Information Security - IT Security Audit Authorities Procedure

Section 1 - Summary

(1) This Procedure ensures the integrity and stability of the University's computing and network environment, Information Technology (IT) will regularly conduct audits on systems at Victoria University.

Section 2 - Scope

(2) This Procedure applies to all staff, students, contractors, visitors and other authorised users of Information and Communication Technology (ICT) facilities and services.

(3) University-owned ICT computers and devices.

(4) Personal (BYOD) equipment and devices located on University premises.

Section 3 - Policy/Regulation

(5) See the Information Security Policy.

Section 4 - Procedures

Part A - Summary of Roles and Responsibilities

Roles	Responsibility
Director / Senior Manager	a. Inform IT staff involved in an audit of their responsibilities under the Information Security policy and associated procedures. b. Maintain a record of all IT Security audits conducted. c. Provide authorisation of IT Security audits to be conducted as required.
IT Staff	a. Adhere to the Information Security Policy and associated procedures when conducting IT security audits.

Procedures

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

(7) 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.

(8) 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 and procedures.
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 a legitimate concern that one or more of the above conditions is not being met.
f. Ensure university resources are used appropriately and for work-related purposes in accordance for work-related purposes in accordance with IT Appropriate Use and Appropriate Workplace Behaviour Policy and associated procedures.
g. Facilitate the recovery of corporate information stored on individual desktop PCs, Laptops or devices etc.

(9) Prior to conducting an audit, personnel performing the IT security audit must be aware of the relevant state, federal and international laws that may be pertinent to their investigation.

(10) 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. Director, ITS Security and Risk Assurance or delegate;
    ii. Deputy Vice-Chancellor Enterprise and Digital or delegate; or
b. Security audits that involve access to confidential material require an audit brief to be prepared for sign-off by the Chief Digital Officer and Executive Director Campus Services or delegate.

(11) 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 the traffic on VU networks.

(12) A record of all IT security 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 IT security audit is to be completed.

Section 5 - HESF/ASQA/ESOS Alignment

(13) HESF: 2.1 Facilities and Infrastructure, 3.3 Learning Resources and Support and 7.3 Information Management.

(14) Outcome Standards for NVR Registered Training Organisations 2025: Standard 1.8 Facilities, Equipment and Resources; 4.3 Risk Management.

Section 6 - Definitions

(15) Nil.

Status and Details

Status	Current
Effective Date	25th February 2020
Review Date	4th September 2026
Approval Authority	Vice-President, Resources and Precincts
Approval Date	10th February 2020
Expiry Date	Not Applicable
Accountable Officer	Lisa Line Deputy Vice-Chancellor Enterprise and Digital Lisa.Line@vu.edu.au
Responsible Officer	Stuart Hildyard Chief Digital Officer and Executive Director Campus Services +61 3 9919 5576
Enquiries Contact	James Munro Associate Director, VU Cyber 0437216020 Information Technology Services