Audit Vulnerability Scan Policy

Section 1 - Overview

(1) The purpose of this policy is to authorise the Information Technology Directorate (ITD) to undertake audit and scanning of UNE IT infrastructure in order to ensure compliance with the Information Security Rule and compliance with relevant statutes. It sets forth an agreement regarding network security scanning by ITD or by a University appointed external agency to audit UNE IT networks, servers and client PCs. Information Technology Directorate or an authorised agency will utilise network auditing/vulnerability software to perform regular electronic scans of the UNE network, PCs and/or firewalls or on any IT system at UNE.

(2) Audits may be conducted to:

a. Ensure integrity, confidentiality and availability of information and resources
b. Investigate possible security incidents and to ensure conformance to UNE security policies
c. Ensure that the University is in compliance with copyright laws and acts.

Section 2 - Scope

(3) This policy covers all computer and communication devices owned or operated by UNE and strategic computer platforms that are managed and operated by the Information Technology Directorate.

(4) This policy also covers any computer and communications device that are present on UNE premises, but which may not be owned or operated by UNE (e.g. personal laptops connected to the UNE network).

(5) The Information Technology Directorate has authority over the UNE main campus network, Wide Area Links, Access Centres, remote campuses and network links to the internet. The Information Technology Directorate will be subject to relevant privacy legislation and nothing in this policy is to be interpreted as an intention to act outside this legislation.

Section 3 - Policy

(6) It is a condition of use of UNE's IT infrastructure that staff and Students consent to allow the Information Technology Directorate or an authorised agency to perform an audit and any associated scans.

(7) ITD Staff or an authorised agency that has been assigned to conduct scans will identify to the helpdesk the dates when the scan is to take place. If staff or students notice any problems during the scans, the Service Desk should be informed.

(8) These scans will require access that may include:

a. user level and/or system level access to any computing or communications device;
b. access to information (electronic, hardcopy, etc.) that may be produced transmitted or stored on UNE equipment or premises;

c. access to work areas (labs, offices, cubicles, storage areas, etc.); and
d. access to interactively monitor and log traffic on UNE networks.

Status and Details

Status	Current
Effective Date	27th July 2015
Review Date	12th January 2015
Approval Authority	Vice-Chancellor and Chief Executive Officer
Approval Date	14th November 2011
Expiry Date	To Be Advised
Unit Head	Angie Hendrick Chief Information Officer 02 6773 2044
Author	Robert Irving Chief Information Officer
Enquiries Contact	Information Technology Directorate +61 2 6773 5000

Glossary Terms and Definitions

"**Student**" - Is an admitted student or an enrolled student, at the relevant time: 1. an admitted student is a student who has been admitted to a UNE course of study and who is entitled to enrol in a unit of study or who has completed all of the units in the UNE course of study; 2. an enrolled student is a student who is enrolled in a unit of study at UNE.