Information Security - IT Security Audit Authorities Procedure

Section 1 - Purpose / Objectives

(1) Information Technology (IT) staff have the authority to conduct a security audit on any system at Victoria University (VU).

(2) IT security audits may be conducted on all computers and communication devices owned or operated by the University as well as any computer and communications devices that are present on the University premises, but may not be owned or operated by the University.

(3) IT Security audits may be conducted to:

a. Ensure integrity, confidentiality and availability of information and resources.
b. Investigate possible security incidents to ensure conformance to the University's security policies.
c. Investigate possible violations of laws applicable in the State of Victoria, the Commonwealth of Australia and any international jurisdiction in which Victoria University (VU) conducts operations.
d. Ensure the University complies with relevant legislation.
e. Monitor user or system activity where there is legitimate concern that one or more of the above conditions is not being met.
f. Ensure university resources are used for work related purposes.
g. Facilitate the recovery of corporate information stored on individual desktop PCs, Laptops etc.

(4) The following security audits may be conducted by an IT staff member:

a. Time of Essence Audit
b. Proactive Integrity Audit
c. Investigative Audit
d. Information Collation Audit
e. Telephony Audit

Section 2 - Scope / Application

(5) The scope of this Procedure:

a. This procedure applies to all VU staff involved in authorising and conducting IT security audits.
b. This procedure applies to all computers and communication devices owned or operated by the University as well as computers and communication devices that are present on the University premises, but may not be owned by the University.

Section 3 - Definitions

(6) Nil

Section 4 - Policy Statement

(7) Nil

Section 5 - Procedures

Roles/Responsibilities

Roles	Responsibility
ICT Security Manager	a. Inform IT staff involved in an audit of their responsibilities under the IT Security policy and associated procedures. b. Review IT Security Audit Authorities as part of a document review or as required. c. Maintain a record of all IT Security audits conducted.
Senior Management	a. Inform IT staff involved in an audit of their responsibilities under the IT Security policy and associated procedures. b. Provide authorisation for IT Security audits to be conducted as required.
IT Staff	a. Adhere to the ICT Security policy and associated procedures when conducting IT security audits.

Procedures

(8) Prior to conducting an audit, personnel performing the IT security audit must sign-off to confirm that they are aware of the relevant state, federal and international laws that may be pertinent to their investigation.

(9) Authorisation to conduct an IT security audit must be obtained as required according to the authority requirements for the type of security audit to be performed.

a. Authorisation to conduct an IT security audit can be obtained from:
    i. ICT Security Manager or delegate;
    ii. Senior Manager or delegate; or
    iii. Executive Director, IT Services or delegate.
b. Security audits that involve access to confidential material require an audit brief to be prepared for sign-off by the Executive Director, IT Services.
c. See References: IT Security Audit Types for the authority level required to conduct a security audit.

(10) Any access as required will be granted to authorised personnel for the purpose of performing an audit. This access 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 VU equipment or premises;
c. Access to work areas (labs, offices, cubicles, storage areas, etc.);
d. Access to interactively monitor and log traffic on VU networks.

(11) Conduct IT Security Audit according to the specific purpose of the type of audit. IT Security audit types:

a. Time of Essence Audit

b. Proactive Audit
c. Investigative Audit
d. Information Collation Audit
e. Telephony Audit

(12) See References: IT Security Audit Types for details on each of the IT security audits including a description, the purpose of the audit, inclusions and exclusion.

(13) A record of all audits will be maintained by the IT Security Office and made available, when required to a University Lawyer or Privacy Officer. If required, a final report detailing the outcome of the security audit is to be completed.

Section 6 - Guidelines

(14) Nil

Status and Details

Status	Historic
Effective Date	6th September 2014
Review Date	31st December 2018
Approval Authority	Vice-Chancellor
Approval Date	6th September 2014
Expiry Date	25th February 2020
Accountable Officer	Lisa Line Deputy Vice-Chancellor Enterprise and Digital Lisa.Line@vu.edu.au
Responsible Officer	Lisa Line Deputy Vice-Chancellor Enterprise and Digital Lisa.Line@vu.edu.au
Enquiries Contact	James Munro Associate Director, VU Cyber 0437216020