IT Security - Device Security Guidelines

Section 1 - Purpose / Objectives

(1) A robust and trustworthy set of procedures governing the operation of servers is therefore critical to the University as compromised machines may lead to loss of sensitive information, provide openings for unauthorised access to other applications, interfere with normal University IT services and generate adverse publicity.

(2) The purpose of the device security procedure is to establish security standards for the base configuration of equipment that is owned and/or operated by Victoria University. Effective implementation of this policy will minimise unauthorised access to Victoria University proprietary information and technology, and therefore protect the business information assets of the University.

Section 2 - Scope / Application

(3) This Guideline applies to:

a. Computer servers host applications, information, raw data, teaching materials, records and various infrastructure services on behalf of the University.
b. All equipment owned and/or operated by Victoria University, and to devices registered under any Victoria University-owned internal network domain.

Section 3 - Definitions

(4) Nil

Section 4 - Policy Statement

(5) Nil

Section 5 - Procedures

(6) Nil

Section 6 - Guidelines

(7) All devices deployed should be compliant with the IT Security Policy .

(8) Configuration changes for production equipment must follow change and release management policies and procedures as appropriate.

(9) Where supported by the Operating System and/or application an appropriate warning banner must be displayed prior to an authentication attempt.

(10) Devices subject to Change Management Data Base (CMDB) inclusion must be compliant with the applicable policies.

(11) Support groups will be responsible for the following:

a. Ensure documentation for equipment and services is maintained and recorded. At a minimum, the following information is required:
    i. Host contacts and location.
    ii. System specifications and operating system/version.
    iii. Main functions and applications.
    iv. Network Services delivered and consumed.
    v. Firewall requirements (for both network and host based firewalls).
b. Passwords must be maintained in accordance with the corporate wide password management system/process.
c. Immediate access to equipment and system logs must be granted to members of ITS upon demand, per the Audit Policy

Server

(12) Operating System and application configuration should be in accordance with best practice guidelines as advised by vendors and the Centre for Internet Security [cisecurity.org].

(13) Services and applications that will not be used must preferably be removed or disabled where practical.

(14) Access to services should be logged and/or protected through access-control methods such as host based firewalls and/or TCP wrappers if possible.

(15) The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

(16) Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.

(17) Always use standard security principles of least required access to perform a function.

(18) Do not use super-user accounts when a non-privileged account will do.

(19) If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

(20) Servers should be physically located in an access-controlled environment as approved by the Infrastructure Services Manager as specified in the Security Access to Controlled IT Areas Procedure .

(21) Servers are specifically prohibited from operating from uncontrolled public areas.

Workstations (including laptops)

(22) Workstations, including laptops, should have appropriate physical and technical safeguards implemented as appropriate for the purpose they are used, such as:

a. Operating systems and application configuration should be in accordance with best practice guidelines as

advised by vendors and the Centre for Internet Security [cisecurity.org].

b. The standard Victoria University SOE must be used on all workstations.
c. Patches and updates must be deployed as soon as possible.
d. All applicable Victoria university policies and procedures will be complied with.
e. Workstations (including laptops) must always be physically secure. Laptops that contain sensitive information should be secured by using cable locks or locked in drawers or cabinets.
f. The loss or theft of any workstation (including laptops) must be reported immediately including a summary of any sensitive information that may have been on the workstation.

PDA/Smart Phone/Mobile Phone/Portable Storage Devices

(23) Any sensitive University data stored on a PDA, Smart Phone, Mobile Phone or Portable Storage device must be saved to an encrypted file system using Victoria University approved software. Due to the reliability of these devices, sensitive University data should only be stored for a short time only.

(24) IPods and MP3 players should not be used to handle data due to poor data storage capacities.

(25) The loss or theft of any mobile device containing University data must be reported immediately to Mobility Servicedesk and relevant line manager with a summary of any sensitive information that may have been on the device.

(26) Device configuration should be in accordance with best practice guidelines as advised by vendors.

Other devices such as Printers, Copiers and Faxes

(27) Devices must be configured with an appropriate level of security that is suitable for the most sensitive information the device is expected to process.

(28) Both physical and technology solutions should be employed where appropriate.

Network Equipment

(29) No local user accounts are configured on the device. Central authentication services must be used.

(30) The enable password on the device must be kept in a secure encrypted form.

(31) Disallow the following by default:

a. IP directed broadcasts
b. Incoming packets at the router sourced with invalid addresses such as RFC1918 addresses from external sources
c. TCP small services
d. UDP small services
e. All source routing
f. All web services running on router

(32) Use corporate standardized SNMP community strings.

(33) Access rules are to be added as business needs arise.

(34) Telnet must never be used across any network to manage a network device where a more secure alternative exists. SSH is the preferred management protocol.

Monitoring

(35) All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

a. All security related logs will be kept online for a minimum of 1 week.
b. Daily incremental tape backups will be retained for at least 1 month.
c. Weekly full tape backups of logs will be retained for at least 1 month.
d. Monthly full backups will be retained for a minimum of 2 years.
e. A copy of all events should be sent to the central log services in real time to ensure compliance.

(36) Security-related events will be reported to the ITS Security Office, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

a. Port-scan attacks.
b. Evidence of unauthorized access to privileged accounts.
c. Anomalous occurrences that are not related to specific applications on the host.

Access control equipment and services

(37) Access control services should be configured for default deny where possible.

(38) Rules should be as succinct as possible to allow for normal business operation.

(39) Always use standard security principles of least required access.

Network Zones

(40) Devices should be deployed into the most appropriate network zone (where applicable) and conform to the rules and regulations of that zone.

Status and Details

Status	Historic
Effective Date	27th October 2015
Review Date	31st May 2019
Approval Authority	Vice-Chancellor
Approval Date	16th October 2015
Expiry Date	18th December 2019
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	Information Technology Services