INFORMATION AND CYBER SECURITY POLICY

Approved by Council: 23 November 2016
Revised by Council: None

Related Documents

Privacy Policy
Inclusion Policy

Privacy and Data Protection Act 2014 (Vic)
Public Records Act 1973 (Vic)
Copyright Act 1968 (Cth)

1. Purpose

1.1 The purpose of this policy is to protect information and information systems by establishing a framework of information security controls, management and governance.

2. Scope

2.1 This policy applies to the management of all University information asset security, information systems and any users or third-party service providers regardless of location. All users of information assets are responsible for its security in accordance with this policy and supporting frameworks, procedures and codes of practice.

3. Definitions

3.1 “Cyber security” means the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. Information security and cybersecurity protects the integrity and functionality of the University.

3.2 “Information asset” means recorded information in any format belonging to the University.

3.3 “Information security” means the preservation of confidentiality, integrity and availability of information assets.

3.4 “Information technology asset” means all hardware, software and connectivity access owned or managed by the University.

3.5 “User” means any person who accesses and uses University information assets.
4. **Principles**

4.1 Information assets are developed and made accessible for legitimate use in delivering the University's mission.

4.2 Information assets are protected against unauthorised access and inappropriate use.

4.3 Users of information assets and information technology assets are aware of their responsibilities, especially in relation to privacy and security, and are informed of the rules for access and usage.

4.4 Information and cyber security is governed effectively, including identification and management of policy breaches.

5. **Responsibilities of the University**

5.1 The Council is responsible for ensuring that sufficient resources are available to give effect to this Policy.

5.2 The Vice-Chancellor is responsible for:

   a) regular assessment of the effectiveness of this Policy
   
   b) reporting any breaches of this Policy to the Risk Management and Audit Committee, and, as appropriate, to the Council
   
   c) maintaining accountabilities for information security throughout all levels of the organisation
   
   d) establishing a Code of Practice for the use of University information technology assets through the approval and modification of Schedule 1 of this Policy
   
   e) the assignment of responsibilities to staff members to implement this Policy through the approval and modification of Schedule 2 of this Policy
   
   f) establishing rules for granting, reviewing, and removing access to University information technology assets through the approval and modification of Schedule 3 of this Policy.

5.3 The Office of the Vice-Chancellor is responsible for:

   a) implementing and maintaining appropriate information security controls within systems and processes, including those relating to third-party relationships
   
   b) identifying changes in threats, technologies and regulatory obligations and recommend strategic actions
   
   c) implementing processes that regular identify any information security exposures, assess information security control effectiveness in business processes, and assess user handling of information assets
   
   d) maintaining records of information security decisions and actions
   
   e) communicating and educating users of the principles of this policy and detailed expectations of their behaviour and accountabilities.
6. Responsibilities of Users

6.1 Users of information assets:

a) must only access and use information assets where permitted and in accordance with the code of practice contained in Schedule 1 of this Policy

b) must secure and restrict access to information assets at all times including where being used outside of University premises

c) may only grant third-party access to information for legitimate business purposes and where the relationship with that third-party is approved and monitored by the University and complies with the Privacy Policy

d) must report any breaches of this Policy immediately to the Vice-Chancellor

6.2 Any user found breaching this policy may be subject to disciplinary action in accordance with University policy and the terms of any agreement defining the user’s relationship with the University.

7. Date of next review

7.1 This policy must be reviewed at least once every two years.

7.2 This policy is to be reviewed no later than 31 December 2018.
SCHEDULE 1: Code of Practice for the use of Information Technology Assets
Approved by the Vice-Chancellor: 1 January 2017

This Code of Practice for the use of Information Technology Assets supports the University of Divinity’s Information and Cyber Security Policy and applies to all users, information assets, and information technology assets (IT assets) as defined within the Policy.

The University monitors the access and use of IT assets to ensure compliance with this code of practice; this includes where IT assets are being used for personal use or where personal devices are accessing IT assets. Users are required to report any actual or suspected breaches of this code of practice by other users or themselves (even inadvertent) as per the requirements of the policy. Users found to be in breach of this code of practice are considered to be in breach of the Policy.

Access to IT assets must only be granted to authorised users who are responsible for all activity that originates from the assets themselves and user software accounts therein. This includes access to connectivity points (such as WiFi) through personal devices.

Access and stewardship of IT assets is granted for the primary purpose of advancing the University towards its mission. Limited personal use of IT assets, where it does not relate to University business, is permitted where it does not require a substantial expenditure of time, adversely affect the University or breach the policy or this code of practice.

Users must:

a) only use IT assets that have been allocated to them, or to which they have been temporarily granted access, by the University.

b) only access IT assets using their unique usernames and associated passwords.

c) maintain total confidentiality of their unique usernames and associated passwords.

d) ensure that physical IT assets are secure at all times both within University premises and when outside University premises.

e) advise any visitors accessing IT assets of the need to act in accordance with this Code of Practice

f) report immediately to the University’s IT Systems Officer if they suspect that IT assets of the University have been inappropriately accessed by third parties (‘hacked’) or where the confidentiality of usernames or passwords may have been compromised.

Users must not:

g) use IT assets to contravene any University Policy or violate local, State, Commonwealth or international Law

h) use IT assets for the purposes of private business, personal gain or profit

i) use IT assets for the purposes of soliciting support or to advertise products except where approved by the Vice-Chancellor

j) use IT assets to access, view or distribute material that is offensive or to engage in behaviour that discriminates against, harasses, bullies or defames others

k) use IT assets for malicious activity designed to weaken or subvert security measures and controls within the University IT networks or in a manner that may bring University reputation into question (this includes using University email accounts to criticise other members of the University or the University itself to external parties).
### SCHEDULE 2: Information and Cyber Security Staff Responsibilities

Approved by the Vice-Chancellor: 1 January 2017

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Financial Officer</td>
<td>Reports regularly to the Risk Management and Audit Committee on the status of information and cyber security at the University</td>
</tr>
<tr>
<td>Director of Academic Services</td>
<td>Authorises the access of academic and administrative staff to University information technology assets including the student record system and learning management system. Ensures that staff and students granted access are aware of their responsibilities under this Policy. Revokes access where required under schedule 3.</td>
</tr>
<tr>
<td>Director of Quality and Standards</td>
<td>Authorises the access of academic and administrative staff to University information technology assets including the student record system and learning management system. Ensures that staff and students granted access are aware of their responsibilities under this Policy. Annually reviews all parties with access to systems.</td>
</tr>
<tr>
<td>IT Systems Officer</td>
<td>Designs Information Technology assets and implements processes for use securely. Undertakes regular information and cyber security audits or reviews and reports results to the Chief Financial Officer. Maintaining records of security frameworks and decisions. Reports any breaches of this Policy to the Vice-Chancellor with recommendations for action.</td>
</tr>
</tbody>
</table>
SCHEDULE 3: Access to University information technology assets

Approved by the Vice-Chancellor: 1 January 2017

This schedule details the process for obtaining and authorities for approving access to the student record system (“TAMS”). Access to TAMS generates access to other University information technology assets including the learning management system.

Users whose access is not automatically generated must complete the IT Systems Access Form published on the University website. Completed forms must be filed securely at the Office of the Vice-Chancellor in accordance with the provisions of the University’s Privacy Policy.

1. **Students**
   
   **Type:** Student
   
   **Level:** Read-only access, only for the student’s own record
   
   **Access:** Access is automatically generated to currently enrolled students once their enrolments have been approved by their Coursework or Research Co-ordinators and entered into TAMS. Access to TAMS is revoked when a student ceases to be enrolled.
   
   **Support:** Students should seek assistance in relation to TAMS access from their College Registrar.

2. **College Academic and Administrative Staff (basic access)**
   
   **Type:** Basic
   
   **Level:** Read-only access to student records
   
   **Access:** Staff must submit a completed IT Systems Access Form to their College Registrars for approval and submission to the Office of the Vice-Chancellor. Access is revoked when employment or appointment at the College has concluded.
   
   **Support:** Staff should seek assistance in relation to TAMS access from their College Registrar.
   
   **Training:** College Registrars.

3. **College Academic and Administrative Staff (advanced access)**
   
   **Type:** Advanced
   
   **Level:** Read and write access to student records relating to the staff member’s College, and read-only access to records of other students.
   
   **Access:** This level of access is usually reserved for Registrars, Academic Deans, or other persons responsible for the entry of student data in TAMS. Staff must submit a completed IT Systems Access Form to their Head of College for approval and submission to the Office of the Vice-Chancellor. Access is revoked when employment or appointment at the College has concluded.
   
   **Support:** Registrars and Academic Deans should seek assistance in relation to TAMS access from the Director of Academic Services.
   
   **Training:** OVC Academic Services Officer
4. Office of the Vice-Chancellor (basic access)

Type: OVC

Level: Read and write access to all student records

Access: Office of the Vice-Chancellor staff must submit a completed IT Systems Access Form to the Director of Quality and Standards for approval. Access is revoked when employment or appointment at the Office of the Vice-Chancellor has concluded.

Support: Office of the Vice-Chancellor staff should seek assistance in relation to TAMS access from the Director of Academic Services or the Director of Quality and Standards.

Training: OVC Academic Services Officer.

5. Office of the Vice-Chancellor (administrator access)

Type: Administrator

Level: System administrator access

Access: Office of the Vice-Chancellor staff must submit a completed IT Systems Access Form to the Director of Quality and Standards for review and recommendation to the Vice-Chancellor. System administrator access may only be granted by the Vice-Chancellor. Access is revoked when employment or appointment at the Office of the Vice-Chancellor has concluded.

Support: Office of the Vice-Chancellor staff should seek assistance in relation to TAMS access from the Director of Academic Services or the Director of Quality and Standards.

Training: Director of Academic Services or the Director of Quality and Standards.

6. Suspension of access

6.1 The Vice-Chancellor may authorise the suspension of any user’s access to TAMS, or the reduction of the level of any user’s access to TAMS, for a period of up to 14 days where reasonable evidence exists to indicate that any of the following circumstances apply:

a) the user has breached the University’s Information and Cyber Security Policy or its Code of Practice;

b) the user has breached the University’s Privacy Policy;

c) the user is subject to disciplinary proceedings by the University;

d) the user has repeatedly entered information inaccurately and has been cautioned in writing that further inaccurate entry of information may lead to suspension of access.

6.2 The Vice-Chancellor must inform the user and the user’s Head of College or Supervisor of the suspension or reduction, the reason for the suspension or reduction, and what action is required, if any, for the resumption of access.