**{Department Name} – Incident Report Template & Guidelines**

**Report Date/Time:**

**Report Incidents**

If the suspected activity involves computers (hacking, unauthorized access, etc.), immediately notify CCMS (cash.credit.services@ttu.edu) and TTU IT Security (security@ttu.edu). They will notify the CISO.

**Confidentiality**

Distribution of this document is limited to the {Department Name}, Cash and Credit Card Management Services, and IT Security. Access should only be granted to those with a business related need-to-know. If you have any questions pertaining to the distribution of this document, please contact the {insert school’s authorizing department manager/executive}.

##### Reporting Party

|  |  |
| --- | --- |
| Name:  |  |
| Title:  |  |
| Telephone/Email: |  |

##### Summary

The summary is at a high level, suitable for upper management. Elements include:

* Basic description of the incident
* Systems, services and/or user communities impacted by the incident
* Whether service was not impacted, degraded, or interrupted
* Duration of the incident (start to finish)

|  |
| --- |
|  |

##### Details of the Incident, Steps Taken To-date

Specifically, what caused the incident (who, what, where, when, how) and what steps have been taken by the reporting party to-date.

* Description of the incident
* Detail the flow of the incident response (i.e. John -> Jim -> Mike)

Systems

|  |  |
| --- | --- |
| Steps Taken To-date: |  |
| Network cable unplugged (time/date): |  |
| Last time machine rebooted (time/date): |  |
| When anomalous activity was noticed (time/date): |  |
| IR Team notified (time/date): |  |
| Additional Details: |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: Title:

##### IRT Lead

* Identify the IR team member assigned to take the lead on this incident.

|  |  |
| --- | --- |
| Name:  |  |
| Title:  |  |
| Telephone/Email: |  |

##### Incident Analysis

Identify the IR

|  |  |
| --- | --- |
| PCI Event Yes/No: |  |
| Justification:  |  |

**If PCI Event is “Yes” complete the following steps.**

##### Time/date of step 5 notification

|  |  |
| --- | --- |
| PCI IRP Step 5 notification (time/date): |  |

##### Steps taken during forensic investigation

|  |
| --- |
|  |

**ATTACHMENTS**

Please attach any supporting documents. These documents may include:

* Logs or error messages
* Contents of trouble tickets
* Contents of e-mail

##### Conclusion, Findings and Recommendations

* What was the basic cause of the incident?
* What could have prevented this?
* Impact (none, degraded performance, downtime)
* Business criticality (revenue producing, business critical, low)
estimated cost (impact + business criticality)
* What prevents the incident from reoccurring?
* What additional actions or research need to happen?

|  |
| --- |
|  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: Title: