Massey University Policy Guide

ENDPOINT SECURITY POLICY

Section	Information Technology Services
Contact	Chief Information Officer
Last Review	April 2016
Next Review	April 2017
Approval	SLT 16/04/72
Effective Date	16 May 2016

Purpose:

The purpose of this policy is to regulate protection of the Massey University network when accessed by "Endpoint" equipment (e.g. such as desktop computers, laptops, tablets, mobile devices or similar).

The objective is to reduce the risk of security breaches that could result from the connection and use of Endpoint devices. This policy seeks to limit security threats by:

- Ensuring staff are aware of the requirements and restrictions around Endpoint devices.
- Enabling protective measures and controls to manage Endpoint security and software compliance risks.

Audience:

All University staff or anyone performing work on behalf of the University (including contractors, consultants and volunteers) are subject to this policy.

Scope:

This policy covers all Endpoint devices connected to the internal Massey University network environment.

Policy:

The Audience is responsible for ensuring that:

Information Security

- All care is taken to prevent unintended exposure, modification, or removal of private, copyright, or confidential information as a result of leaving this information on the screen or desk, or exposed in such a way that it can be viewed or accessed by an unauthorised individual. This includes information stored on portable storage media or hard copy.
- Any private, sensitive, or confidential information that is stored on such an Endpoint device has the appropriate security controls to restrict and prevent retrieval or intercept by an unauthorised third-party.
- Business information and work is stored in such a way as to enable an authorised back-up service to store and protect the information.

Endpoint Software

All software contains security vulnerabilities, and software vendors are constantly supplying updates (patches) to address these vulnerabilities when they are identified.

- Endpoint software Operating Systems (OS) and application software are to be kept up to date with the latest security related patches, as soon as it is practical to do so, i.e.:

  - Critical security patches are applied within 1 week of them being released by vendors.
  - Important security patches are applied within 8 weeks of them being release by vendors.
  - Endpoint systems must be restarted following installation, to ensure security patches have been fully installed.
  - Where possible, it is recommended that Endpoint devices are set to auto-update their security patch levels, and restart if necessary to complete the installation.
- OSs that reach end of support life are by default not permitted to connect to the University network. This is because security patches are no longer provided by vendors and this poses a growing security threat to the environment over time. If a special exemption is required, this must be requested formally via the ITS Service Desk (refer below for contact details) and approved by the CIO.
- ITS will install Endpoint device management software, as required, on any Endpoint connected to the Massey network in order to manage Massey University policy, legal, and commercial compliance requirements.
- The removing or disabling of Endpoint device management software without prior approval of ITS is considered a breach of this policy.
- ITS will audit Massey owned Endpoint devices on the Massey Domain as required, and has the ability to install updates to software on these devices to address software vulnerabilities or licensing issues with ITS managed software.
- Departments who choose to operate and manage their own specific software on Endpoint devices accept responsibility for the associated licensing, installation, updates, and security as it relates this software, in accordance with this policy.

Administrative Access

- In accordance with the principle of least privilege, unnecessary administrative access on Massey owned Endpoint devices will be restricted.

Authentication

- Endpoint devices containing Massey information assets that are not publicly available, or devices which attach to Massey's network, must be secured as appropriate by a network or locally based user code and password or a PIN.

Antivirus Software & Firewalls

- All Endpoint devices capable of running an antivirus software program are required to do so before being connecting to the Massey internal network. Additionally, any such antivirus software must be running the latest virus definitions to accurately detect the latest viruses and malware, and be set to automatically update when newer definitions become available.
- Disabling or removing of Antivirus software, or disabling of Antivirus software definition updates on endpoints is prohibited.
- All Endpoint devices capable of running local Firewall software are required to do so to protect the device from external threats such as hacking by unauthorised parties.

Servers & Web Applications

- All Servers (or devices exposed to the internet, in the DMZ, or running web services), will be 'hardened', meaning they will have all the necessary security updates applied to their Operating System's, hardware patches (firmware updates), and installed software; to reduce the chances of vulnerabilities being exploited. All such updates must be reviewed and maintained regularly to ensure they remain up to date. It is the Server Administrator's responsibility to manage this.
- New Services that are externally (internet) facing will require independent security vulnerability and penetration testing to be performed by a security specialist prior to implementation, and subsequently added to the IT Security Review Schedule, to provide assurance that data or services won't be exposed to medium or high risk security threats.

Network Segmentation

- Endpoint devices will be attached to Massey's network within the appropriate network segment as determined by applicable Endpoint security controls.

Personal devices

- Personal devices (i.e. those not purchased or owned by Massey University) that are authorised to connect to the Massey University network remain the responsibility of the owner, and must comply with this policy.

Information Technology Services (ITS) Security Services

ITS will:

- Provide support and advice on this policy via the ITS Service Desk, by phone on 06-356-9099 ext. 82111, or via http://AskIT.massey.ac.nz
- Maintain and manage the University's security infrastructure, such as firewalls, and implement intrusion detection and prevention practices in order to limit threats and provide early detection of security breaches where possible.
- Provide anti-spam and anti-virus protection on endpoints they are directly responsible for, and ensure these are kept up to date.
- Work with departments on the security principle of "least privilege" in order to manage the security model for both user and endpoint devices.
- Manage the accounts and user code policies and technology necessary to manage device and user authentication, as well as install any necessary controls required to manage Endpoint devices that connect to the network.
- Monitor endpoint device connectivity and activity as it relates to managing and protecting the University network.
- Disconnect, isolate, or restrict, any endpoint device without notice that is identified to pose a threat or is impacting the confidentiality, integrity, or availability of the Massey network.
- Manage the IT infrastructure network Internet Protocol (IP) numbering and network segmentation scheme to administer and isolate the environment, and apply necessary protective controls to manage endpoints as securely as possible.
- Apply any required security or encryption standards necessary to protect endpoints that are identified as storing sensitive or confidential institutional data.
- Apply security updates as per this policy for Endpoint devices, on-behalf of the University.

Endpoint device policy exemptions

- Requests for exemptions to this policy must be formally requested via the ITS Service Desk (contact details above) with the business reasons.
- Any exemptions to this policy will be conditional on the department involved accepting responsibility for maintaining adequate security and licensing controls. Exemption may also be conditional upon limiting network access and risk acceptance sign-off.
- Any exemption approved does not preclude ITS from disconnecting or isolating such devices if they are shown to be causing harm to the confidentiality, availability or integrity of Massey University Information Security.

Definitions:

Endpoint	An electronic device connected to the IT infrastructure that generates or terminates an electronic information stream. These could be computers, servers, tablets, mobile devices, or any similar network enabled device.

Hard copy	A physical copy of a document, record, or information. For example, a facsimile, photocopy, handwritten form, or printed document.
Malware	Programming code, scripts, active content, and other software designed to disrupt, collect private information, or gain unauthorised access to system resources.
Firewall	An application running on a device designed to protect and control network traffic to and from the device.
Massey Internal Network	The Massey University corporate internal computer network accessible by authorised staff, which is segmented and protected from the internet and other less trusted zones.
Network segmentation	Massey's computer network is segmented into areas based on zones of trust. Placement in and access between devices located within these segments are based on the sensitivity of information assets within those segments and, and the applicable security controls on the devices in those segments. Sensitive or confidential information will be placed within the more secure network segments, and endpoints must meet stricter requirements to have access to the services within these sensitive zones.
VPN	Or Virtual Private Network is a secure and encrypted connection between a remote client device and the internal Massey network. It acts to secure data transmitted over a typically insecure network (such as the internet) to a corporate (private) network.
DMZ	DMZ or demilitarized zone is a physical or logical Firewalled network that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. It provides an additional layer of separation between the Internet and the Massey internal network, thereby adding an extra layer of protection.
ITS Managed Software	Software that is under the jurisdiction of Massey University Information Technology Services (ITS) as national shared service provider. This includes Massey-wide 'standard' software, for example: Windows and Macintosh computer fleet software such as operating systems , office suite software, communications software, web browsers, standard plug-ins (extension/feature software), and business application software that is centrally managed by ITS.
Least Privilege	In information security, this principle requires that in a particular layer of a computing environment, every module (such as a process, a user, a device, or a program depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose (e.g. to perform their role, while at the same time not impacting on academic freedom).
Endpoint device management software	Refers to the necessary management software required to audit and review application software versions and license numbers, and manage software installations (where required) on an Endpoint device. This includes Microsoft System Centre Configuration Manager, Casper, and Active Directory services. Refer to the Active Directory Domain Policy for more information.

Relevant Legislation:
Privacy Act, 1993.
Copyright Act, 1994.

Legal compliance:
- Privacy Act, 1993.
  Establishes a set of privacy principles to ensure the protection of personal privacy in respect of both public and private sector organisations. The Act is of prime importance and should be clearly understood by all information management professionals.

- Copyright Act, 1994.
  Contains references to the requirements for documenting copyright in original works, transferring copyright and licensing for use/copying. This includes ownership of published works in audio/visual, or electronic form.

Related policy and procedure compliance:
Desktop Hardware and Software Policy
Telecommunications Policy
Data Network Policy
Internet Use and Digital Communications Policy
User Code and Password Policy

Related procedures / documents:
ISO/IEC 27000:2014 – Information technology – Information security management systems
Risk Management @ Massey University.

Document Management Control:
Prepared by: Information Technology Services
Authorised by: The Chief Information Officer
Approved by:
Date issued: 15th July 2015
Last review: Month and year
Next review: Month and year