Information Security - Internet Filtering Procedure

Section 1 - Summary

(1) The purpose of this Procedure is to:

a. Ensure that all University use of the Internet is legal, and complies with University values and policies.
b. Ensure staff and students have access to web sites and Internet services legitimately needed for their University work.

(2) The Internet Filtering Procedure and Guidelines supports the IT Appropriate Use Policy and the Information Security Policy.

Section 2 - HESF/ASQA/ESOS Alignment

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

Section 3 - Scope

(4) This Procedure applies to:

a. All VU staff, students, contractors, visitors and other authorised users of ICT facilities and services.
b. All authorised users connecting to ICT services from either personal (BYOD) of VU owned facilities.

Section 4 - Definitions

(5) Spyware: Programs which can collect many different types of information about a user. More benign programs can attempt to track what types of websites a user visits and send this information to an advertisement agency. More malicious versions can try to record what a user types to try to intercept passwords or credit card numbers. Yet other versions simply launch popups with advertisements.

(6) Web filtering: A term for content-filtering software, especially when it is used to filter content delivered over the internet. Content filtering software determines what content will be available on a particular machine or network; the motive is often to protect children or to prevent employees from viewing non-work-related sites.

Section 5 - Policy/Regulation

(7) See Internet Security Policy.

Section 6 - Procedures

Part A - Summary of Roles and Responsibilities

Roles	Responsibilities
Chief Digital Officer and Executive Director Campus Services	Power to grant exclusions to web filtering. Power to approve the blocking of sites believed to be in contravention of legislation or University policies and values. Power to resolve disputes regarding the classification, blocking or unblocking of internet categories.

Part B - Internet Filtering

(8) The internet has become an essential tool in education and research, however, some information and sites on the internet condone or promote matters which are illegal in Australia or directly contravene VU values, standards and policies.

(9) VU ICT facilities and services must be used in accordance with the IT Appropriate Use Policy and Appropriate Workplace Behaviour Policy.

(10) Internet Filtering can reduce the risk to the University from those who practise antisocial behaviour like creating viruses, distributing spyware, attempting to break into computer networks and sending unsolicited commercial emails.

(11) VU subscribes to a Web Content Filtering service. This service has been employed to block access to Internet sites with particular categories of content as well as sites which may threaten University security. See IT Security - Internet Filtering Appendix.

(12) Filtering can also be used as an economic tool to save expense to cost-centre managers. For example, a computer lab may be filtered to provide only intranet services.

(13) Due to copyright concerns all networks which enable the sharing of content files containing audio, video, data or anything in digital format from one client machine to another will be blocked (peer-to-peer, P2P).

Part C - Exclusion from Web Filtering

(14) VU staff and students may have a need to be excluded (in part or in whole) from web filtering if their University work, studies or research requires access to these sites in accordance with the IT Appropriate Use Policy. This will be handled on a case by case basis.

(15) Requests for exclusion from web filtering will require the approval of:

a. The head of the relevant organisational unit, and
b. The Chief Digital Officer and Executive Director Campus Services or delegate.

(16) If the request is approved, specific machines will be granted an exemption as the existing blocking system is IP address-based, not user-based.

Part D - Additional Web Blocks

(17) VU staff and students may request the blocking of sites they have good reason to believe are in contravention of legislation or University policies and values.

(18) Blocking of these sites will require the approval of the Chief Digital Officer and Executive Director Campus Services or delegate.

(19) Some cost-centre managers may need to impose further restrictions on computers they are responsible for. This could range from additional website categories through to additional services.

Part E - Web Filter Categorisation Review

(20) VU staff and students may request a review of the classification of a website for web filtering purposes.

(21) In the event that a website has been misclassified, ITS will submit the request to the Web Content Filtering Service for review and notify the staff member or student of the outcome.

(22) If the website has been correctly classified or the Web Content Filtering Service declines to re-categorise the website, the request can be referred to the Chief Digital Officer and Executive Director Campus Services or delegate for a decision to approve the creation of a local override.

(23) Requests for the review of the classification of a website can be submitted using the online form via the IT service desk system.

Part F - Internet Filtering Disputes

(24) If there is any dispute regarding the classification, blocking or unblocking of internet categories the Chief Digital Officer and Executive Director Campus Services will be the final arbitrator.

Section 7 - Supporting Documents and Information

(25) See Content Filtering Security Standard.

(26) See IT Security - Internet Filtering Appendix.

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 +61 3 9919 5576
Enquiries Contact	James Munro Associate Director, VU Cyber 0437216020 Information Technology Services