Information Security Policy (MPF1270)

1. Objective

The objective of this policy is to ensure the confidentiality, integrity, availability and accountability of the University's information 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's 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) AS ISO/IEC 27001:2015 – Information technology – Security techniques – Information security management systems – Requirements;

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

(g) Payment Card Industry Data Security Standard (PCI DSS)

4. Policy

4.1. The security of, and appropriate access to, the University's information assets is a critical priority for the University and its information technology structure.

4.2. All users are responsible for information security in accordance with this policy.

4.3. Heads of divisions:

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

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

(c) ensure that the information security policy and all supporting processes have been effectively implemented for their areas of responsibility;

(d) identify and define positions or roles that have unrestricted access to one or more information assets to ensure that personal background checks are conducted on individuals in these positions; and

(e) communicate to staff members leaving the University their ongoing responsibilities to the University (eg ongoing confidentiality requirements on University information assets).

4.4. University divisions that operate IT facilities 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 from the Executive Director, Infrastructure Services.

4.5. The University gives external providers access to this policy and makes clear that compliance with the policy is expected.

4.6. The Information Security Management Committee (ISMC), a sub-committee of the Risk Management Advisory Group, has functions including:

(a) recommending the strategic direction of the information security program;

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

(c) making policy recommendations on information security matters.

4.7. The ISMC measures the effectiveness of the information security program through the collection and analysis of metrics, self-assessments and independent review.

5. Procedural Principles

Responsibilities of asset owners

5.1. The information assets that must have a nominated asset owner are:

(a) financial data – Vice-Principal Administration and Finance & CFO, and/or head of division

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

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

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

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

5.2. Asset owners approve all requests for new access and changes to existing access privileges. All requests must be in writing and approved before they are fulfilled. To help establish accountability for events on related systems, documents or records reflecting these requests will be retained for a period of at least two years.

5.3. Asset owners are responsible for:

(a) ensuring information assets within their responsibility are managed and used in accordance with this policy and any applicable legislative or compliance requirements (such as privacy and records management);

(b) judging 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 their information assets;

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

(g) communicating to others the classification of the information assets; and

(h) monitoring compliance with this policy and initiating corrective action for breaches of this policy.

5.4. Asset owners ensure that users are provided with access to information systems based on their role and the functions they are required to perform as part of their duties, in accordance with sections 5.5–5.7.

5.5. University systems identify and authenticate all users of information systems when they are accessing information that has not been classified as ‘public’.

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

(a) the principle of least privilege, ie only required privileges are assigned (and no more);

(b) on a need-to-know basis as appropriate to the user’s job function.

5.7. Asset owners ensure that:

(a) where technically feasible, providers implement controls to prevent breaches of segregation of duties;

(b) segregation of duties conflicts are considered before authorising and allocating account access privileges; and

(c) if segregation of duties cannot be implemented, compensating controls are in place with an approved documented exception.

5.8. Asset owners ensure users of assets are given a collection notice when personal, sensitive or health information is requested.

5.9. Asset owners ensure that when a user changes from one role to another, their access is amended to reflect the requirements of their new job. Access rights that are no longer required will be removed.

5.10. Asset owners ensure that all of a user's access privileges are revoked or disabled:

(a) immediately after the user's relationship with the University is terminated, by either the University or the user; or

(b) when the user account has not been accessed for more than 160 days.

5.11. Asset owners document the security classification ratings of information assets for which they are responsible and assign an asset custodian to each asset.

5.12. Asset owners ensure that 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 various named individuals, including any personally identifiable information or credit card data
Confidential	Information assets intended strictly for distribution/use by a small selected group
Internal	University information intended only for all employees and approved non-employees such as contractors, vendors or students
Public	Information available to the general public and intended for distribution outside the University

5.13. Asset owners advise the security team of the ratings so that information assets are adequately protected.

5.14. Asset owners ensure that:

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

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

(c) all information assets and information systems access is provided only on the basis of least privilege and need to know; and

(d) security controls are implemented using a defence in depth approach which includes multiple layers of defence, unless considered unnecessary through a risk assessment.

5.15. Asset owners ensure that any application or system storing data classified as internal, confidential or restricted denies access by default and implements identification controls using username and at least one other appropriate authentication method in accordance with the relevant supporting process.

5.16. Asset owners may delegate the day to day management of information asset security to asset custodians who may be persons, groups or external providers (eg IT service providers). Administrative responsibilities can be delegated to asset custodians, but overall ownership of, and responsibility for, information assets always remains with the asset owner.

5.17. Asset owners must ensure that guest logins for conference delegates or use of guest logins in libraries and 'kiosk' settings are acceptable and take appropriate measures to manage the risk of misuse or security compromise.

5.18. Asset owners ensure that all visitors and contractors are given temporary authorisation for system access that expires on their expected departure date or contract end date.

5.19. Asset owners must approve any group, shared or generic accounts before they are created.

5.20. Asset owners ensure systems enforce rules intended to make passwords as strong as possible.

5.21. Asset owners ensure that an information security risk assessment and privacy impact assessment is completed when:

(a) new technology services are developed at the service charter stage as part of the service change lifecycle or at an appropriate point of the system's development lifecycle; and

(b) deploying changes with a moderate, high and significant residual risk into the production environment in accordance with the University's ISMF guidelines, and aligned with the overall University Risk Management Framework.

5.22. Service owners ensure that:

(a) application or infrastructure projects fulfil the requirements specified and approved at the service charter and service design stages;

(b) systems developed are built and/or configured and maintained according to the relevant security configuration standard determined by the IT Security and Risk Team; and

(c) configuration items that cannot be built to the standards are identified and assessed to determine if compensating controls exist, or if the configuration item must be raised as a deviation requiring approval in accordance with this policy.

5.23. The Vice-Principal Administration and Finance & CFO may issue directives that will be followed by all asset owners.

Responsibilities of asset custodians

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

5.25. 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;

(d) maintaining a register of risks to each information asset that is critical to the University; and

(e) documenting any decisions taken on identified risks such as risk acceptance, risk transference, risk avoidance or risk mitigation to each critical information asset.

Responsibilities of all users

5.26. All individuals issued with a user identifier (user ID) acknowledge a compliance statement that indicates they understand and agree to abide by the Information Security Policy.

5.27. Any action performed under a user ID is attributed to the owner. 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.

5.28. Users must:

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

(b) not write passwords down unless they are encoded in a way that is not obvious to others;

(c) not use the same password for accessing University information and information systems as non-University systems;

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

(e) distribute information assets only if there is a valid business need to distribute, transmit or move such information.

5.29. Users must not store information assets classified as 'confidential' or 'restricted' on facilities of external providers unless use of the facility has been approved by the applicable asset owner and the Executive Director, Infrastructure Services.

Responsibilities of providers

5.30. Providers ensure that guidelines for computer operations are documented, maintained and made available to all University staff, contractors and external providers who need them.

5.31. Providers allocate a unique user ID to individuals for system access.

5.32. Providers keep records of individuals' access to, and use of, University computer systems, infrastructure and information assets.

5.33. Providers ensure that all enterprise applications and systems containing data classified as confidential or restricted, record and retain an audit log of user access.

5.34. Providers ensure that all computing infrastructure, application and operating system software is configured in accordance with the relevant University security configuration standard.

5.35. Providers establish network zones to separate networks from one another. Separate network zones will be established for: research, development/testing, production servers, workstations, and other relevant zones. Network zones will be created for systems with similar security and connectivity requirements.

5.36. Providers ensure 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.

5.37. Providers ensure that:

(a) testing activities for application or infrastructure projects fulfil the service transition stage requirements;

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

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

(d) testing (such as vulnerability scanning, configuration reviews and penetration testing of the system) is performed before deployment into the production environment to provide assurance that no known security vulnerabilities exist.

5.38. Providers perform regular system checks and capacity monitoring (such as memory, network performance, disk-space utilisation and processing power) to ensure optimum performance.

5.39. Providers 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 will ensure that appropriate measures are taken (eg applying patches or other compensating controls) to address the associated risk.

5.40. Providers ensure that all incidents that could have an impact on the University are identified, handled and resolved promptly, through a series of formal processes that minimise impacts and allow all affected processes to be quickly resumed.

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

5.42. Providers document all monitoring processes as evidence of completeness and timeliness of system and data batch jobs.

5.43. Providers ensure that:

(a) University server and network hardware and access to such assets are physically protected by establishing a security perimeter, including barriers such as walls, reception desks, alarms, auditable locks and/or electronically access-controlled doors;

(b) access to data centres is approved by an authorised person, and that records of approval and authorisation are retained;

(c) staff and visitors who access a data centre are clearly identifiable by the visible display of identity badges;

(d) processes are implemented and maintained to grant, update and revoke issued identity badges;

(e) visitors to University data centres are accompanied by a duly authorised person at all times;

(f) contractors working in data centres are inducted on site;

(g) University server and network hardware is protected from damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or artificial disaster;

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

(i) data centres are monitored through the use of security cameras placed, at a minimum, at the entry and exit points;

(j) security camera recordings are kept for at least 14 days; and

(k) security cameras are installed and managed in accordance with University design standards and the Property Policy.

5.44. Providers ensure that physical and logical network documentation is created, reviewed and maintained for all wired, wireless and phone networks.

5.45. Providers document the configuration of all systems under their control including servers, networking hardware, workstations and mobile devices.

5.46. Providers ensure that system documentation is reviewed and updated to reflect changes in configurations at least annually or after every major change.

External providers

5.47. The University specifies information security controls in all contracts for services or acquisition of equipment.

5.48. External providers implement, operate and maintain the appropriate information security controls as specified in their contracts with the University.

5.49. Asset owners monitor and review external provider services, and manage any changes to external provider contracts taking into account the importance of impacted systems and business processes.

5.50. Providers ensure that strong end-to-end encryption is used to protect data transmitted over external network connections to and from the University network. Information classified as public does not require encryption.

5.51. Providers ensure that remote access to University information assets is through the use of a virtual private network (VPN) connection. Asset owners must approve other access methods.

5.52. Providers ensure that all users connecting to the University network via VPN are limited to the access they require to perform their studies or duties. Access will be limited to specific hosts and ports/services/protocols as is required.

5.53. Providers ensure that a VPN connection is mandatory for connections to zones with administration/maintenance access to network devices, servers, databases and other supporting infrastructure.

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

Business continuity and disaster recovery

5.55. Divisions develop, implement and maintain business continuity and disaster recovery plans to ensure the ongoing availability and/or recovery of critical information assets within acceptable business timeframes.

5.56. Asset owners ensure that disaster recovery plans for the business-critical applications that are their responsibility are tested at least annually. The Executive Director, Infrastructure Services guides and advises asset owners on acceptable types of testing.

5.57. The Executive Director, Infrastructure Services ensures the development and currency of a master information technology disaster recovery plan that:

(a) identifies the technical services that make 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

5.58. Asset owners ensure that users receive information security induction and awareness training on commencement of employment/enrolment and at least every two years. The training includes consideration of information security policies and related processes, and the correct use of information asset processing facilities.

5.59. Information security awareness training content includes consideration 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/facility security including building access, security controls and reporting of incidents; and

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

Compliance

5.60. The Executive Director, Infrastructure Services monitors compliance with this policy and supporting processes.

5.61. An authorised deviation from this policy may be granted if it is clear that the costs and resources necessary for compliance far outweigh the risks of non-compliance. Written permission must be obtained from the relevant asset owner and Executive Director, Infrastructure Services.

5.62. The Manager, IT Security and Risk logs and manages all deviations.

5.63. Asset owners ensure that all deviations from this policy have a documented and approved remediation plan. If no remediation activity is available, appropriate controls must be in place to mitigate risks so that all remediation activity is:

(a) time bound and has a realistic delivery date; and

(b) risk-assessed to understand its intrinsic value of benefit provided versus cost of implementation.

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

Breaches and non-compliance

5.65. Any breach of this policy may infringe relevant legislation as listed in section 3 of this policy and expose persons to liability under such legislation.

5.66. Any breach of this policy or related processes may constitute misconduct under University policy or applicable legislation, including staff and students exposure to disciplinary action.

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

5.68. Users must promptly report breaches of this policy and suspected information security weaknesses to the Executive Director, Infrastructure Services.

5.69. Users must notify the asset owner and the IT Service Desk immediately if 'internal', 'confidential' or 'restricted' information:

(a) is lost or disclosed to unauthorised parties; or

(b) is suspected of being lost or disclosed to unauthorised parties.

5.70. Anyone who identifies any damage to, or loss of, University server, network hardware or software must promptly report relevant details to the IT Service Desk and University security staff.

5.71. Asset owners must ensure that faults with business-critical applications are reported to the Executive Director, Infrastructure Services as quickly as possible.

6. Roles and responsibilities

Role/Decision/Action	*Responsibility*	*Conditions and limitations*

Responsible for the roles set out in sections 5.2–5.23 of this policy	*Asset owner*	In accordance with this policy and supporting processes
Responsible for the roles set out in sections 5.24–5.25 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 sections 5.26–5.29 of this policy	*Users*	In accordance with this policy and supporting processes
Responsible for the roles set out in sections 5.29–5.46 of this policy	*Providers*	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 - Guide and advise asset owners on acceptable types of disaster recovery plan testing - Ensure a master IT disaster recovery plan exists - Monitor compliance with this policy and supporting processes - May authorise a deviation from this policy	*Executive Director, Infrastructure Services or nominee*	In accordance with section 5.29 of this policy In accordance with section 5.56 of this policy In accordance with section 5.57 of this policy In accordance with section 5.61 of this policy
Maintain a register of information assets	*Director, Business Intelligence and Reporting*	The register accounts for all significant information assets and lists the asset owner. These records will be reviewed annually.

7. Definitions

Asset custodian, asset custodianship mean users who perform operations within information systems to manage, operate and protect information assets on behalf of the asset owner.

Asset owner means all individuals who have been allocated responsibilities and hold accountability for an information asset.

Central facilities means the data networks owned or operated by the University for which the Executive Director, Infrastructure Services 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, as the case may be.

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

External provider means an external entity which provides computing and network facilities to the University.

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 preservation of confidentiality, integrity and availability of information assets; it may also include other properties such as authenticity, accountability, non-repudiation and reliability.

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 is a combination of people, hardware, software, communication devices, network and data resources that processes (can be storing, retrieving, transforming information) data and information for a specific purpose.

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

Least privilege means an information security concept that entities (people, processes, devices) must be assigned the fewest privileges consistent with their assigned duties and functions. For example, this approach defines zero access by default and then opens or adds access as required, but provides no more than the minimum necessary to perform the 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, Infrastructure Services is not responsible, whether or not that network is also connected to the central facilities, including all associated computing and network facilities.

Non-compliance means any action or inaction that is contrary to this Information Security Policy and its related processes or standards. Breaches of this policy and suspected security weaknesses should be promptly reported to the line manager or the Executive Director, Infrastructure Services.

Privileged user means a user with a high level of access to data (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 which provides and manages any part of the facilities.

Segregation of duties means controls that represent the separation of incompatible duties and/or responsibilities. Segregation of duties helps to ensure that one person is 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.

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 the central facilities or a local facility.

User(s) means any member of staff or a student, or any other person who uses the central facilities or a local facility, including a provider and any officer, employee or agent of a provider.

POLICY APPROVER

Vice-Principal Administration and Finance & CFO

POLICY STEWARD

Executive Director, Infrastructure Services

REVIEW

This policy is to be reviewed by 2 June 2021.

VERSION HISTORY

Version	Authorised by	Approval Date	Effective Date	Sections modified
1	Vice Principal Administration & Finance on behalf of the Senior Vice-Principal	27 Mar 2014	27 Mar 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.