**Reporting an Incident Procedures**

|  |
| --- |
| * Ensure all facts about the incident are properly documented, verified and validated before reporting to ITSC
 |

|  |
| --- |
| * Who should be informed or notified about the incident?
* Follow the chain of command within your department before reporting an incident to ITSC
 |
| Primary contact | {Name of Person} | {Contact number} |
| Alternate contact | {Name of Person} | {Contact number} |

|  |
| --- |
| * Who should report the incident to ITSC?
* The designated person responsible for contacting ITSC should have all the pertinent facts and information about the incident
 |
| Primary | {Name of Person} | {Contact number} |
| Alternate | {Name of Person} | {Contact number} |

|  |
| --- |
| * Call ITSC at 604-822-6141 – Per [Incident Response Plan](http://cio.ubc.ca/sites/cio.ubc.ca/files/documents/resources/UBC%20Incident%20Response%20Plan.pdf) and [Information Security Standard #04](http://cio.ubc.ca/sites/cio.ubc.ca/files/documents/standards/Std%2004%20Reporting%20Information%20Security%20Incidents.pdf)
 |

|  |
| --- |
| * When do you contact Campus Security and/or RCMP?
* You may initially contact Campus Security and/or RCMP if the incident involves an imminent danger or physical threat
 |
| Campus Security | Vancouver Dispatch (24/7) | 604-822-2222 |
| Campus Security | Okanagan: Administration | 250-807-8859 |
| Campus Security | Okanagan: After Hours Emergency | 250-807-8111 |
| UBC RCMP | Vancouver Detachment | 604-224-1322 |
| UBC RCMP | Okanagan Detachment | 250-762-3300 |

|  |
| --- |
| * Business Recovery and Continuity Procedures
 |
| * POS/PIN pad
 | Discontinue the use of the POS device (PIN pad/parking machine) and disconnect from network or telephone line – Contact ITSC |
| * Virtual Terminal
 | Contact ITSC |
| * Server
 | Contact ITSC |

|  |
| --- |
| * Any contact with the Acquirer/Card Companies (regarding an incident) is coordinated through the PCI Working Committee and not by the Merchant
 |

Fill up the name of the contact person and number and distribute this information to all of the staff involved in credit card processing. The Incident Assessment Questionnaire outlines the gathering of information that will easily facilitate the communication of the incident to ITSC.

**Incident Assessment Questionnaire**

|  |  |
| --- | --- |
| **Question** | **Response/Comments** |
| When was the incident discovered? |  |
| When did the incident occur (if different from date of discovery)? |  |
| Who discovered the incident? |  |
| What type of incident occurred? | System/Data CompromiseNetwork Attack/Malware/VirusLost/Stolen EquipmentLost/Stolen DataPhysical Compromise of POS (e.g. damage/tampering)UBC Policy Violation, e.g PCI DSS, emailOther – please describe \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Was cardholder data involved?NoYes – select what type of data is involved | Credit Card NumberCardholder NameExpiration DateNone |
| Was sensitive authentication data involved? | Full Magnetic Stripe DataCVVPINNone |
| What is the estimated number of people or records impacted? | None0-499500 or above |
| Does the incident compromise business operation continuity (availability)? | NoPotentiallyYesUnknown |
| Is there a need for client/customer notification? | NoPotentiallyYes |
| What steps have been taken to resolve or rectify the incident? |  |