Information Security Procedure

Section 1 - Policy Statement

(1) This Procedure is governed by the Information Security Policy.

Section 2 - Scope

(2) This Procedure is applicable to all members of the University community, staff, student, visitors, volunteers and contractors.

Section 3 - Access Control

(3) All users of the University's Information Environment must be authorised to access the appropriate systems and information resources. Access is managed and monitored in accordance with University policy. The elements involved in managing and monitoring access include identification, authorisation and authentication.

Identification

(4) All members of the University community – staff, students and authorised visitors - are assigned a unique User Identifier (ID) to enable access to the ACU Information Environment and Resources.

(5) User IDs must not be shared. If deemed necessary for business or operational reasons, approval must be obtained from the Chief Information and Digital Officer. Information Technology (IT) must maintain a documented record of shared user IDs.

(6) Users are responsible for safeguarding their individual IDs and are accountable for all transactions recorded against their individual ID.

(7) The Chief Information and Digital Officer or delegate, may approve the temporary creation and use of generic identifiers, in particular circumstances, such as testing and training.

Authorisation

(8) Systems Owners are responsible for granting appropriate levels of access privileges, to enable members of the University community to undertake their respective duties.

(9) Systems Owners are responsible for the recording and regular review – at least every six months - of Authorisation levels for all systems within the System Owner’s area of responsibility. Any irregularities should be addressed as a matter of priority.

Authentication

(10) Access to the University Information Environment and all University systems that require Authentication will only be granted through the use of a valid set of ACU assigned credentials.

Password / Passphrase Standards

(11) Passwords are used for various purposes at ACU. Some of the more common uses include user (logon accounts, web application accounts, email accounts, screen saver protection, voicemail password, and to access other services).

(12) For the purposes of this Procedure, Passwords and Passphrases are subject to the same standards set out below. The use of the term Password/s in this Procedure also includes Passphrase/s.

Passwords Composition Guidelines

(13) Passwords must be a minimum of eight alphanumeric characters in length.

(14) Passwords must include at least (one) 1 upper and (one) 1 (lower case character (e.g., a-z, A-Z).

(15) Consider the use of punctuation marks, numeric and special characters in a password where this functionality is available. e.g., (0-9, !@#$%^&*()_+|~-=\`{}[]:";'< />?,./)

(16) Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Please do not use any of these examples as passwords!

(17) Passwords must not contain:

a. the User ID in any form (as-is, reversed, capitalised, doubled, etc.);
b. the user's first or last name in any form;
c. the name of a person, pet, place or inanimate object;
d. dictionary words (including foreign and technical dictionaries);
e. simple patterns of letters on keyboards;
f. words related to the University or work project;
g. vehicle registration plate numbers;
h. date of birth;
i. telephone numbers; or
j. address details.

Password Management

(18) Passwords:

a. all initial and reset passwords must be generated randomly;
b. on receipt of an initial or reset password, users must immediately change the password;
c. all user-level passwords used to access general information services such as, desktop computer, email, the Internet, etc. must be changed every 40 (forty) days. This requirement may be enforced;
d. passwords should never be written down and left in clear view near workstations or insecure locations;
e. passwords should not be stored in plain text;
f. passwords must never be given to anyone even if requested via phone, email or in person. Failure to comply may result in disciplinary action by the University;
g. passwords should not be shared with anyone, including executive officers or administrative assistants;
h. passwords used for University systems should not be reused for other systems or services; and
i. passwords must not be inserted into email messages or other forms of electronic communication without strong

encryption.

(19) Passwords believed to have been compromised, must be changed immediately and the matter referred to a supervisor and the IT Security Officer.

Use and Control of Privileged User Access

(20) For some system and application administrative tasks system administrators and other authorised staff require deeper levels of access to systems and applications in order for them to undertake their duties. Privileged users may include systems, application and database administrators, and their supervisors. It should be noted that in some instances, privileged user access could potentially permit access to an entire system.

a. Privilege User Access should be restricted to a minimum, and strong authentication protocols must be used particularly if the privilege level provides access to information classified as Internal Restricted or Internal Protected.
b. Systems Owners are responsible for ensuring that privilege level is the minimum needed for the individual to undertake their assigned tasks.
c. Systems Owners are responsible for the approval; recording and regular review - at least every six months - of staff with Privileged User Access levels. Any irregularities should be addressed as a matter of priority.
d. System Owners are responsible for approving Contractors and third party access. These parties must comply with the requirements of this Procedure.
e. IT must hold a record of all roles and individuals with Privilege.
f. User Access.
g. Any irregular activity or identified security incidents must be reported to University IT security. Remediation is coordinated from the Office of the Chief Information and Digital Officer through the IT Security Officer or an authorised delegate, as appropriate.

Section 4 - Digital Messaging

(21) The following is subject to the provision of the ICT Acceptable Use Policy. This section sets out the protocol for using Digital Messaging in all its forms, including the security aspects of information transfer within the University and with any external entities.

(22) The Procedure applies to all forms of information transfer, including emails and attachments, blog entries, wikis, voicemail, text messaging, social media and any other forms of digital communications.

Permissible Use

(23) The use of ACU messaging services must be related to the work of the University, including learning and teaching, research, community engagement, administration and / or other associated official activities of the University. Incidental and occasional personal use of messaging services are permissible provided that in each case the personal use is moderate in time and does not incur significant cost for the University.

Prohibited Use

(24) The University's messaging services must not be used for:

a. any purpose(s) that is restricted by University regulations and / or policy, and / or any applicable State and / or Federal regulations or laws, including those relating to copyright, freedom of information, breach of confidentiality, privacy and anti-discrimination;

b. personal monetary gain or for commercial purposes not directly related to University business;
c. sending copies of electronic materials in violation of copyright laws or the inclusion of the work of others into electronic communications in violation of copyright laws;
d. creating and exchanging messages that can be interpreted as offensive, harassing, obscene, racist, sexist, ageist, pornographic, intimidating or threatening as defined by the Code of Conduct for Staff, the Discrimination and Harassment Policy, and the Student Conduct Policy;
e. sending messages that interfere with the ability of other users to conduct University business;
f. sending unsolicited messages to groups or individuals, irrespective of the medium of transmission;
g. sending Chain Letters, sending messages to groups or University distribution lists without proper authorisation;
h. disseminating confidential information about the University;
i. knowingly causing or taking action likely to cause interference with or disruption to any computer, computer network, information service, equipment or any user thereof; or
j. disseminating personal contact information of staff or students without their written consent.

Section 5 - Operations Management

Operating Procedures

(25) The following sets out the operating procedures to ensure the protection of information and the secure operations of networks and supporting processing facilities.

Documented Operating Procedures

(26) Responsibilities and procedures for the management and operation of all information-processing facilities e.g. Data Centres must be established. This includes the development of appropriate operating Procedures. Operating Procedures must be documented, maintained, and made available on request.

Segregation of Duties

(27) Duties and areas of responsibility must be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of University information assets.

Separation of Operating Environments

(28) Development, test, and production environments must be separated, to reduce the risks of unauthorised access or changes to the production system.

Controls against Malicious Code (including viruses)

(29) To protect the integrity of software and information assets, IT managed equipment must be maintained with the most recent anti-virus signature updates via a centrally managed console. The updates must be automatically distributed, with no manual intervention required by the end user or IT staff.

(30) Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures must be implemented.

Backup and Restore

(31) To maintain the integrity and availability of information and information processing facilities, routine procedures must be established to implement back-up processes across all IT managed equipment:

a. backup processes must be thoroughly documented and tested;
b. routine restores of data must be performed to confirm the restore capability.

Network Security Management

(32) Networks must be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

(33) The Chief Information and Digital Officer is responsible for ensuring security features, service levels and management requirements of all network services are identified and included in any network services agreement, whether these services are provided in-house or outsourced.

Media Handling

(34) Appropriate operating procedures must be established to protect documents, computer media, input / output data and system documentation from unauthorised disclosure, modification, removal, and destruction:

a. all media including removable media must be controlled and physically protected by the support teams;
b. where Internal Restricted and Internal Protected information is stored on removable media, appropriate controls such as password protection and encryption must be applied at a minimum to protect the information.

Monitoring

(35) Procedures for monitoring use of information processing facilities must be established and the results of the monitoring activities reviewed regularly:

a. the level of monitoring required must be determined through risk assessment;
b. any monitoring must comply with all relevant legal requirements applicable to the monitoring activity.

Protection of Log Information

(36) Logging facilities and log information must be protected against tampering and unauthorised access:

a. controls must aim to protect against unauthorised changes and operational problems with the logging facility;
b. logging information must be made available for audit as required;
c. system administrator and system operator activities must be logged and must include:
    i. the time at which an event (success or failure) occurred;
    ii. information about the event (e.g. files handled) or failure (e.g. error occurred and corrective action taken);
    iii. the account and administrator or operator details involved;
    iv. details of the processes involved.
d. system administrator and operator logs must be reviewed on a regular basis. Any abnormalities must be reported to the IT Security Officer for further investigations;
e. faults must be logged, analysed, and appropriate action taken;
f. faults reported by users or by system programs related to problems with information processing or communications systems must be logged. There must be clear rules for handling reported faults including:
    i. review of fault logs to ensure that faults have been satisfactorily resolved; and
    ii. review of corrective measures to ensure that controls have not been compromised, and that the action taken is fully authorised.

Clock Synchronisation

(37) The clocks of all relevant information processing systems within the University must be synchronised with the au.pool.ntp.org time source.

Section 6 - Physical and Environmental Security Data Centres

Physical Security Perimeter

(38) ACU managed information processing facilities must be physically separated from those managed by third parties.

(39) Critical or sensitive information processing facilities must be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They must be physically protected from unauthorised access, damage, and interference.

(40) A staffed reception area or other means to control physical access to the site or building must be in place; access to sites and buildings must be restricted to authorised personnel.

Physical Entry Controls

(41) Secure areas must be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

(42) The date and time of entry and departure of visitors must be recorded, and all visitors must be supervised unless their access has been previously approved; they must only be granted access for specific, authorised purposes and must be issued with instructions on the security requirements of the area and on emergency procedures.

(43) Access to areas where sensitive information is processed or stored must be controlled and restricted to authorised persons only; authentication controls, e.g. access control card plus PIN, must be used to authorise and validate all access; an audit trail of all access must be securely maintained.

(44) All staff, contractors, third party users and visitors must be required to wear some form of visible identification and must immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification.

(45) Third party support service personnel must be granted restricted access to secure areas or sensitive information processing facilities only when required; this access must be authorised and monitored.

(46) Access rights to secure areas must be regularly reviewed and updated, and revoked when necessary.

(47) Photographic, video, audio or other recording equipment, such as cameras in mobile devices, must not be allowed, unless authorised.

Equipment Security

(48) Equipment must be sited to minimise unnecessary access to work areas.

(49) Items requiring special protection must be isolated to reduce the general level of protection required.

(50) Controls must be adopted to minimise the risk of potential physical threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications

interference, electromagnetic radiation and vandalism.

(51) Guidelines for eating, drinking, and smoking in proximity to information processing facilities must be established.

(52) Environmental conditions, such as temperature and humidity, must be monitored for conditions, which could adversely affect the operation of information processing facilities.

(53) Lightning protection must be applied to all buildings and lightning protection filters must be fitted to all incoming power and communications lines.

Supporting Utilities

(54) Equipment must be protected from power failures and other disruptions caused by failures in supporting utilities.

(55) All supporting utilities, such as electricity, water supply, sewage, heating / ventilation, and air conditioning must be adequate for the systems they are supporting. Support utilities must be regularly inspected and tested as appropriate to ensure their proper functioning and to reduce any risk from malfunction or failure.

(56) A suitable electrical supply must be provided that conforms to the equipment manufacturer's specifications.

(57) Wherever possible, multiple feeds with diverse physical paths should be installed.

Secure Disposal or Re-use of Equipment

(58) All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

(59) Devices containing sensitive information must be physically destroyed or the information must be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

Section 7 - System Acquisition, Development and Maintenance

Security Requirements of Information Systems

(60) The requirements set out below are in place to ensure that information security forms an integral part of information systems across the entire lifecycle. These requirements apply to the acquisition of new information systems, as well as upgrades or enhancements to existing systems, including systems that provide services over public networks:

a. system documentation must address security;
b. authentication processes must conform to ACU standards;
c. transaction logging and monitoring must be accessible;
d. access to program source code must be restricted;
e. information about technical vulnerabilities must be obtained from authoritative sources such as AUSCert; and
f. patch management processes must be established and embedded within Change control processes.

Section 8 - Supplier Relationships

Access to Information Assets by External Service Providers

(61) To mitigate the risks associated with access to ACU information resources by external service providers, security controls should address processes and procedures across all participating parties. The controls should:

a. identify and document the type of supplier, e.g. IT services, financial services, infrastructure services etc.;
b. include a lifecycle management approach;
c. define the types of information access that different suppliers will be permitted, and monitor and control access. Processes should take account of supplier agreements and disclaimers;
d. define the minimum information security requirements for each type of access, to be used as the basis for individual supplier agreements, based on the University's business needs and risk assessment;
e. clearly set out the information security obligations of each party, including sub-contractors;
f. detail change management processes and procedures;
g. detail the handling procedures for incidents, defect resolution, recovery, resiliency and associated contingencies;
h. detail conflict resolution processes;
i. define the support arrangements, rules of engagement and contact details;
j. clearly specify the management processes for the transition of information, information processing facilities and related activities to ensure information security throughout the transition period; and
k. make provision for security audit checks, to ensure compliance with University requirements.

Section 9 - Information Security Incident Management

Management of Information Security Incidents and Improvements

(62) Management responsibilities, plans and processes should be established to ensure a rapid, effective and orderly response to information security incidents. Established plans should be communicated widely within the University. Processes should include:

a. procedures for monitoring, detecting, analysing and reporting of information security incidents;
b. procedures for logging incident management activities – Incident Report;
c. procedures for handling forensic evidence;
d. procedures for assessment of and decisions on information security vulnerabilities;
e. authorisation of delegated roles for handling of information security incidents. e.g. contact with authorities; and
f. procedures for the provision of feedback.

Section 10 - Information Security Aspects of Business Continuity Management

Information Security Continuity

(63) This section sets out the requirements for managing information security in adverse situations, e.g. a crisis or

disaster:

a. information security requirements must be considered during the planning of business continuity and disaster recovery;
b. documentation must be maintained and clearly outline the supporting processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation;
c. a management structure must be established to prepare for, mitigate and respond to a disruptive event;
d. incident response teams should be in place, with the necessary responsibility, authority and competence to manage an incident and maintain information security; and
e. plans should be tested to ensure processes and procedures are operational and effective.

Section 11 - Compliance

Compliance With Legal and Contractual Requirements

(64) All relevant legislative statutory, regulatory and contractual requirements for information systems, should be explicitly identified, documented and maintained. These should include:

a. clear definitions of the legal use of software and information systems, to ensure copyright is not violated;
b. maintenance of appropriate asset registers;
c. records and evidence of ownership of licences, master media (disks) manuals etc.;
d. controls to ensure maximum number of users – permitted within the licence - are not exceeded;
e. compliance with terms and conditions for software and information obtained from public networks;
f. procedures for the retention, storage, handling and disposal of records and information;
g. maintenance of a register of key information sources; and
h. technical compliance reviews of operational systems e.g. penetration testing and vulnerability assessments.

Section 12 - Review of this Procedure

(65) As an extension of the Information Security Policy, this Procedure will be reviewed every three (3) years from the date of approval, or more frequently if appropriate.

(66) Unless otherwise indicated, this Procedure will still apply beyond the review date.

Status and Details

Status	Current
Effective Date	28th February 2024
Review Date	30th April 2024
Approval Authority	Vice-Chancellor and President
Approval Date	28th February 2024
Expiry Date	Not Applicable
Responsible Executive	Russell Parker Chief Information and Digital Officer
Responsible Manager	Russell Parker Chief Information and Digital Officer
Enquiries Contact	Information Technology