Information Security - Security Access to Controlled IT Areas Procedure

Section 1 - Purpose / Objectives

(1) This procedure specifies appropriate physical security measures to be used to protect computer systems, personnel, and data and communications systems located in secure locations. Access to such areas must be restricted to those who have an approved need to be there.

(2) All critical and sensitive information handling activities must take place in areas that are physically secured and protected against unauthorised access, interference, damage and to minimise equipment theft.

(3) Servers, routers, switches, PABX and related hardware, shall be located in a room with appropriate levels of access control. Monitoring of access and removal of equipment is a requirement, as other security controls (e.g. passwords) can be bypassed if physical security is not maintained.

Section 2 - Scope / Application

(4) The scope of this Procedure:

a. This procedure applies to all VU staff, contractors and visitors authorised to access Controlled Areas at VU.
b. This procedure specifies levels of access and monitoring to protect servers, routers, switches and other related hardware, including data and software stored on these devices, located in Controlled Areas.

Section 3 - Definitions

(5) Nil

Section 4 - Policy Statement

(6) Nil

Section 5 - Procedures

Roles/Responsibilities

Roles	Responsibility
Information Technology Services	- Maintain a register of authorised equipment installed or removed from controlled areas. - Maintain a register of authorised visitors to controlled areas. Provide training and induction programs for individuals authorised to access controlled areas. - Maintain a register/log of persons approved to access controlled areas. - Provide authorization for the relocation or removal of equipment from controlled areas.
Infrastructure Services Manager	- Ensure IT Security policies and procedures are followed for access to Data Centres.
Communications Infrastructure Manager	- Ensure IT Security policies and procedures are followed for access to Communication Rooms.
Staff entering secure areas	- Comply with all VU policies and procedures regarding the handling of information at all times. - Never permit an unauthorised person to enter the facility in their company.
ITS Contractors	- Complete appropriate induction and training programs. - Carry work orders (or similar) indicating the area of the University that they are working in and any related OHS risks and responsibilities. - Wear ID at all times.

Procedures

(7) A controlled area at VU is:

a. Primary computer rooms (Data Centre) currently located at Footscray Park, Building D and Sunshine, Whitten Building;
b. Communication closets (Comms Rooms) housing central network equipment located within all buildings of the University.

(8) Security Access to Controlled Areas in IT Procedures:

a. Physical access to a controlled area containing critical computing equipment must be:
    i. Restricted to University staff and authorised visitors who need access as part of their job function;
    ii. Authorised by the relevant manager;
    iii. Enforced through physical security barriers and electronic security techniques;
    iv. Recorded in an on-going security access log, capturing details of time, date and identity of staff member/visitor.
b. Authorised visitors who require access to a controlled area as part of a specific job function, such as vendor maintenance, must:
    i. Complete an appropriate induction and training program, unless exempted by the Executive Director, IT Services or nominee;
    ii. Be escorted in the Controlled Area at all times. Where it is inappropriate for an on-going escort, for example for extended periods of time, this will be recorded in the access log and signed by the relevant manager;
    iii. Be authorised by the Executive Director, IT Services or nominee;
    iv. Be recorded in an on-going security access log, capturing details of time, data, identity, escorting staff member and reason for the visit;
    v. Carry a work order (or similar) that indicates the area of the University and ITS Controlled Area that the work is to be performed in as well as any related OHS risks and responsibilities;
    vi. Wear approved identification at all times.
c. The relevant manager, or delegate, will keep a register/log of those approved to access the controlled area.

This register will be reviewed every 12 months to ensure access to the controlled area is relevant and appropriate for each listed staff member.

d. ITS will ensure any contractors accessing ITS Controlled Areas have sufficient insurance for the potential loss of VU equipment under their care and custody.
e. Outside normal working hours physical access to controlled areas must be:
    i. For scheduled access, request through the Facilities Service Desk a minimum 48 hours prior to access requirement;
    ii. For unscheduled access, request through the Security Control room (9919 4999), quoting the following security code: Access2013;
    iii. Via electronic fob access or key pads.
f. No equipment is to be relocated or removed from the controlled areas without explicit permission of the relevant manager, or delegate.
g. Authorised equipment being installed in or removed from a controlled area will be recorded in a register.
h. Registers for controlled areas shall be maintained so that they can be audited as required.
i. IT staff must have clear passage to all controlled areas at all times.
j. Controlled areas will not be used for storage or any purpose other than that approved by IT.

Section 6 - Guidelines

(9) Nil

Status and Details

Status	Historic
Effective Date	12th August 2015
Review Date	16th August 2019
Approval Authority	Vice-Chancellor
Approval Date	28th July 2015
Expiry Date	26th 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 Information Technology Services