT INDICATORS

- Signs of break-in/damage on a secured, locked cabinet storing payment card data;
- Lost paper forms containing payment card data;
- A skimming device or unusual attachment on a POS device;
- A tamper warning message or a broken tamper proof seal on a POS device;
- Serial numbers on the PIN pad device not matching those on record, indicating a switch;
- A missing POS device, indicating theft or loss;
- Unfamiliar equipment surrounding your PCI terminal or POS device;
- Hidden camera recording entry of authentication credentials;
- Multiple refunds going to the same card;
- Customer reports compromised credit/debit card;
- Suspicious behaviour around devices

⊗ **STOP** processing transactions immediately

⚠ DO NOT unplug power

⚠ If IP-connected - **unplug network cable**

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

✓ Preserve logs and 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/deputy

✓ Notify PCICompliance@Carleton.ca

✓ Log all actions taken