IT SECURITY PROCEDURES

These Procedures are made under the IT Acceptable Use and Security Policy, to support the principles enunciated in that Policy by:

a) Establishing clear responsibilities of University IT Custodians, including Information Technology & Digital Services.
b) Establishing requirements for technical controls to protect the security of information assets.

Definitions

Change Advisory Board (CAB) is the governance body operated by ITDS for reviewing and approving changes to production University IT environments.

Technical Design Board (TDB) is the governance body operated by ITDS for reviewing and approving new University IT and major changes and integrations to existing University IT.

University data means data generated by or on behalf of the University or otherwise within the University's custody.

All other defined terms have the same definitions as used in the IT Acceptable Use and Security Policy.

1. IT Security Principles

Responsibility: University IT Custodians

a) The University recognises information assets are critical for supporting the mission of the institution, and is committed to protecting them from loss, misuse and harm through judicious investment in people, process and technologies, regardless of whether IT assets are managed and residing on University premises or held in trust and managed by third parties or business partners.
b) The University's Chief Information Officer (CIO) is responsible for the oversight of all activities relating to planning, implementation, and operations of security controls.
c) The University shall maintain a Cyber Security Framework (CSF) aligned to ISO/IEC 27001 standard and aim to continuously enhance security posture based on business needs, risks, and regulatory requirements.
d) The University shall maintain a Cyber Security Strategy aimed at prioritising initiatives aimed at risk mitigation and compliance with regulations and other contractual obligations.
e) The University shall establish a governance structure that will have an oversight of the CSF operations, including review and endorsement of security standards and procedures as well as monitoring and enhancement of the framework.
f) All Custodians, including ITDS, must comply with the security standards and procedures defined in the CSF unless written exemption has been granted by the CIO.
g) Standards must be communicated and made widely available and promulgated to all IT Custodians.

2. Personnel Security and Cyber Resilient Culture

Responsibility: Business Owners, University IT Custodians

a) Business owners of University IT systems are responsible for ensuring that background verification checks on all candidates for employment, contractors, and third party users are carried out at a level that is proportional to classification of the information to be accessed and perceived associated risks. Screening may include, but not limited to: reference check, validation of claimed academic and professional qualifications, independent identity validation, national police check, and national security clearance.

b) The University is committed to cultivating a secure and cyber resilient culture founded on each user "doing the right thing" to protect the security of university information assets. To this end, the University shall develop and make available security awareness and training materials to all users.
c) Where security training is deemed mandatory, incentives and penalties will be devised to help ensure full compliance.

3. Asset Management & Posture Assessment

Responsibility: University IT Custodians

a) All University IT assets (any system or a device owned or managed by the University, service that connects to the University network, and third-party services holding University data) should be identified, inventoried, and documented in the University's IT asset management database with key metadata including, but not limited to, business owner, nominated custodian, and maximum data sensitivity.
b) The University should ensure that all hardware and/or software meet the University's security requirements before being deployed to the University's environments.
c) All University IT assets must undergo periodic security risk assessment including penetration testing in accordance with a schedule determined by the Chief Information Security Officer (CISO).

4. Development, Acquisition and Change

Responsibility: University IT Custodians

a) Acquisition or development of University IT, including implementation of commercial off-the-shelf (COTS) solutions, purchase of hardware and software, development of an IT application, use of third-party hosted ("cloud" or "software as a service (SaaS)") solutions must be done in such a way that it:
    i. Meets business requirements.
    ii. Aligns with current University architectural principles.
    iii. Integrates with and does not duplicate existing investments.
    iv. Documents any risks to the University and ensures that it is not exposed to unacceptable levels of information security risk.
    v. Is compliant with other University policies (including but not limited to the Contracts and Agreements Policy, Strategic Procurement Procedures, and the Disability Action Plan) as well as laws and regulations.
b) All new University IT must be reviewed and endorsed by the Technical Design Board (TDB) for their alignment to architectural principles unless exemption has been granted.
c) The University will maintain a change management process and a change advisory board (CAB) that will ensure all changes affecting production systems have been tested and communicated to reduce the risk of disruptions.
d) University IT that includes presence on the public internet that will be branded as, and/or recognised as, part of the University must undergo a review and approval by Marketing and Recruitment.
e) Where a new University IT is being developed, either using internal or external sources, a secure development and coding standard must be developed and utilised to ensure the product remains free from security vulnerabilities.
f) Where University data is to be hosted or stored by a third-party vendor, a security due-diligence procedures as defined in the CSF must be followed.
g) Critical business applications should have a separate production, user acceptance testing (UAT) and development environment to ensure only tested and authorised code is migrated to production environment.

h) Developers should not have the ability to modify application program code or configurations in production or UAT environments; a non-developer staff should be responsible for migrating code between environments.
i) Sensitive data should not be used in non-production environments; dummy or scrambled data, or de-identified/masked data should be used instead where it is practical to do so.
j) Internally developed and commercial-off-the-shelf (COTS) applications configured and hosted on-premises must undergo a penetration testing before go-live and on a periodic basis as determined by risk.

5. Information Classification and Protection

Responsibility: University IT Custodians

a) The University will maintain a framework for consistently classifying information based on sensitivity, as well as a set of standards for applying controls to protect the security of information assets at levels commensurate with the value and sensitivity of information being protected.
b) All University assets and information should be classified according to the University's information classification standard and appropriate level of protection must be implemented for each information asset commensurate to its sensitivity level.
c) Business owners are responsible for assigning the appropriate classification to information assets and work with the IT custodian and assist users to ensure required security controls are implemented.
d) ITDS is responsible for certifying University IT that are fit to store and process data with sensitive classification.

6. Third Party and Supplier Risk Management

Responsibility: University IT Custodians

a) Third parties who will store and/or process University data or supply IT equipment to the University must undergo a security due diligence process via ITDS security function to ensure that their services and/or products comply with the University's security requirements and/or mitigate security risks to a level that is commensurate with the University's risk appetite.
b) Third party risk assessment must be re-performed on a periodic basis or at a time of contract renewal to help ensure that security posture and security risks associated with the third party has not substantially changed.
c) The level of required vetting should be commensurate with the level of risk as determined by such factors as the sensitivity and importance of data being stored or processed, number of users, and combine examination of factors including but not limited to:
    i. Services Organization Control (SOC) 2 Type II (based on SSAE16, 18 standard)
    ii. ISO/IEC 27001 information security management system certification
    iii. Payment Card Industry Data Security Standard (PCI DSS) certification
    iv. Information Security Registered Assessors Program (IRAP) certificate
    v. Evidence of regular independent security testing
    vi. Completion of a security controls checklist
    vii. Independent security testing by the University

7. Identity and Access Management

Responsibility: University IT Custodians

a) All users of University IT must be uniquely identified using an approved authentication mechanism.
b) Generic and shared accounts should be avoided and require approval by both the business owner and ITDS prior to being issued.

c) Minimum password and account requirements must be defined and enforced to ensure passwords meet minimum requirements. Current requirements are as follows:

Account Type	Password	Password Rotation	Lockout	MFA
User Account	Minimum of 14 characters with mixture of upper and lower alphabets	Periodic password rotation is not enforced	After 5 failed login attempts for 15 minutes	Enforced for applications accessible from the internet for each new devices or every 90 days for trusted devices
Privileged Account	Minimum of 20 characters with a mix of upper, lower, numeric, and symbol	Change every 90 days	After 5 failed login attempts indefinitely	Enforced for all access including SSH and RDP
System Account	Randomly generated password with a minimum of 32 characters	Annual password rotation is performed by the account owner	After 5 failed login attempts for 30 minutes	Not required

d) Multi Factor authentication (MFA) must be enforced for
    a. all forms of remote access including Virtual Private Networks (VPN)
    b. when an application is accessible from the internet
    c. when there is elevated risk of credential theft
    d. when using privileged, administrative access to systems.
e) Access to systems and data must be granted based on the principle of “least privilege” and in accordance to the business and security requirements.
f) Role-based access control (RBAC) should be used wherever practical to enforce consistent security commensurate with job function, and to enforce segregation of duties (SoD).
g) Regular audits should be performed on access granted to users to ensure they remain appropriate and to remove excessive access.
h) The University will establish an automated mechanism for on-boarding and off-boarding user accounts based on affiliation with the University such that:
    a. Only authorised persons are granted an active logon to University IT
    b. Access is automatically revoked in a timely fashion when the person's association with the University ceases
i) Access requests managed outside of the automated on-boarding (e.g., granting and revoking access to systems) must be approved and documented in accordance with defined user access management process for each system.

8. Physical and Environmental Security

Responsibility: University IT Custodians

a) Physical University IT assets, including servers, network devices, communication equipment, appliances must be stored in authorised and secured locations (data centres, communication rooms, etc) with appropriate environmental controls (air conditioner, fire and smoke alarm, etc) commensurate with risk.
b) On-premise University IT assets supporting critical business operations must be stored in purpose-built Tier 3 data centres.
c) Physical access to the University's IT facilities (e.g., data centres, computer rooms etc.) where critical information is stored or processed and the supporting infrastructure (such as communications room, power boards, and network, etc.), must be adequately controlled to prevent unauthorised access, damage and unwanted disruption.
d) In particular, the following minimum controls should exist for data centres:
    i. Security camera monitoring the entrance and interior
    ii. Swipe card access control with access limited to authorised individuals
    iii. Annual review of staff with access to data centres
    iv. Environmental controls
    v. UPS and power generator
e) Where a commercial data centre or shared hosting service is used, they should be certified against accepted industry standards and provide up-to-date Services Organisation Controls (SOC) 2 Type II report.

9. Network and Server Security

Responsibility: University IT Custodians

a) The University's network must be designed in such a way as to enable effective and efficient segmentation in alignment with the principles of least privilege and defence in depth in order to mitigate the risk of both external and internal threats.
b) Network access policy must be based on "block by default" rule, and only allow those traffic that are required for network communication between devices to support business objectives.
c) End user devices connecting to the University network should be identifiable to the user's University ID where relevant, so that traffic can be attributed to an individual and security controls applied as required based on the individual's roles and responsibilities.
d) Network perimeters as well as key internal gateways should be protected using stateful packet-inspection firewalls equipped with intrusion detection and prevention capabilities.
e) Firewall rules must be reviewed at least annually.
f) Network traffic metadata should be logged in the University's Security Information Event Management (SIEM) to detect anomalous or suspicious network traffic.

10. Endpoint Security

Responsibility: University IT Custodians

a) Endpoint devices and operating system (including firmware) that store and process University data and/or connect to the University network, including servers and SOE, should be "hardened" at a level that is commensurate with the value of data in order to mitigate the risk of unauthorised access/modification and loss of data.
b) The University must deploy and maintain a standard operating environment (SOE) that is "hardened" for use by all staff.

c) By default, end users shall not have local administrative privileges on SOE devices.
d) Only devices, operating systems and firmware that are supported by the manufacturer and eligible to receive updates and patches should be used.
e) Servers and client computers must have an authorised anti-malware software running all the time that can detect and prevent malicious activities.
f) Servers should be configured with host-based firewalls that will limit ingress and egress traffic to those that are required for performing their functions.
g) Audit logging should be enabled with logs forwarded to the University's SIEM.

11. Patching and Vulnerability Management

Responsibility: University IT Custodians

a) Software and hardware firmware must be updated on a periodic basis.
b) Any "out-of-band" emergency security patches must be applied expediently in accordance with likelihood and impact of exploitation.
c) Periodic vulnerability scans must be performed across all University IT assets to discover vulnerabilities such as unpatched systems and weak configurations.
d) A risk-based approach should be used to evaluate and apply fixes to discovered vulnerabilities in a timely fashion.

12. Resilience, Data Backup and Disaster Recovery

Responsibility: University IT Custodians

a) University IT must be architected with resilience capabilities commensurate with business criticality and remove single points of failure where possible to prevent outages.
b) University data must be backed up and retained according to schedule as agreed between the Business Owner and the IT custodian.
c) Periodic restore testing should be performed to ensure that backups remain viable in case of a disaster.
d) IT custodians must develop and periodically test a disaster recovery plan to ensure resumption of services with timeframe agreed with the business owner.
e) Business units should develop and periodically test a business continuity plan that describes workarounds when key IT services become unavailable during a disaster scenario.

13. Logging, Monitoring and Incident Response

Responsibility: University IT Custodians

a) The University will maintain a security operations centre (SOC) capability to proactively detect security incidents based on analysis of logs and user behaviour with ability to respond to incidents on a 24x7 basis.
b) The University will develop and maintain a security incident response framework including an incident response plan and playbooks addressing different scenarios such as ransomware.
c) Security logs must be protected against unauthorised changes and analysed on a regular basis in order to identify potential unauthorised activities and facilitate appropriate follow up action.