IT Management Policy and Procedure		
Code: E2.17	Area: Non-Academic E	
Policy Owner: EMG	Version #: 1.2	Date: 12 Nov 2021
Policy Developer/Reviewer: QAM	Review date: 11 Nov 2024	

VERSION HISTORY

Version	Updated by	Approval Date	Details
1.0	EMG	4 Dec 2019	Document creation
1.1	PRG	9 Jun 2020	Updated to link to the new *Learning Technologies Policy*
1.2	EMG	12 Nov 2021	Unauthorised access tests now biennial.

PURPOSE AND SCOPE

The purpose of this policy is:

- Define the rules that must be observed while using information technology (IT) facilities and services at the Sydney Institute of Traditional Chinese Medicine (SITCM); and
- Outline the security measures in place to safeguard these IT facilities and services.

This policy applies to all SITCM staff and students, contractors, visitors and any other party accessing SITCM IT facilities and services.

1 OVERVIEW

SITCM provides Information Technology (IT) facilities and services for teaching, learning and administration activities. Security measures are in place to protect these facilities and services from damage or loss.

This policy has been informed by the *Higher Education Standards Framework (Threshold Standards) 2015* Section 3.3 Learning Resources and Educational Support, the *Spam Act 2003*, the *Privacy Act 1988* and the *Workplace Surveillance Act 2005*.

2 POLICY

2.1 RESPONSIBILITY

1) The IT Officer is responsible for the general implementation of this policy.
2) The Librarian is responsible for providing staff and students with access to and training for the SITCM library and online databases.
3) The Clinic Manager is responsible for providing staff and students with access to and appropriate training for SmartTCM.

2.2 INFORMATION TECHNOLOGY FACILITIES AND SERVICES

2.2.1 GENERAL

1) SITCM provides all staff and students with certain IT facilities and services for teaching, learning and the related administrative activities.
2) All staff and students have free access to the following on-campus IT facilities and services:
    a. Wi-Fi;
    b. desktop computers with internet access;
    c. printers; and
    d. scanners.
3) All personal data that becomes available to SITCM through its IT facilities and services will be treated in accordance with the *Privacy Policy*.

2.2.2 STUDENTS

1) The IT Officer provides all new students upon their enrolment with the following IT facilities and services (and any necessary training for their use):
    a. A password-protected account on the Moodle learning management system, with SITCM's Moodle training detailed in the *Learning Technologies Policy*;
    b. A password-protected SITCM webmail account; and
    c. A password-protected account on PaperCut, the print management software;
    d. An online discussion group for enrolled students to communicate with each other (students are added upon request), administered by the IT Officer.
2) The Librarian provides all new students with the following IT facilities and services (any any necessary training for their use):
    a. A password-protected SITCM Library account (by their first week of class);
    b. A SITCM account for the online databases EBSCO and Wanfang (by their first week of class); and
    c. A workshop for use of library resources, including online databases (within their first fortnight of class).
3) The Clinic Manager provides a password-protected account for SmartTCM (the clinic record management system) upon a student's enrolment in a clinic placement unit.
    a. SmartTCM training is provided by the Clinic Manager upon commencement of the student's first clinic practicum unit.

2.2.3 STAFF

1) The IT Officer provides all new staff with the following IT facilities and services (and any necessary training for their use):
    a. A password-protected account on Moodle, with SITCM's Moodle training detailed in the *Learning Technologies Policy*;
    b. A password-protected SITCM webmail account;
    c. A password-protected account on PaperCut; and
    d. An online discussion group for staff to communicate with each other (staff are added upon request), administered by the IT Officer.
2) Upon request, the Librarian provides all new staff with the following IT facilities and services (and any necessary training for their use):
    a. A password-protected account for the SITCM Library; and
    b. A SITCM account for EBSCO and Wanfang databases.
3) Operations staff use Dropbox to store and share files.

  a. Dropbox files are grouped into folders, with access determined by position in order to facilitate sharing of relevant information while maintaining appropriate data security.

2.2.4 SITCM WEBSITE

1) Before the start of every semester, the SITCM website is reviewed to ensure all information is accurate and up to date.
2) The IT Officer implements all changes to the website that are identified as necessary during a review.
3) The responsibility for conducting a website review, and notifying the IT Officer of any necessary changes, is held as follows:
   a. The Dean: for all website information related to Higher Education courses.
   b. The Associate Dean: for all website information related to VET courses.
   c. The Quality Assurance Manager: for all other website information.

2.3 ACCEPTABLE USE OF IT FACILITIES AND SERVICES

1) All users of SITCM IT facilities and services (including students, staff, contractors, visitors and any other party accessing SITCM IT facilities and services generally) must observe the conditions of use as outlined in this policy.
2) Users are responsible for all activities that originate from their account, and for the protection of their account passwords.
3) Users may use SITCM's IT facilities and services:
   a. For purposes related to work or study at SITCM; and
   b. For incidental personal use, such as checking emails and news sites.
4) Users must not use SITCM's IT facilities and services to create, access, transmit or otherwise deal with content which is illegal or which a reasonable person would regard as abusive, offensive, defamatory, obscene, indecent, harassing, intimidating, harmful or distressing and which may expose SITCM to legal liability. This would include (but is not limited to):
   a. Obscenity of any kind;
   b. Unauthorised access to any facilities, including hacking and the deliberate spreading of viruses or malicious code;
   c. Reproducing, distribution, transmission or otherwise dealing with copyright material or other intellectual property in breach of the intellectual property rights of any person(s);
   d. Unauthorised commercial activities; and
   e. Any illegal activity.
5) Users should be aware that some third party applications licensed to SITCM have their own terms and conditions which may apply over and above this policy.
6) If a user accesses SITCM IT facilities from a personally owned device, that user has a responsibility to ensure that their personal device is free of malware by:
   a. Password-protecting their device(s) and turning on automatic updates; and
   b. Installing appropriate security software on their device(s).
7) A staff member's failure to comply with this section may constitute a breach of the *Staff Manual* and and incur consequences as outlined in the *Staff Misconduct Policy and Procedure*.
8) A student's failure to comply with this section may constitute a breach of the *Student Manual* and incur consequences as outlined in the *Non-Academic Misconduct Policy and Procedure*.

2.3.1 SECURITY CULTURE

1) To ensure users are familiar with their obligations, this policy is accessible:
   a. On the SITCM website; and
   b. In both the staff and student sections on Moodle.
2) Students are directed to this policy in each orientation.
3) Staff are directed to this policy in each induction.
4) Information sheets outlining user responsibilities are displayed on campus.

2.4 CYBER SECURITY

2.4.1 INTERNAL MEASURES

SITCM has internal servers for SmartTCM, the Library and shared office files. SITCM's on-campus computers and internal servers have the following security protections:

1) Antivirus and firewall software which runs in real-time and performs weekly scans;
2) Internal servers are:
   (i) Automatically backed up daily to a mirror system;
   (ii) Manually backed up twice a year to an external storage drive. An additional external backup is put into a bank safety deposit box.
3) Automatic updates are turned on for all operating systems and software on campus computers;
4) All publicly accessible computers are checked for unnecessary or unusual software weekly; and
5) All computers that are not for public use are password-protected.

2.4.2 EXTERNAL MEASURES

SITCM's website, Moodle and shared Dropbox files are stored on external servers, which have the following protections:

1) SITCM uses the security system Wordfence as an endpoint firewall and malware scanner, and to block websites which are criminal and/or pornographic;
2) SITCM's IT Officer blocks websites which are criminal and/or pornographic from internal access; and
3) SITCM performs an external backup twice a year to an external storage drive. An additional external backup is put into a bank safety deposit box.

2.4.3 UNAUTHORISED ACCESS TESTS

1) SITCM engages an independent IT expert biennially to undertake unauthorised access tests (UATs) for the following IT systems:
   a. Moodle (externally accessible).
   b. The SITCM website (externally accessible).
   c. SmartTCM (not externally accessible).
   d. The internal SITCM server (not externally accessible).
2) The UAT results, together with any corrective actions, are communicated via the IT Officer and reported to the Executive Management Group (EMG).

2.4.4 IT INCIDENTS

1) An 'IT incident' refers to any suspected or confirmed IT security breach.
2) An IT incident may be determined to be a critical incident in accordance with the *Critical Incident Policy and Procedure*.
3) An IT incident will be determined to be an 'eligible data breach' if:

   a. There is unauthorised access to, disclosure of or loss of personal information held by SITCM which is likely to result in serious harm to any individuals to whom the information relates, and
   b. SITCM has been unable to prevent the likely risk of serious harm with remedial action.

4) All IT incidents should be reported to the IT Officer immediately via the reception desk, on (02) 9212 1968.
5) Upon notification of an IT incident, the IT Officer will follow the procedure outlined in Section 3.1 (IT Incident Procedures).

3 PROCEDURES

3.1 IT INCIDENT PROCEDURES

1) A suspected or confirmed IT security breach occurs.
2) The IT Officer becomes aware of the incident.
3) The IT Officer reviews all relevant logs for security breaches.
4) If a security breach is found to not have occurred, the IT Officer will notify the party who reported the incident as soon as possible.
5) If a security breach is found to have occurred, the IT Officer will:
   a. Notify all affected users as soon as possible.
   b. Oversee all remedial action to mitigate the breach and prevent reoccurrence.
      i. If data is lost, backups will be used.
      ii. Damaged or destroyed IT equipment will be replaced as soon as possible, and in most cases within one (1) working day.
   c. Report the breach to the Executive Management Group.
6) If a security breach is determined to be an eligible data breach, the IT Officer will provide to the Australian Information Commissioner, and all individuals affected by the breach, a statement containing the following information:
   a. SITCM’s name and contact details;
   b. A description of the eligible data breach;
   c. The kind or kinds of information concerned; and
   d. Recommendations on what steps the affected parties should take in response to the data breach.

   The statement will also be published on the SITCM website.
7) If a security breach is determined to be a critical incident, the IT Officer will assume the responsibilities of the Coordinator and follow the procedure outlined in the *Critical Incident Policy and Procedure*.

4 RELATED POLICIES AND OTHER DOCUMENTATION

1) Higher Education Standards Framework (Threshold Standards) 2015.
2) Spam Act 2003.
3) Privacy Act 1988.
4) Workplace Surveillance Act 2005.
5) E2.16 Privacy Policy.
6) A1.04 Learning Technologies Policy.
7) Australian Information Commissioner Act 2010.
8) E2.20 Critical Incident Policy and Procedure.