Category: Facilities and IT
Version: 6
Document Type: Policy
Document Status: Published
Approved On: 06 November, 2019
Audience: Staff, Students, Research, Academic, Affiliate
Effective Date: 14 November, 2019
Review due by: 06 October, 2024
Policy Approver: Vice-President Administration & Finance And Chief Operating Officer
Policy Steward: Executive Director, Business Services And Chief Technology Officer
Supporting Process: Information Technology Processes

Information Security Policy (MPF1270)

1. Objective

The objective of this policy is to:

(a) provide a framework for managing the security of University information systems and assets;

(b) assist the University to ensure the confidentiality, integrity and availability of these systems and assets; and

(c) identify the roles, responsibilities and accountability of users and providers of information systems and assets.

2. Scope

This policy applies to:

(a) the management of all information security matters in the University;

(b) all University information systems and information assets regardless of location;

(c) all users of University information systems and information assets;

(d) all providers, for the facilities they provide; and

(e) all asset owners, for the assets they own.

3. Authority

This policy is made under the *University of Melbourne Act 2009* (Vic) and the Vice-Chancellor Regulation and supports compliance with the:

(a) *Copyright Act 1968* (Cth);

(b) *Health Records Act 2001* (Vic);

(c) *Privacy and Data Protection Act 2014* (Vic);

(d) *Public Records Act 1973* (Vic);

(e) *Privacy Act 1988* (Cth), where applicable;

(f) General Data Protection Regulation (EU) 2016/679, where applicable;

(g) AS ISO/IEC 27001:2015 – Information technology – Security techniques – Information security management systems – Requirements;

(h) AS ISO/IEC 27002:2015 – Information technology – Security techniques – Code of practice for information security management; and

(i) ISO 27001:2017 control objectives.

4. Policy

4.1. All users of information assets are responsible for information security in accordance with this policy, and its supporting processes and standards.

4.2. University divisions that operate information systems, and providers of information systems to the University, should include among the duties of one or more of their staff, the role of overseeing information security and providing expert local advice as required. Information security and risk management advice is available to University divisions from the Executive Director, Business Services and Chief Technology Officer.

4.3. External providers engaged by the University must comply with this policy and supporting processes and standards, as applicable to their role.

4.4. Information security is governed within the University, including by:

(a) development of an information security strategy;

(b) planning, monitoring, reviewing and ensuring the effectiveness of the overall Information Security Management Framework (ISMF);

(c) development of comprehensible and workable information security processes;

(d) measuring the effectiveness of the information security program through the collection and analysis of metrics, self-assessments and independent review; and

(e) providing guidance and support to role-bearers under this policy to fulfil their duties.

4.5. The University generally conducts internal audits at planned intervals to assess and inform whether the ISMF and the information security program:

(a) conform to the University's requirements; and

(b) are effectively implemented and maintained.

4.6. The University endeavours to continually improve the suitability, adequacy and effectiveness of the ISMF and the information security program.

4.7. The University aims to manage information security risks using a risk-based approach aligned to the University's Risk Management Policy and framework.

5. Procedural principles

Responsibilities of asset and service owners

5.1. Information assets have the following nominated asset owners:

(a) financial data – Vice-President (Administration & Finance) and Chief Operating Officer, and/or head of division;

(b) human resources data – Executive Director, Human Resources and OH&S, and/or head of division;

(c) student data – Executive Director, Student & Scholarly Services and Academic Registrar, and/or head of division;

(d) research data – Executive Director, Research, Innovation and Commercialisation, and/or head of division; and

(e) division-specific data – faculty executive director and/or head of division.

5.2. Where new access or changes to existing access or privileges are requested, the Service Owners will endeavour to:

(a) gain the approval of all relevant Asset owners before the request is fulfilled; and

(b) formally record the access changes and retain these records for a period of at least two years.

5.3. Service owners are responsible for:

(a) information assets within their responsibility being managed and used in accordance with this policy and any applicable legislation, regulations, or other University policy (including privacy and records management requirements);

(b) determining the importance, value and sensitivity of the information asset in accordance with relevant legislation, supporting processes and standards;

(c) deciding how and by whom the information asset may be used;

(d) specifying the business controls applying to the information asset;

(e) maintaining controls to protect information assets for which they are responsible;

(f) specifying the protection requirements for the information asset;

(g) monitoring compliance with this policy and initiating corrective action for breaches of this policy;

(h) the protection of the confidentiality, integrity and availability of information assets and information systems by appropriate controls determined through a risk-based approach;

(i) the classification of information assets and information systems in accordance with this policy and the relevant supporting processes;

(j) communicating the classification of the information assets to relevant stakeholders; and

(k) using a defence in depth approach to the implementation of security controls.

5.4. Service owners provide users with access to information systems based on the user’s role and the system’s associated functions.

5.5. Service Owner ensure that the Information systems should be configured to identify and authenticate all access to information assets that have not been classified as ‘public’ and deny access by default.

5.6. Service owners approve the assignment of access privileges or authorisations based on:

(a) the principle of least privilege, which dictates that only the required privileges are assigned (and no others); and

(b) on a need-to-know basis as appropriate to the user's role.

5.7. Service owners implement segregation of duties principles and consider any conflicts prior to access being granted.

5.8. Asset owners are responsible for privacy collection notices being provided to individuals when their personal or health information is collected or otherwise processed.

5.9. Line Managers are responsible for ensuring that a user's access is changed when that user's role changes, so that it reflects the requirements of their new role. Access rights not required for the new role should be revoked.

5.10. Line Managers are responsible for requesting users' access privileges are revoked or disabled immediately after a user's relationship with the University is terminated or when access is no longer required.

5.11. Asset owners document the security classification of the information assets for which they are responsible.

5.12. University information systems and assets are classified as:

Classification	**Definition**
Restricted	Information that is extremely sensitive, of great value to the University, and intended for use only by specific roles or named individuals.
Confidential	Information intended strictly for distribution to, or use by, a selected group of University employees and approved non-employees.
Internal	University information intended for all employees and approved non-employees such as contractors, vendors or students, but not the general public.
Public	Information available to the general public and intended for distribution outside the University.

5.13. Service owners are responsible for:

(a) the confidentiality, integrity and availability of information assets and information systems being protected by appropriate controls that are determined through a risk-based approach;

(b) the classification of information assets and information systems in accordance with this policy and the relevant supporting processes; and

(c) security controls being implemented using a defence in depth approach, unless considered unnecessary through a risk assessment.

5.14. Asset owners may delegate the routine management of information asset security to asset custodians, for example to a service owner. Administrative responsibilities may be delegated to asset custodians, but overall ownership of, and responsibility for, information assets remains with the asset owner.

5.15. Service owners are responsible for ensuring that all visitors and contractors are given temporary authorisation for appropriate system access, which will expire on the visitor or contractor's expected departure date or contract end date.

5.16. Service owners are responsible for ensuring that information systems enforce University password requirements.

5.17. Service owners are responsible for ensuring that an information security risk assessment and privacy impact assessment are completed, in consultation with Legal and Risk and the Cybersecurity team in Business Services, at planned intervals, and when:

(a) new information systems are being developed or acquired;

(b) a significant change is planned that may exceed the University's risk appetite; and

(c) new risks to production information systems are identified.

5.18. Service owners are responsible for ensuring that:

(a) application or infrastructure projects fulfil the requirements specified; and

(b) information systems that are developed are built, configured and maintained according to the relevant University security standards.

Responsibilities of asset custodians

5.19. Asset custodians have administrative and operational responsibility for information assets and follow all relevant information security policies, processes and standards to ensure the protection of information assets.

5.20. Asset custodians are responsible for:

(a) protecting the information asset in accordance with the directions of the asset owner;

(b) exercising sound business judgement in protecting the information asset;

(c) reporting to the asset owner on the discharge of asset custodianship activities; and

(d) maintaining individual registers of risks in relation to information assets that are critical to the University in line with the University's Risk Management Framework.

Responsibilities of heads of divisions

5.21. Heads of divisions are responsible for:

(a) actively supporting information security through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities;

(b) ensuring that all information security roles and responsibilities are clearly allocated;

(c) ensuring that the Information Security Policy and all supporting processes are effectively implemented in their areas of responsibility;

(d) conducting risk assessments to identify and define the positions that require applicants to pass personal background checks as part of the recruitment process; and

(e) communicating to staff members leaving the University their ongoing responsibilities to the University (which include ongoing confidentiality requirements in relation to University information assets).

Responsibilities of all users

5.22. Any action performed under a user ID is attributed to the person represented by the user ID. If an action performed under a user ID breaches, or leads to a breach of, University policy or process, then the user accepts responsibility for the breach, unless there is reasonable doubt that they are responsible for the breach.

5.23. Users must:

(a) keep passwords confidential and not disclose them to others;

(b) change their password as soon as possible if they suspect, or come to know, that their password has been compromised;

(c) distribute, transmit, move or delete information assets only if there is a valid business or academic need to do so;

(d) not remove a University information asset or equipment from University facilities without prior authorisation. Authorisation is deemed to have been granted to use University issued portable devices (such as laptops, mobiles, and tablets) to conduct daily business activities from remote locations; and

(e) distribute, transmit, move or delete information assets in accordance with University information handling standards and relevant contractual regulations and legal regulations as set out in section 3.

5.24. Users must not store information assets classified as ‘confidential’ or ‘restricted’ on the facilities of external providers, unless use of the facility has been approved by the applicable asset owner and the Executive Director, Business Services and Chief Technology Officer.

Responsibilities of all providers

5.25. Providers should ensure that operations that may impact the security of information assets are documented, with instructions maintained and communicated to all relevant parties.

5.26. Providers should allocate a unique user ID to each individual for information system access.

5.27. Providers should keep records of individuals’ access to, and use of, University computer systems, infrastructure and information assets.

5.28. Providers should ensure event log records of user activities, exceptions, faults and information security events are produced, kept securely and regularly reviewed.

5.29. Providers should ensure that information systems are configured in accordance with the relevant University information security standards and policies, including the Privacy Policy .

5.30. Providers are responsible for ensuring information assets are protected and they:

(a) place information assets in logical network zones with similar security and connectivity requirements; and

(b) use network segmentation and information flow controls appropriate to the information classification.

5.31. Providers are responsible for ensuring that they:

(a) segregate duties between staff assigned to development and testing environments, and staff assigned to production environments;

(b) where segregation of duties is not feasible, put a tracking mechanism and monitoring activities in place to trace production changes to an individual for accountability;

(c) segregate development, testing and production environments where resources permit; and

(d) where segregation of environments is not feasible, establish compensating controls to prevent the integrity, availability and confidentiality of the information asset from being compromised.

5.32. Providers should ensure that:

(a) test plans and cases are documented, testing is performed, and test results recorded and retained;

(b) test data and accounts are deleted from the developed system or application, and from third parties' systems, before deploying software into the production environment;

(c) security testing is performed prior to deployment which provides assurance that residual security vulnerabilities have been formally risk accepted; and

(d) security testing is periodically performed in accordance with University information security standards.

5.33. Providers are responsible for performing regular system checks and capacity monitoring (such as memory, network performance, disk-space utilisation and processing power) to ensure optimum performance.

5.34. Providers should obtain timely information about technical vulnerabilities of all systems being used, assess the University's exposure to identified vulnerabilities and perform a risk assessment. Based on the results of the assessment, providers should ensure that appropriate measures are taken (including applying patches or other compensating controls) to address the associated risk.

5.35. Providers are responsible for ensuring that all incidents that could impact on the University are promptly identified, managed and resolved, through formal information security incident management processes that minimise these impacts and allow affected processes to be quickly resumed.

5.36. Providers should ensure that information critical to the University is backed up and/or copied to an alternative site on a regular and frequent basis.

5.37. Providers should ensure information security processes and controls are monitored, evaluated and outcomes documented to ensure their continued effectiveness and timeliness.

5.38. Providers should ensure that University information systems are physically protected in accordance with relevant University physical security standards.

5.39. Providers should ensure that:

(a) University information systems in controlled areas, such as data centres, are physically protected by establishing a security perimeter, access controls, intrusion detection, environmental protection, surveillance, and ensuring the availability of utilities;

(b) any individual who accesses a data centre must provide their access card for identification purposes when requested;

(c) processes are implemented and maintained to grant, update and revoke access to data centres;

(d) all individuals accessing data centres either:

(i) complete an on-site induction prior to their access; or

(ii) for visitors, are accompanied at all times by an authorised person (who has completed induction).

(e) University information systems are protected from damage by fire, flood, earthquake, explosion, civil unrest, and other forms of natural or artificial disaster;

(f) a data centre recovery plan is created, maintained and tested annually to allow the continuous operation of the data centre;

5.40. Providers ensure that physical and logical network documentation is created, reviewed and maintained for all networks under their control.

5.41. Providers document the configuration of all systems under their control and ensure that they review and update documentation to reflect changes in configurations at least annually or after every major change.

5.42. Providers ensure that access to administration/maintenance zones requires two-factor authentication.

External providers

5.43. External providers must not commence handling or processing any information assets for the University until it has entered into an appropriate contract with the University that includes relevant information security controls with which the provider must comply.

5.44. Without limiting external providers' other obligations set out in this policy, external providers must implement, operate and maintain the appropriate information security controls as specified in their contracts with the University.

5.45. Heads of division monitor and review external provider services and manage any changes to external provider contracts taking into account information assets and information systems.

5.46. External providers must ensure that they only connect devices to the University network using approved secure access methods.

Business continuity and disaster recovery

5.47. Develop, implement, maintain and test business continuity and disaster recovery plans with the goal of ensuring that the recovery of business processes and critical information assets is within acceptable business timeframes, and to promote the ongoing availability of business processes and critical information assets.

5.48. The Executive Director, Business Services and Chief Technology Officer is responsible for the development and currency of a master information technology disaster recovery plan that:

(a) identifies the technical services making up a business service and the interdependencies between these technical services; and

(b) presents an overall plan for recovering and restoring the University's technological services and capabilities after a disaster.

Information security awareness

5.49. The Executive Director, Business Services and Chief Technology Officer is responsible for:

(a) staff receiving information security induction and awareness training upon commencement of a role;

(b) training reoccurring at least every two years and at a frequency meeting the University's obligations in relation to the staff's role;

(c) such training including the information security policy, related guidance, and the correct use of information assets and information systems; and

(d) users formally acknowledging, and agreeing to abide by, the information security policy at a frequency relevant to the staff's role.

5.50. The University's information security awareness program aims to promote awareness, through a number of methods, of:

(a) this policy and supporting processes;

(b) the types of information asset that may be encountered;

(c) how information assets should be handled and transmitted;

(d) information security concerns such as viruses, malware and social engineering;

(e) workplace and facility security, including building access, security controls and incident reporting;

(f) the consequences of failure to comply with this policy and related processes; and

(g) information security considerations as appropriate to the individual's role.

Compliance

5.51. The Executive Director, Business Services and Chief Technology Officer monitor compliance with this policy and supporting processes.

5.52. An authorised deviation from this policy may be granted if, following risk assessment, the impact of non-compliance is outweighed by the benefit of non-compliance. All deviations must be approved by the Executive Director, Business Services and Chief Technology Officer.

5.53. The Executive Director, Business Services and Chief Technology Officer is responsible for ensuring that:

(a) a register of policy exceptions is maintained;

(b) remediation is tracked, and effectiveness reviewed;

(c) an assessment is performed to identify other systems requiring a similar exception; and

(d) changes are recommended to the ISMF based on identified nonconformities.

5.54. With respect to any exceptions from this policy, asset owners are responsible for:

(a) performing a risk assessment to understand the impact of the exception;

(b) documenting a time-bound remediation plan;

(c) providing advice to the Director of Cybersecurity to maintain the exceptions register; and

(d) ensuring that the exception, and the actions to be taken to control and correct it, are formally approved by relevant asset owners, service owners and the Executive Director, Business Services and Chief Technology Officer.

5.55. Any record created as a result of this policy must be managed in accordance with the University's Privacy Policy and Records Management Policy .

Breaches and non-compliance

5.56. Any breach of this policy or related processes may result in:

(a) suspension of access to the information system or asset, or other systems;

(b) disciplining action under the relevant disciplinary instrument, and/or;

(c) termination of contract or future legal action.

5.57. External providers who breach this policy will be subject to suspension of access, termination of contract and/or further legal action.

5.58. Users must promptly report potential breaches of this policy and suspected information security weaknesses to the Executive Director, Business Services and Chief Technology Officer.

5.59. Users must notify the IT Service Centre and the University Privacy and Data Protection Officer immediately of any potential breach if 'internal', 'confidential' or 'restricted' information (including personal or health information):

(a) is accidentally or unlawfully lost, misused, or altered, or if it is accessed by or disclosed to unauthorised parties; or

(b) is suspected of being accidentally or unlawfully lost, misused, altered, or accessed by or disclosed to unauthorised parties.

5.60. Anyone who identifies any damage to, or loss of University server or network hardware or software must promptly report this to the IT Service Centre and University security staff.

5.61. Asset owners and service owners are responsible for ensuring that faults with business-critical applications are reported to the Executive Director, Business Services and Chief Technology Officer as quickly as possible.

6. Roles and responsibilities

Role/Decision/Action	***Responsibility***	***Conditions and limitations***
Responsible for the roles set out in sections 5.1-5.8, 5.11-5.18, and 5.61 of this policy	*Asset owner and Service Owner*	In accordance with this policy and supporting processes
Responsible for the roles set out in sections 5.9-5.10 of this policy	*Line managers*	In accordance with this policy and supporting processes
Responsible for the roles set out in sections 5.19–5.20 of this policy	*Asset custodian*	In accordance with this policy and supporting processes . Where an asset custodian is also a provider, the asset custodian also has the same responsibilities as a provider (see below).
Responsible for the roles set out in section 5.21 and 5.45 of this policy	*Heads of Division*	In accordance with this policy and supporting processes

Responsible for the roles set out in sections 5.22–5.24, 5.58, and 5.59 of this policy	*Users*	In accordance with this policy and supporting processes
Responsible for the roles set out in sections 5.25–5.42 of this policy	*Providers*	In accordance with this policy and supporting processes
Responsible for the roles set out in sections 5.43, 5.44, and 5.46 of this policy	*External providers*	In accordance with this policy and supporting processes
Responsible for the roles set out in sections 5.49 and 5.53 of this policy	*Executive Director, Business Services and Chief Technology Officer*	In accordance with this policy and supporting processes
May approve storage of information assets classified as 'confidential; or 'restricted' on facilities provided by external providers	*Executive Director, Business Services and Chief Technology Officer*	In accordance with section 5.24 of this policy
Ensure a master IT disaster recovery plan exists	*Executive Director, Business Services and Chief Technology Officer*	In accordance with section 5.48 of this policy
Monitor compliance with this policy and supporting processes	*Executive Director, Business Services and Chief Technology Officer*	In accordance with section 5.51 of this policy
May authorise a deviation from this policy	*Executive Director, Business Services and Chief Technology Officer*	In accordance with section 5.52 of this policy

7. Definitions

Asset custodian means an individual, group or external provider to whom responsibility for the information security of an information asset is delegated by the Asset owner. Asset custodian will commonly be a Service Owner but may also be the owner of a non-technical business service or process.

Asset owner means an individual who holds accountability for an information asset. An asset owner is the owner of specific data elements, wherever the data resides. An asset owner may delegate operational responsibility to many asset custodians.

Availability refers to ensuring that authorized parties are able to access the information when needed. Information only has value if the right people can access it at the right times.

Central facilities means the data networks owned or operated by the University for which the Executive Director, Business Services and Chief Technology Officer is responsible and includes all associated computing and network facilities but does not include any local facilities.

Computing and network facilities includes computers, computer systems, data network infrastructure, dial■in network access facilities, email and other communications and information facilities together with associated equipment, software, files, and data storage and retrieval facilities, all of which are owned or operated by the University and form part of the central facilities or the local facilities.

Confidentiality is the property, that information is not made available or disclosed to unauthorised individuals, entities, or processes.

Defence in depth means the practice of layering information asset defences to provide added protection.

External provider means an external entity which provides an information system to the University or a service that involves the handling or processing of information assets.

Generic user account means an account that does not have a named owner or does not belong to any one individual.

Information asset means recorded information in any format.

Information security means the preservation of confidentiality, integrity and availability of information assets, and may also include other properties such as authenticity, accountability, non-repudiation and reliability of information assets.

Information Security Management Framework (ISMF) governs the processes and responsibilities comprising the overall information security framework. It is supported by a suite of policies, processes and metrics which apply to all information assets accessed by employees, students, contractors, agents and third parties.

Information security program means the operations, initiatives and activities that are undertaken to ensure the confidentiality, integrity, availability and accountability of the University's information assets.

Information system means hardware, software, devices, networks, media and other resources that store, process or transmit information assets, whether individually or in combination.

Integrity means that information assets, facilities and services are what they are reasonably represented as. They are protected from tampering which would make their content or functionality other than what would be reasonably expected.

Least privilege means that entities (whether these are people, processes, or devices) must be assigned the fewest privileges consistent with their assigned duties and functions. Under this approach, zero access is the default access level, and access is added or opened as required, but no more than the minimum access levels necessary to perform required functions or tasks.

Line manager means the direct manager in a division who is responsible for the management of employees.

Local facility means a network of interconnected computers and equipment operated by a particular faculty, department or other organisational unit of the University and for which the Executive Director, Business Services and Chief Technology Officer is not responsible, whether or not that network is also connected to the central facilities. This includes all associated computing and network facilities.

Non-compliance means any action or inaction that is contrary to this policy and its related processes or standards.

Privileged user means a user with a high level of access to data (with the power to read, update, delete) and is able to perform functions over and above those that can be completed by the majority of users.

Provider means the University division or third-party provider which provides and manages any part of the facilities.

Segregation of duties means the controls that support the separation of incompatible duties and/or responsibilities. Segregation of duties helps to ensure that individuals are not able to:

(a) conceal errors and/or irregularities;

(b) cause the inaccurate or incomplete reporting of financial information; and

(c) commit fraud, theft or other illegal acts.

Service owner means an individual who has been allocated responsibility for an information system (such as an. application, device, network, cloud service, or a specific component thereof). There is only one service owner for each information system. A service owner will commonly be delegated asset custodian responsibilities by several asset owners.

Significant assets means information assets that support the efficient and effective operation of key business processes. Significant assets can be identified by undertaking an assessment in accordance with the University's Risk Management Policy to determine if the information has value to the University.

Student has the meaning given to it in Part 8, Division 1 – Student Misconduct – of the Academic Board Regulation.

Use means any act or omission by a user which affects in any way the operation of an information system.

User(s) means any person who uses, or may impact the security of, university information assets whose activity the University may reasonably expect to able to exert authority. This includes, but is not limited to staff, students, officers, third parties and other agents.

POLICY APPROVER

Vice-President (Administration & Finance) and Chief Operating Officer

POLICY STEWARD

Executive Director, Business Services and Chief Technology Officer

REVIEW

This policy is to be reviewed by 6 October 2024.

VERSION HISTORY

Version	Authorised by	Approval Date	Effective Date	Sections modified
1	Vice Principal Administration & Finance on behalf of the Senior Vice-Principal	27 March 2014	27 March 2014	N/A

2	Vice-Principal Administration and Finance & CFO	2 June 2016	21 July 2016	New version arising from the Policy Consolidation Project. This policy and its supporting processes replace the former Information Security Policy MPF1270, Computer Operations Procedure MPF1272, Data Centre Physical Security Procedure MPF1273, Disaster Recovery Procedure MPF1286, Information Classification and Handling Procedure MPF1274, Logging and Monitoring Procedure MPF1275, Network Security Procedure MPF1276, Service Development Security Requirements Procedure MPF1277 and User and System Access Procedure MPF1278.
3	-	-	-	*Created in error*
4	University Secretary	24 May 2019	4 June 2019	Amended Policy Approver title. Editorial amendments to correct minor errors or align with the University's policy style guide.
5	University Secretary	31 July 2019	1 August 2019	Amended Policy Steward title.

6	Vice-President (Administration & Finance) and Chief Operating Officer	6 November 2019	14 November 2019	Amendments made across various sections to improve internal consistency and clarity, as well as ensure the policy statements and procedural principles align with industry best practice including ISO27001 control objectives, NIST Cybersecurity framework, Copyright Act 1968, Public Records Act 1973, and privacy related legislation including the EU General Data Protection Regulation (GDPR), Privacy and Data Protection Act 2014, Privacy Act 1988 and the Health Records Act 2001.