Information and Communications Technology Security procedure

Section 1 - Preamble

(1) This Procedure is effective from 18 January 2018.

Section 2 - Purpose

(2) The Procedure documents the university's ICT security measures.

Section 3 - Scope

(3) This Procedure applies throughout the university.

Section 4 - Policy

(4) This Procedure is pursuant to the Information and Communications Technology Security policy.

Section 5 - Procedure

Security Standards

(5) The IT Security Manager will develop information and communications technology (ICT) security standards and maintain them according to industry-wide standards.

(6) The IT Security Manager will undertake an ICT security risk assessment annually, and report to the Chief Digital Officer and the Director, ICT Infrastructure Services on ICT security incidents, current security concerns and service improvement needs for the coming year.

(7) Staff members with responsibilities for managing or supporting ICT facilities, services and materials will ensure that:

a. each device or application is configured and managed according to the ICT security standards developed by the eSolutions
b. where confidential information from production systems is used in development or testing environments, the ICT security requirements for the production system will apply to the development or testing systems.

(8) Staff members with responsibilities for managing ICT facilities, services and materials used for financial transactions will ensure that digital certificates and encryption are used for the transfer and storage of payment information, such as account numbers and credit card information.

Connecting to university facilities

(9) The Chief Digital Officer and the Director, ICT Infrastructure Services will determine which staff members can authorise access to the operating systems or security systems of any ICT facility, service or material connected to the Deakin University network.

(10) Staff members will ensure that new connections of, or changes to, any ICT facility, service or material connected to the Deakin University network are managed and approved according to the Deakin University ICT change management process, facilitated by the eSolutions.

(11) Staff members will ensure that any ICT facilities, services or materials installed or configured to protect Deakin University information are of a type and standard approved by the IT Security Manager prior to being implemented on any Deakin University-owned or managed ICT facility or service.

(12) Staff members will ensure that non-Deakin University owned ICT devices, excluding personal computing devices such as laptops or personal digital assistants (PDAs), connected to the Deakin University network abide by the same ICT security standards and requirements as those applied to the Deakin University-owned assets.

Usernames

(13) Deakin University usernames in the Deakin University directory service will not be reused within 12 months, unless for use by the same staff member as previously assigned that Deakin University username.

Passwords

(14) Depending on the class of user, the following minimum requirements apply to user passwords where technically possible:

a. Students
    i. be at least eight characters long
    ii. contain a combination of at least three of the following four character types:
        - lowercase letters
        - uppercase letters
        - numbers
        - other symbols
    iii. no password ageing
    iv. password history: new passwords must be different from the previous five passwords
b. Staff/Visitor Normal Account
    i. be at least eight characters long
    ii. contain a combination of at least three of the following four character types:
        - lowercase letters
        - uppercase letters
        - numbers
        - other symbols
    iii. changed at least every 180 days. Accounts with passwords older than this will be locked
    iv. minimum age: A new password cannot be changed for at least 1 day unless the password change was a reset performed by eSolutions
    v. password history: new passwords must be different from the previous five passwords
c. Non expiring password staff. Users may request to be placed in this class where regular password changes are

not required, the IT Security Manager is responsible for reviewing any applications. The following password controls apply:

i. be at least 12 characters long
ii. contain a combination of at least three of the following character types:
    - lowercase letters
    - uppercase letters
    - numbers
    - other symbols
iii. password history: new passwords must be different from the previous five passwords

d. Service Account. These are accounts that are not associated with an individual, but with a device, service, interface or other technical reason. The requirements for these passwords are to be maintained in a standard managed by the Cybersecurity team of eSolutions. Under no circumstances can these accounts be used by a person for interactive login except for support purposes.

(15) Vendor-supplied default passwords must be changed before or immediately after any ICT facility, service or material is connected to the Deakin University network.

(16) Where access is granted to vendors, partners, consultants and other users who are not staff or students of Deakin University, this access will be reviewed at least annually to ensure that the access and the privileges granted are still applicable.

(17) Where available, mechanisms to detect and prevent multiple failed login attempts to a user account must be enabled and configured in one of two ways. After multiple failed login attempts, an account:

a. is automatically locked; or
b. has delays between attempts of at least 15 minutes imposed.

Monitoring, patching and auditing

(18) The Executive Director, ICT Infrastructure Services will monitor for security breaches as specified in the Information and Communications Technology Acceptable Use procedure.

(19) Excluding personal computing devices, logs of system, application and ICT user activity that are generated automatically must be kept for a minimum of two years. Such logs will contain both non-identifying and identifying data, which may include Deakin University username, computer name and location, time of activity and screens accessed.

(20) All changes to production data must be made via an application or system interface that automatically logs activity or via standard batch jobs. Where this is not possible, changes must be made and tracked via the ICT change management process, with the details of the change record kept for a minimum of two years.

(21) All changes to logging mechanisms that affect the ability to monitor or audit system, application and ICT user activity must be authorised through the Deakin University ICT change management process and must be able to be audited.

Patch management

(22) All critical and key patches shall be applied on a regular and recurrent cycle after thorough testing.

(23) Appropriate ICT staff must monitor all applicable vendor informational sites on a regular basis to stay aware of when operating system and application patches are made available.

(24) Patches must be tested in an appropriate development/test environment, when available, to understand the impact of deploying the patch in the production environment.

(25) Prior to production deployment, a back out plan must be in place to roll back changes in the event the patch causes issues with the production environment.

(26) Prior to production deployment, the Change Manager must approve the change to the production environment. A communication plan must be established before the change occurs.

(27) If a patch cannot be implemented in the production environment, then an exception request must be filed and approved by Cyber Security in ServiceNow, and it must document why the patch cannot be implemented in the production environment and must enumerate mitigating controls that will be put in place to reduce the risk to the system and data given that the patch cannot be applied.

User access management

(28) Privileged access is only granted to authorised individuals. Users with privileged access have a responsibility to protect the confidentiality of any information they encounter while performing their duties. Staff requiring access to a system must have a genuine business requirement, verified by their supervisor, to access the system in a privileged capacity. All individuals who are granted privileged access must have appropriate training for the relevant systems.

(29) Privileged access is only to be used for purposes for which it was granted. Privileged access does not imply authorisation to undertake activities that are enabled via the privileged access but are not within the purposes for which it was granted.

(30) A bi-annual (every six months) privileged user account audit will be performed by the system administrators/Cyber Security to determine that assigned privileged user access is appropriate.

(31) Privileged access applies to a particular period of time and includes only specific tasks. Time periods are based on the required tasks; the time period may be brief, such as one-time access, intermittent access, or longer. Privileged access will end at the close of the time period granted. Privileged access will be reviewed, re-verified, and authorised by the user, their manager, and the applicable data owner every time the user's job duties change, or bi-annually.

(32) Individuals with privileged access have an obligation to keep informed of procedures, business practices, policies and operational guidelines pertaining to the activities of their unit.

(33) Individuals with privileged access must be aware of, and follow, change control processes before making changes to production systems.

(34) Individuals with privileged access must respect the privacy of system users, respect the integrity of systems and related physical resources, and comply with relevant laws and regulations.

(35) Individuals with privileged access shall take necessary precautions to protect the confidentiality of information encountered in the performance of their duties.

Awareness and education

(36) The IT Security Manager will provide an ICT security awareness program for ICT users, including information about their obligations in relation to:

a. access to and use of ICT facilities, services and materials
b. reporting of ICT security incidents, breaches or concerns.

(37) Managers will ensure that their staff members, including consultants and contractors, are aware of and educated

about ICT security, including the ICT security requirements appropriate to their role.

(38) Staff must comply with the ICT security requirements required by their role, including but not limited to:

a. compliance with ICT security policy, procedure and standards
b. ensuring that their computers are not left unattended and logged into the Deakin University network, without first activating a screen saver with password protection.

External parties

(39) The IT Security Manager will ensure that all external parties with connectivity to the Deakin University ICT network have a formal agreement in place defining access provisions, which will be commensurate with Deakin University measures, to protect unauthorised or improper use of the Deakin University ICT facilities, services or materials.

(40) Staff will obtain approval in writing from the IT Security Manager before disclosing outside of the University any specific matter regarding security controls that are in use or the way in which these controls are implemented.

Exemptions

(41) Where an exemption from the ICT security policy, procedure or standards is required, approval in writing must be obtained from the Director, ICT Infrastructure Services and the information owner where applicable.

Breaches

(42) ICT Users must immediately report any suspected or perceived breach of the Information and Communications Technology Security policy, procedure or standards to the Director, ICT Infrastructure Services or nominee via the IT Service Desk.

(43) The Director, ICT Infrastructure Services may deny or restrict an ICT User's access to the University's ICT facilities, services and materials, and/or remove or disable any data, service or device from the ICT facilities, as a result of violations of the Information and Communications Technology Security policy, procedure or standards pending further investigation, disciplinary and/or judicial action.

(44) If the Chief Digital Officer and the Director, ICT Infrastructure Services are satisfied, based on investigations, that a violation of policy and/or law has occurred, they will undertake disciplinary action in accordance with that outlined in the Information and Communications Technology Acceptable Use procedure.

Section 6 - Definitions

(45) For the purpose of this Procedure:

a. data: as defined in the Information and Communications Technology Security policy.
b. Deakin Directory Service: as defined in the Information and Communications Technology Security policy.
c. information: as defined in the Information and Communications Technology Security policy.
d. information and communications technology (ICT) facilities: as defined in the Information and Communications Technology Security policy.
e. information and communications technology (ICT) services and Materials: as defined in the Information and Communications Technology Security policy.
f. information and communications technology (ICT) user: as defined in the Information and Communications Technology Security policy.

g. information owner: the person who is responsible and accountable for information and records management for an organisational unit of Deakin University, and who will ensure appropriate storage, access, use, distribution and disposal of information and records.

Status and Details

Status	Current
Effective Date	18th January 2018
Review Date	18th January 2021
Approval Authority	Vice-Chancellor
Approval Date	15th January 2018
Expiry Date	To Be Advised
Implementation Officer	Craig Warren Executive Director, ICT Infrastructure Services +61 3 52278840
Author	Craig Warren Executive Director, ICT Infrastructure Services +61 3 52278840
Enquiries Contact	eSolutions +61 3 52278773