

University of New England

Audit Vulnerability Scan Policy

Document data:

| | |
|---|---|
| Document type: | Policy |
| Administering entity: | ITD |
| Records management system number: | D11/30639 |
| Date approved: | 14 November 2011 |
| Approved by: | Vice-Chancellor |
| Indicative time for review: | 3 years |
| Responsibility for review: | ITD |
| Related policies or other documents: | UNE Risk Management Policy, Rules for the Use of Information and Communications Facilities and Services, Information Technology Security Policy, IT Security Objectives and Framework , General Password Policy, P2P File Sharing Policy, Personal Mobile Computing Policy, Standards and Guidelines for all Users of University Computing and Network Facilities, Standards and Guidelines for Desktop Computers, Standards and Guidelines for Non-Strategic Systems, Standards and Guidelines for Strategic Systems |

1. Rationale and Scope

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 IT Security Policy 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. ITD 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.

Audits may be conducted to:

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

This policy covers all computer and communication devices owned or operated by UNE and strategic computer platforms that are managed and operated by IT.

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).

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

2. Policy

It is a condition of use of UNE's IT infrastructure that staff and students consent to allow IT or an authorised agency to perform an audit and any associated scans.

IT 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.

These scans will require access that may include:

- User level and/or system level access to any computing or communications device.
- Access to information (electronic, hardcopy, etc.) that may be produced transmitted or stored on UNE equipment or premises.
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on UNE networks.

Approval signature

Vice-Chancellor