Information Security - Virus Protection Procedure and Guidelines

Section 1 - Purpose / Objectives

(1) List the application of the procedure to university policy and the policy purposes/objectives.

(2) This purpose of the Virus Protection Procedure and Guidelines is to ensure the effective and efficient prevention, containment or minimisation of damage to the organisation from computer viruses.

(3) The Virus Protection Procedure and Guidelines supports the IT Appropriate Use Policy and the Information Security Policy .

Section 2 - Scope / Application

(4) This procedure applies to:

a. Identify who the procedure applies to, specifying any exclusions.
b. All VU staff, students, contractors, visitors and other authorised users connecting to the University network.
c. Identify what the procedure applies to, specifying any exclusions
d. All networked or standalone devices, susceptible to contamination that is under ITS control. This includes but is not limited to Desktop PC's, Laptops, Mobile devices and any other device capable of storage data.
e. Devices not under ITS control are covered to the extent of preventing them from causing damage to the rest of the University.

Section 3 - Definitions

(5) Virus: A computer program that is designed to replicate itself by copying itself into the other programs stored in a computer. It may be benign or have a negative effect, such as causing a program to operate incorrectly or corrupting a computer's memory.

Section 4 - Policy Statement

(6) Nil

Section 5 - Procedures

Part A - Roles/Responsibilities

Roles	Responsibility
ITS	ITS is responsible for providing informed advice and protection. This protection is limited to the means available from antivirus companies. ITS is responsible for updating virus protection on PCs that are directly under its control. For example, open access computer laboratories.
VU Staff, Students, other Users	Individual members of the University community are responsible for using antivirus software to maintain a safe and predictable working environment.

Part B - Procedures

Antivirus Software

(7) Antivirus software is provided to the University community to protect against the damage caused by virus attacks.

(8) Antivirus software is available for Staff and Students of VU to download and run on their home PC/Laptop to protect their data and minimise the risk of spreading viruses to the University network.

(9) Any person wishing to connect a PC or laptop to the University network, does so on the understanding that the device must be equipped at all times with the latest antivirus software in accordance with the IT Appropriate Use Policy .

(10) Anti-virus protection is the responsibility of the owner of the PC or laptop and this responsibility is then delegated to whoever is performing the desktop support function:

a. Individual owners and/or users of home-based PC's and laptops are responsible for ensuring adequate anti-virus protection.
b. ITS is responsible for ensuring anti-virus protection for PCs that are directly under its control. Example, Open Access Computer Laboratories.

Virus Protection Procedures

Network:

(11) ITS will respond to any detected, likely or imminent attack to the University network as it sees appropriate in accordance with the Information Security Policy .

(12) If an attack is likely or imminent, ITS may isolate the University network from the rest of the Internet if no other protection is available.

(13) If the network has been infected, ITS may isolate the contaminated portion of the University network from the rest of the University.

Device:

(14) A PC, laptop or other device that has been infected will be disconnected from the University network.

(15) The infected device will need to be cleaned and cleared of any threat to the University network.

(16) The device may be required to be presented for inspection by ITS before reconnection to the University network is permitted.

(17) Members of the University community are required to abide by the Desktop Virus Protection Guidelines to reduce the risk of virus problems.

File:

(18) If an infection to a file occurs, the following steps apply:

a. If a file can be cleaned, it is cleaned.
b. If it can't be cleaned, and the file is recoverable from backup, it is deleted.
c. If it can't be cleaned, and the file is not recoverable from backup, it is quarantined off the network.

(19) In exceptional circumstances, where the file holds great importance, it can be sent to an antivirus company at the file owner's expense for possible (but not guaranteed) de-contamination and recovery.

Section 6 - Guidelines

Antivirus

(20) Most viruses are spread through an external source. Some common examples include email messages with attachments and Internet downloads.

(21) There are three main protection mechanisms in place:

a. Antivirus mail gateway.
b. Antivirus workstation protection.
c. Antivirus server based protection.

(22) The antivirus mail gateway prevents inbound and outbound virus infected emails from spreading.

(23) The antivirus workstation protection updates network attached PCs with the most recent release of antivirus software. Currently, the distribution process is automated and runs transparently in the background. Home-based users can download and install the latest antivirus software from University Intranet site .

Desktop Virus Protection Guidelines

(24) Recommended actions to prevent virus problems:

a. Always run the University standard, supported anti-virus software available from the University download site. Download and run the current version; download and install anti-virus software updates as they become available. This is installed and updates are deployed over the network on University PCs, however users must install and update at home.
b. NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
c. Delete spam, chain, and other junk email without forwarding.
d. Never download files from unknown or suspicious sources.
e. Never provide your personal information to anyone by email , e.g. date of birth, password (Requests for this type of information is known as Phishing).
f. Avoid clicking on unknown internet sites (URLs) that are received from unknown sources via emails as by connecting to these sites you may be infected by a Trojan.
g. Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
h. Always scan a CD, DVD, USB stick or external hard drive from an unknown source for viruses before using it.
i. Back-up critical data and system configurations on a regular basis to a network drive or, if using portable media, store the data in a safe place.

j. If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

k. New viruses are discovered almost every day. Periodically check that your anti-virus software and definition files are up-to-date.

Status and Details

Status	Historic
Effective Date	22nd April 2015
Review Date	31st May 2019
Approval Authority	Vice-Chancellor
Approval Date	10th April 2015
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