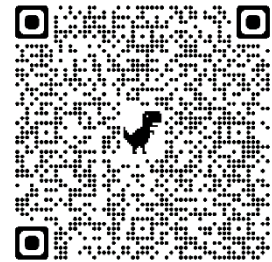# Payment Card Data Security Incident Response Plan

Standalone Cellular (wireless) and Wired Terminals

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;
- ➤ QR code tampering;
- ➤ 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
- ✅ Notify your supervisor and the designated incident response lead/deputy
- ✅ Report the incident indicating urgency, PCI & credit card breach to the ITSServiceDesk@cunet.carleton.ca or call **613-520-3700**
- ✅ Notify PCICompliance@Carleton.ca
- ✅ Log all actions taken