IT Security Incident Reporting Form

Instructions: This form is to be completed as soon as possible following the detection or reporting of an Information Technology (IT) security incident. All items completed should be based on information that is currently available. This form may be updated and modified if necessary.

1. Contact Information for this Incident	
Name:	
Title:	
Department:	
Work Phone:	
Mobile Phone:	
Email address:	

2. Incident Title or Work Order Number:

Provide a brief description:

3. Impact / Potential Impact Check all of the following that apply to this incident.

- □ Loss / Compromise of Data
- □ Damage to Systems
- □ System Downtime
- □ Financial Loss
- □ Other Organizations' Systems Affected
- □ Damage to the Integrity or Delivery of Critical Goods, Services or Information
- □ Violation of legislation / regulation
- □ Unknown at this time

Provide a brief description:

4. Sensitivity of Data/Information Involved Check all of the following that apply to this incident.

Sensitivity of Data	
Category	**Example**
DCL1: **Public Data**	This information has been specifically approved for public release by Public Relations department or Marketing department managers. Unauthorized disclosure of this information will not cause problems for OTC, students, faculty & staff, or its business partners. Examples are marketing brochures and material posted to OTC web pages.
DCL2: **Sensitive**	This information is intended for use within OTC between departments and in some cases business partners. Unauthorized disclosure of this information to outsiders may be against laws and regulations, or may cause problems for OTC, students, faculty & staff, or its business partners. This type of information is already widely distributed within the college, or it could be distributed within the organization without advance permission from the information owner. Examples are documents stored on the R drive and most internal electronic mail messages.
DCL3 or DCL4: **Restricted or Highly Restricted**	This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Unauthorized disclosure of this information to people without a business need for access may be against laws and regulations, or may cause significant problems for OTC, students, faculty & staff, or its business partners. Decisions about the provision of access to this information must be cleared through the information owner. Examples include and data that contains personal identifiable information (PII). PII is any data that could potentially identify a specific individual or information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data.
Unknown/Other	Describe in the space below.

□ DCL1 □ DCL2	□ DCL3 or DCL4 □ Unknown / Other

Provide a brief description of data that was compromised:

5. Who Else Has Been Notified?

Provide Person and Title:

6. What Steps Have Been Taken So Far?

Check all of the following that apply to this incident.

□ No action taken
□ System Disconnected from network
□ Updated virus definitions & scanned system

□ Restored backup from tape
□ Log files examined (saved & secured)
□ Other – please describe:

Provide a brief description:

7. Incident Details

Date and Time the Incident was discovered:	
Has the incident been resolved?	
Physical location of affected system(s):	
Number of sites affected by the incident:	
Approximate number of systems affected by the incident:	
Approximate number of users affected by the incident:	
Are non-OTC systems, such a business partners, affected by the incident? (Y or N – if Yes, please describe)	
Please provide any additional information that you feel is important but has not been provided elsewhere on this form.	

Please email this completed form to:
OTC Information Security
security@otc.edu