Information Security - Virus Protection Procedure

Section 1 - Summary

(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 - HESF/ASQA/ESOS Alignment

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

Section 3 - Scope

(5) 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 4 - Definitions

(6) 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 5 - Policy/Regulation

(7) Nil.

Section 6 - Procedures

Part A - Summary of Roles and 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

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

(9) 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.

(10) 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.

(11) 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:

(12) 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.

(13) 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.

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

Device:

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

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

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

permitted.

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 7 - Supporting Documents and Information

(20) Antivirus Software.

Status and Details

Status	Current
Effective Date	26th February 2020
Review Date	1st October 2023
Approval Authority	Vice-President, Resources and Precincts
Approval Date	11th 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 9919 5576
Enquiries Contact	James Munro Associate Director, VU Cyber 0437216020 Information Technology Services