Information Security - Internet Filtering Procedure

Section 1 - Purpose / Objectives

(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 - Scope / Application

(3) This procedure applies to:

a. All VU Staff, Students and other authorised users using VU Internet Access.
b. Access to websites and Internet services using VU ICT facilities and services.

Section 3 - Definitions

(4) 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.

(5) 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 4 - Policy Statement

(6) Nil

Section 5 - Procedures

Part A - Internet Filtering

(7) 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.

(8) The IT Appropriate Use Policy states that VU ICT facilities and services must not be used by staff and students:

a. For the purpose of creating, accessing or transmitting or otherwise dealing with content which may reasonably be regarded as objectionable or offensive (bearing in mind the cultural diversity of the environment in which the University operates), or
b. In a manner which is contrary to other University policies; or
c. In a manner which may otherwise expose the University to legal liability.

(9) Some examples of activities prohibited by the above restriction include (but are not limited to) activities which relate to:

a. content which would be reasonably regarded as pornographic;
b. content which contains racial vilification, cruelty or violence;
c. content which is defamatory;
d. content which is illegal; or,
e. content which breaches copyright.

(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 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 B - 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 Director of ITS Operations.

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

Part C - 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 Director of IT Operations.

(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 D - Web Filter Categorisaton 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 referred to the Director of ITS for a decision to approve the creation of a local override.

Part E - Internet Filtering Disputes

(23) If there is any dispute regarding the classification, blocking or unblocking of internet categories the Director, IT Operations will be the final arbitrator.

Part F - Internet Filtering Forms

(24) Web Filter Categorisation Review Request

(25) Internet Filtering Expansion Request (Additional Blocks form)

(26) Web Filter Exemption Request Form

Section 6 - Guidelines

(27) Nil

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