UTS
UNIVERSITY OF TECHNOLOGY, SYDNEY

IT SECURITY INCIDENT REPORTING PROCEDURE

UTS:INFORMATION TECHNOLOGY DIVISION

OVERVIEW

The IT Security Incident Reporting Procedure ensures the UTS Information Security team is properly informed of any information security incident.

PURPOSE

The IT Security Incident Reporting Procedure provides all UTS personnel, vendors, contractors, third parties and service providers the appropriate information to report an information security incident.

SCOPE

The procedure encompasses all UTS data and IT resources.

INCIDENT IDENTIFICATION

Each person has a different interpretation of what an information security incident entails. The following list provides a few examples of what should be reported as an information security incident:

- A compromised account (e.g. email account)
- Stolen IT property that contains UTS data
- Out of the ordinary network activity
- Attempted unauthorised access to an IT system
- A violation of the IT Security Policy or one of the IT directives.

This list is by no means exhaustive. If there is any doubt of whether or not to report an incident, you may contact the Information Security team on **(02) 9514 9009** or via email at **itsecurity@uts.edu.au** for more information.

INCIDENT REPORTING

Once an incident has been identified, alert the Information Security team via phone.

The Information Security team may be reached on **(02) 9514 9009**

If unavailable, contact the IT Support Centre on **(02) 9514 2222**

The Information Security team will record and document relevant information. We will then provide you with an Incident Response Form to complete and return.

The proper response to incidents often depends on timely action, requiring all incidents be reported as soon as possible. Incidents must be reported within 24 hours of identification.

INCIDENT RESOLUTION

The Information Security team will evaluate the incident and decide what steps need to occur next. Depending on the severity of the situation, an Incident Response Team (IRT) may be deployed to look into the situation further or the incident may be documented by the Information Security team and taken care of by a resource administrator.