ELECTRONIC INFORMATION ACCESS CONTROL POLICY

Section	Information Technology Services
Contact	Chief Information Officer
Last Review	August 2016
Next Review	August 2019
Approval	SLT 16/08/162
Effective Date	August 2016

Purpose:

The purpose of this policy is to establish and operate effective access control methods across IT Systems, to reflect and mitigate the associated information security risks.

The objective being to limit and manage access to data and information processing facilities based on business information security needs. It is intended that this policy be read in conjunction with the Data Management Policy.

Audience:

All users of the University's IT Systems.

Scope:

This policy covers Massey University institutional data and information assets, as well as related information systems used to store, access, or transmit such data.

Policy:

- Service Owners will ensure that:
  - Information Security requirements for IT Systems are documented and formally accepted, and comply with this policy, and the Data Management policy.
  - Information that is stored electronically is classified and managed consistently across all information systems, based on the Massey University Privacy Management Framework (refer to Privacy @ Massey University).
  - All software and websites that require authentication, and/or access data not classified as Public, will require a high level of encryption to be implemented before being made accessible over the Internet.
  - A minimum of two-factor authentication is required for data not classified as Public, unless the risk to the University of such Data being exposed or lost is deemed as low. This excludes data that is only accessible via the internal Massey network (i.e. from a staff computer on site, or over VPN).
  - Applying a principle of least privilege, access must be explicitly requested and approved in order to access non-public facing information assets. Personal, sensitive, and confidential information will have access controls applied accordingly.
  - Management of access rights is applied in such a way as to enable a high-level of quality and security assurance. This means that clear segregation of access control duties are applied for those individuals requesting, authorising, and administering access.
  - Credit card information will not be stored or processed by internal Massey University systems. Due to the high costs of complying with Payment Card Industry (PCI) standards, PCI accredited third-party payment services will be used to fulfil such requirements.

- IT System Controllers will ensure that:
  - The process and requirements for formal access authorisation is documented and used.
  - The process for removal of access rights is documented and used.
  - Access to sensitive or personal information is periodically reviewed.
  - Audit logging of all significant events concerning the use and management of user identities and access control is enabled, and archival of these events is managed in such a way as to keep these logs for a period of seven years for financial management systems, or a minimum of 1 year for non-financial systems.
  - User and device identity and password policies will utilise the appropriate Massey University enterprise Lightweight Directory and Access Protocol (LDAP) where ever possible.
- IT System users will ensure that:
  - If they identify or suspect that they may have inappropriate access to private or sensitive information they will advise their manager immediately.
  - Incidents (issues) related to information security that occur will be reported immediately to the ITS Service Desk by phone on 06-356-9099, ext. 82111.
- ITS will:
  - Provide information security incident response to IT Systems users, Controllers, and Service Owners.
  - Provide advice and information on IT security policies and standards.
  - Support Service Owners and Controllers by providing information security risk assessments and treatment options.

Definitions:

Controller	Any person or organisational role responsible for the technical management of an IT System; this could include the delegated IT System administrator or the relevant Head of Department.
Encryption	Encryption is the process of encoding messages or information in such a way that only authorised parties can read it. For websites, Secure Sockets Layer (SSL) is a standard technology established to perform this encryption between the webserver and the client. *For information on the correct SSL standard required, please contact the ITS Service Desk.*
Information Security	Directly relates to providing for the confidentiality, integrity and availability of all digital resources within Massey University. This provides assurance that information is only accessible by those who are authorised to view it, records and data are valid and correct, and mission critical information is accessible when it is needed.
IT System	Refers to an information technology or communication system used to deliver a business service (such as email), including its computing equipment, business applications, audio visual, data network, telecommunication and other communications systems, storage media and peripheral devices.
Lightweight Directory and Access Protocol (LDAP)	It is a standard technology for network directories. Network directories are specialised databases that store information about devices, applications, people and other aspects of a computer network.. It is a network protocol, with support for encryption that is used to access a hierarchical directory of information on a directory server.
Principle of least privilege	Means giving a user account only those privileges which are essential to that user's work. The principle is also applied to technology elements of information system as "No part of a system will have a higher level of access to other parts of that system than are required, to perform its legitimate function." This protects both the user and the integrity of a system, as well as provides the mechanism for

	authorisation and accountability in an information system.
Public Facing Information assets	Information, or an information system, that is designed to be accessible and readable by anyone (e.g. an e-commerce or informational website). A staff intranet is considered a non-public facing information asset as the intent is for only current staff to view information on it.
Payment Card Industry (PCI) compliance	PCI compliance is adherence to a set of specific security standards that were developed to protect bank and credit card information during and after a financial transaction. PCI compliance is required by all card brands. Failure to comply can result in significant fines, loss of merchant status, and damage to reputational brand.
PCI accredited third-party services	A service provider (vendor) who provides electronic credit card and banking transaction and processing services, and is responsible for ensuring the services they provide protect the confidentiality, integrity and availability of credit card and personal information. These providers are also responsible for ensuring they remain PCI compliant.
Service Owner	Refers to the business owner of a particular IT Service. This is usually a senior manager and financial sponsor of an information system who has a level of accountability and/or responsibility around decision making as it applies to a particular information system. This reflects the line management and delegated responsibility applied to a role by the University.
Security Policies	Refers to information security policies accepted by the University's Information Security Governing Body.
Two factor authentication	Is an extra layer of security that is known as "multi factor authentication" that requires not only a password and username but also something that only that user has on them, i.e. a piece of information, an extra security feature (such as a Virtual Private Network client) known or physically carried only by the authorised user.

Audience:
All staff

Relevant Legislation:
Privacy Act 1993
Electronic Transactions Act 2002

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.
- Electronic Transactions Act 2002
  This act addresses the legal implication and requirements for the use of electronic information and media.

Related policy and procedure compliance:
Information Security Policy
Privacy Policy
Data Management Policy
Records Management Policy
Usercode and Password Policy
Active Directory Domain Policy
Data Network Policy

Related procedures / documents:

ISO/IEC 27002:2013 – Information technology – Code of practice for information security controls
Massey University Information Security Manual
Information Security @ Massey University
Risk Management @ Massey University
Privacy @ Massey University

Document Management Control:

Prepared by: Information Technology Services
Authorised by: The Chief Information Officer
Approved by: SLT 16/08/162
Date issued: August 2016
Last review: August 2016
Next review: August 2019