Information & Communication Technology (ICT) Security Standard

Purpose and Scope

This standard states the University principles for protecting information and communication technology assets, ensuring data confidentiality, integrity, and availability, and promoting secure practices across all digital environments.

This standard applies to all staff, students, tenants, contractors, visitors.

Overarching Policy

ICT Security Policy

D&T Conditions of Use Policy

D&T Network Infrastructure Standard

Security Policy

Information Classification Policy

Password Policy

Standard

1. MALICIOUS SOFTWARE

1.1 To protect Murdoch University's information and ensure business continuity, it is essential that the University has an effective malicious software management system. The system should:

1.1.1 Minimise the risk of malicious software throughout the University;

1.1.2 Provide a central management function; and

1.1.3 Enable automated configuration and deliver:

(a) automated updates of malicious software data files;

(b) upgrading of system version(s); and

(c) downloads of new updates when required.

1.2 Murdoch implements the software management systems in *Table 1* to manage malicious software on all systems deployed by the University.

1.3 Murdoch systems that are not deployed by Digital and Technology (D&T) and are connected to the IT network must:

1.3.1 Receive approval from the relevant school or organisational unit manager to allow Digital and Technology to install and configure security software including malware protection, centralised management and monitoring and alerting software; and

1.3.2 Be verified in coordination with Digital and Technology to ensure proper installation of security software.

1.4 In accordance with the *ICT Security Policy* and *D&T Conditions of Use Policy* , any activity with the intention to create and/or distribute malicious programs to Murdoch University's IT networks e.g. viruses, worms, Trojan horses, email bombs, etc. is prohibited.

1.5 Removal, disablement or reconfiguration of Security software implemented by Digital and Technology on a system that is connected to Murdoch University's IT network infrastructure is prohibited.

1.6 Any system that does not adhere to the *ICT Security Policy* and ICT Security Standards may be immediately disconnected from Murdoch University's IT network infrastructure by Digital and Technology and should not be reconnected until remediated in line with these requirements.

1.7 If a system is infected by malware it will be removed from the Murdoch network by Digital and Technology until it has been remediated.

1.8 Peer to peer network traffic will be monitored and filtered by Digital and Technology to prevent malicious software incidents.

1.9 In accordance with the *ICT Security Policy* and *D&T Conditions of Use Policy* users are not permitted to run auto execution programs that run automatically from an external drive, such as a USB drive, on any Murdoch University owned asset. Any user with a requirement to run an auto execute program must:

1.9.1 Obtain permission from Digital and Technology to copy the file to the desktop and execute it; or

1.9.2 Request the assistance of Digital and Technology to install the auto execute program.

Table 1 Software management systems

Type	Product	Description
Email Gateways	Microsoft Defender for Office	This product scans all incoming email destined for registered email services removing known virus and malicious email content.
Anti-Virus for Servers/Networks	Microsoft Defender for Endpoint	Deployed to all servers this product prevents the infection of services and distribution of viruses through shared files.

Anti-Virus for Clients	Microsoft Defender for Endpoint	Available for Microsoft Windows, Apple OS, and Linux operating systems. All University owned workstations must have this software.

2. NETWORK SECURITY

In accordance with the *ICT Security Policy* and *D&T Conditions of Use Policy* all devices connected to the Murdoch network must comply with the following requirements:

2.1 Network Device Authentication

2.1.1 Access to network services and local (console) interfaces must be secured using passphrases or other robust authentication mechanisms. Exceptions apply only where the service or device is explicitly intended to provide unauthenticated access (such as public web servers or kiosks) and does not pose a security risk through potential misuse.

Authentication is mandatory for the following services:

- Proxy services
- Email (SMTP) relays
- Wireless access points
- Remote desktop
- Secure shell (SSH) access
- Printer administrative interfaces

2.1.2 Devices that do not support authentication may be exempted from this requirement provided that physical access is restricted.

This exemption does not extend to network-facing services running on the device.

2.2 Console Sessions

2.2.1 All devices must be configured to automatically lock or log out after 20 minutes of inactivity, requiring user re-authentication to resume access. Exceptions to this requirement include:

(a) Devices without auto-lock or logoff capability

Devices that cannot be configured to automatically lock or log off, such as network appliances or consumer electronics, may comply through alternative safeguards, such as being stored in physically restricted locations (e.g., a locked office)

(b) Physically secured devices

Devices located in secure environments that prevent access by unauthorised individuals are exempt from this requirement.

(c) Kiosks and other public-use devices

Devices designated as kiosk workstations (e.g., public-use terminals in libraries or room/event scheduling panels) are exempt, provided physical access is limited to authorised personnel.

2.3 Security Patches

2.3.1 All campus network-connected devices must operate only software that receives timely security patch updates. Available patches must be applied according to a schedule that reflects the severity of the vulnerabilities they address.

Software that cannot be patched must be formally exempted by the D&T Cyber Security team (also known as the Information Security team) and recorded in the Digital and Technology Vulnerability Exemption Register.

2.3.2 Network Administration Accounts

Privileged and super-user accounts (Administrator, root, etc.) must not be used for non-administrator activities. A secure mechanism to escalate privileges (e.g. via User Account Control or via Sudo) with a standard account is acceptable to meet this requirement. Network services must run under accounts assigned the minimum necessary privileges.

The following case is exempted from this requirement:

(a) Devices that do not support separation of privileges

Devices that do not provide separate facilities for privileged; or unprivileged access (e.g. some network appliances and printers with embedded operating systems) are exempt from this requirement.

3. WIRELESS NETWORK SECURITY

3.1 The only approved method of connecting to the Murdoch wireless network is via wireless access points installed and managed by Digital and Technology.

3.2 All wireless network installations must comply with the *D&T Network Infrastructure Standard*.

4. VIRTUAL PRIVATE NETWORK SECURITY

4.1 Virtual Private Network (VPN) access will only be available to clients with appropriate authorisation to access the secure system.

4.2 VPNs at Murdoch University are to use an IPSec enabled VPN client to provide a securely encrypted data tunnel between the client and a VPN server.

4.3 A VPN server is used to:

4.3.1 Authenticate the client ensuring only authorised users can connect to the Murdoch University network;

4.3.2 Encrypt the data stream and provide a secure data path to critical systems; and

4.3.3 Provide a means by which a client can be identified.

4.4 Unless permission has been provided by Digital and Technology an individual may not create or connect a VPN server, router or termination point within the University network.

4.5 Any user accessing university resources via VPN must use a system that has been configured by Digital and Technology with the current version of University provided Security software and operating system patches (Windows, Linux or Mac OS).

5. DATA DELETION MANAGEMENT

5.1 In accordance with the *Digital Media Disposal Standard* all information must be removed from any electronic storage devices including, but not limited to, computers, external disk drives, multifunction devices and portable devices prior to lease return, sale, transfer or destruction of a device.

5.2 Information should be removed by one of the following methods:

5.2.1 Overwriting information with a minimum of three random data passes;

5.2.2 Degaussing and rendering data stored on the device unreadable; or

5.2.3 Physical destruction of the device.

5.3 Storage devices held by Digital and Technology for deployment, transfer, repair or disposal will be recorded, securely stored and safeguards put in place to prevent unauthorised access.

5.4 Data storage disks replaced as part of an IT repair must:

5.4.1 Be returned to Digital and Technology; and

5.4.2 Have all information removed in accordance with Section 5.2 before disposal.

6. DATA ACCESS REQUEST PROCESS

6.1 In accordance with the *ICT Security Policy*, and *Data Classification Policy*, all user data access requests such as, but not limited to, confidential and operational access must be approved by the following authority:

Confidential Request

6.1.1 This request primarily entails any investigations including preliminary investigations towards suspected/actual fraud, corruption, misconduct or matter regarding legal obligations.

6.1.2 The Vice Chancellor of Murdoch University will be the approver for all Confidential Requests.

Operational Request

6.1.3 Any request for information that does not meet the criteria of confidential request will be operational requests.

6.1.4 All operational requests must have approval from respective School Deans or Directors and People & Culture.

6.1.5 Chief Experience Officer or Head of D&T Operations will authorise release of information.

6.1.6 Written consent must be obtained from current staff who are the subject of the operational request.

6.2 All requests must be made using the Confidential & Operational Data Access Request Form.

7. VULNERABILITY MANAGEMENT

7.1 Digital and Technology will obtain timely information about technical vulnerabilities for all systems at Murdoch University, assess the University's exposure to identified vulnerabilities and perform a risk assessment. Based on the results of the assessment appropriate measures will be taken (e.g. applying patches or other compensating controls) to address the associated risk.

7.2 IT and non-IT Application and System owners will grant auditors and security analysts the appropriate access to systems and data for the purposes of performing vulnerability assessments.

7.3 Digital and Technology may designate actions to remediate identified technical vulnerabilities to appropriate staff within the University. If fix actions are not addressed in a timely manner Digital and Technology will mitigate exposure to the risk by removing the affected system from the University network.

7.4 Digital and Technology run vulnerability scans and conduct security assessments of University systems on a regular basis.

8. LOG RETENTION

8.1 IT infrastructure and services providers at the University will maintain logs for:

8.1.1 All servers including Windows, Linux, Mac OS X;

8.1.2 Network communication devices including switches and routers; and

8.1.3 Application, network and server-based firewalls.

8.2 Any individuals who administer a University network device will ensure that logging is enabled, and the device time syncs with either Active Directory or the University NTP (Network Time Protocol) servers. The log events will be forwarded to the University's Central Log Repository and retained for twelve (12) months. Logs are forwarded to the Security Incident and Event Management (SIEM) system for correlation and notification and to ensure nonrepudiation.

9. PASSWORDS

9.1 To protect passwords from unauthorised or unintended disclosure and minimise the likelihood of unauthorised use, all staff, students and authorised visitors must comply with the University's Password Policy and Password Standard.

10. ACCESS CONTROL

10.1 In accordance with the *D&T Conditions of Use Policy* and *ICT Security Policy* access controls are used to protect the confidentiality, integrity, and availability of University information maintained in IT resources. Owners of University IT resources are responsible for ensuring that IT security access control standards are adhered to.

10.2 User Identification

10.2.1 Unique user identification ("userid") is assigned to everyone that has a business or educational need to access Murdoch University IT resources:

(a) Students are assigned a userid (i.e. student number) at the time they are offered a place at the University;

(b) Employees of the University are assigned a userid (i.e. staff number) at the time of employment; and

(c) All contractors, consultants, or other non-employees, who require user credentials to fulfil a business, education, and/or research obligation on behalf of Murdoch University must request a user account (i.e. MAIS other) from an authorised agent at the University.

10.3 Authentication

10.3.1 Authorised user credentials are retained in a centralised system managed by Digital and Technology that ensures restricted University systems are only accessible after users have authenticated through the system.

10.3.2 Unless otherwise authorised by Digital and Technology, IT resources will use encrypted authentication mechanisms.

10.3.3 Any service which meets one or more of the following criteria must not send authentication information (i.e. passwords) over the University IT network without secure data encryption:

(a) A server with active users;

(b) A server that receives daily service authentications;

(c) A system that contains sensitive University data or data that is critical to University business continuity; or

(d) The system has had a serious security incident in the past.

10.3.4 Authentication credentials for University IT resources should not be coded into programs or queries unless encrypted and if no other reasonable option exists Digital and Technology should be consulted.

10.4 Authorisation

10.4.1 IT resource owners must establish specific authorisation privileges for IT resource access with appropriate privileges assigned to the following groups:

(a) User Accounts;

(b) System Accounts; and

(c) Administrator Accounts.

10.4.2 The principle of 'least privilege' will be applied when allocating access that is, only the minimum privileges necessary to complete required tasks, for the role the user is employed for. shall be assigned to individual that use IT resources.

10.4.3 Administrative access to IT resources should be minimal and only available to individuals who have been authorised by Digital and Technology

10.4.4 Assigned privileges to users must be reviewed on a regular basis and modified or revoked upon a change of status at Murdoch University. When privileges assigned to individuals change, including a change in role or responsibilities, access to IT resources must be adjusted accordingly.

10.4.5 Privileged users must not modify production data in an unauthorised manner. If modification to production data is required, it must be in line with the University's established policy and procedures.

10.5 Access Controls

10.5.1 Digital and Technology will accompany access controls with mechanisms to detect, record, and generate alerts regarding repeated failed attempts to access IT resources.

10.5.2 Account lockout capabilities, including a maximum number of ten login attempts and a thirty (30) minute lockout time duration must be implemented on all University IT resources.

10.5.3 Access control permissions for all non-public University IT resources must default to no access to block unauthorised user access.

10.5.4 IT resources will be designed and configured by Digital and Technology to default to no access (denial of privileges to end-users) in the event of a malfunction.

10.5.5 IT resource access should use password-protected screensavers whenever possible and access time out after a five (10) minute or less period of inactivity.

10.5.6 Testing or attempting to compromise internal controls, when outside of the scope of an individual's employment duties at Murdoch University, is prohibited unless specifically approved in advance with Digital and Technology using the D&T Security Control Exception catalogue item.

10.5.7 All contractors, consultants, or other non-employees of Murdoch University will only be given appropriate IT resource access privileges if an IT resource owner, or their designee, determines there is a legitimate business need. These privileges must be enabled only for the time period required to accomplish approved

tasks and then promptly disabled upon completion of the approved tasks.

10.6 Remote Network Access

10.6.1 Secure remote access to Murdoch University is only available to selected staff and affiliated bodies of the University (such as approved Service Providers) after permission has been obtained by the appropriate School or organisational unit manager and Digital and Technology if there is a business need.

11. APPLICATION SECURITY

11.1 All individuals who are a valid Murdoch University user, contractor or Service Provider developing or administering applications designed to handle or manage University data must:

11.1.1 Prominently display a 'Murdoch University' banner to the screen or interface in use by the application;

11.1.2 Ensure applications validate input properly and restrictively, allowing only the type of input that is known to be correct. Examples include, but are not limited to checking for SQL injection, cross-site scripting and buffer overflow errors;

11.1.3 Ensure applications execute proper error handling so that errors will not provide detailed system information, deny service, impair security mechanisms, or crash a University system;

11.1.4 Ensure applications processing data authenticate users through central authentication systems;

11.1.5 Establish authorisation for applications by affiliation, membership, or employment, rather than by individual authorisation;

11.1.6 If individual authorisations are used, these should expire and require renewal on a periodic (at least quarterly) basis;

11.1.7 Use central authorisation tools and if additional functionality is needed coordinate development with Digital and Technology;

11.1.8 Ensure applications make use of secure storage for University data in accordance with the *ICT Security Policy*;

11.1.9 Implement the use of application logs and log access to University data for all users and times of access;

11.1.10 Conduct code-level security reviews with professionally trained peers for all new or significantly modified applications including those that affect the collection, use, and/or display of confidential data and document the actions that were taken;

11.1.11 Conduct quarterly security tests of applications in addition to application testing that is identified as required by Digital and Technology;

11.1.12 Ensure that obsolete applications, or portions of applications, are removed from any possible execution environment;

11.1.13 Adhere to the University *Information Security Change Management Guidelines* for changes to existing software applications;

11.1.14 In accordance with the *ICT Security Policy* authorised third parties, including Service Providers, providing software and/or receiving University data must enter into written agreements with Murdoch University to secure systems and data;

11.1.15 Maintain a full inventory of all applications that include descriptions of authentication and authorisation systems, level of criticality for each application, the custodian assigned to each application and the data classification in accordance with the *Data Classification Policy*;

11.1.16 Document clear rules and processes for checking and granting authorisations;

11.1.17 On a quarterly basis, review and adjust/remove all authorisations/access for individuals who have left the university, transferred to another school or organisational unit, or assumed new job duties within the department.

11.2 Individuals who administer computer systems associated with University data or engage in programming or analysis of software that runs on such systems must:

11.2.1 Complete a Murdoch University *Conflict of Interest Declaration* (online at https://goto.murdoch.edu.au/ConflictOfInterest) and adhere to the Codes of Conduct.

11.2.2 Acknowledge these minimum standards on a yearly basis or for the term of the administration role.

11.3 Digital and Technology will also monitor, review and audit privileged administration access on an annual basis.

11.4 All new applications and services must undergo a formal compliance assessment to ensure alignment with Murdoch University's regulatory and security requirements prior to being onboarded into the University environment. Vendors are required to complete and return a Higher Education Community Vendor Assessment Toolkit (HECVAT), which must be reviewed and approved by the Cyber Security team before any product implementation activities commence.

Where data will be stored in a data centre not operated by Murdoch University or an approved partner, the vendor's SOC 2 Type II Assurance Reports must be evaluated by the Cyber Security team to confirm that security and compliance controls are appropriately designed and operating effectively. If the assessment identifies that the application contains sensitive data, a 12-month review cycle for the Assurance Reports will be recorded in the compliance register.

Murdoch University data must not be uploaded to any application or service without explicit approval, or a documented exception, from the Cyber Security team.

12. MOBILE COMPUTING SECURITY

12.1 All Murdoch University owned mobile devices used by staff or University affiliates, to access, store, or manipulate University data must:

12.1.1 Have appropriate safeguards applied to mitigate the risk of unauthorized information exposure or disclosure due to loss or theft as defined in "Table 2: Required safeguards by device type". These safeguards may be verified at Digital and Technology discretion;

12.1.2 Support encryption to access, store, or manipulate critical information;

12.1.3 Be reported to the IT Service Desk telephone +61 8 9360 2000) or email itservicedesk@murdoch.edu.au) if lost, stolen, or otherwise compromised;

12.1.4 Use tracking and recovery software to facilitate return/remote wipe if lost or stolen;

12.1.5 At the time of disposal comply with the *Digital Media Disposal Standard*;

12.1.6 Have a durable physical or electronic label with contact information sufficient to facilitate an expedient return if a lost device is found;

12.1.7 Be used and stored in a manner that deters theft e.g. stored out of plain site/locked away.

Table 2 Required safeguards by device type

Mobile	**Passcode**	**Intrusion Prevention**	**Encryption**	**Remote Wiping**
Handheld mobile device (i.e. Smart Phone, Tablet, etc.)	Required: Meet University *Password Policy and Standards* requirements AND Auto lock after a maximum of five (5) minutes of inactivity	Required: Lockout after ten (10) incorrect attempts within thirty (30) minutes	Recommended: In all cases if supported by the device Required: For all intended use involving critical University information	Help Desk incident response or Digital and Technology will assist with remote wiping based on the circumstances of reported loss or theft.
Laptop /Notebook Computer	Required: Meet University	Required: Lockout after ten (10)	Required: Full disk	Not applicable

	Password Policy and Standards requirements AND Auto lock after a maximum of five (5) minutes of unattended inactivity	incorrect attempts within thirty (30) minutes		

Governance

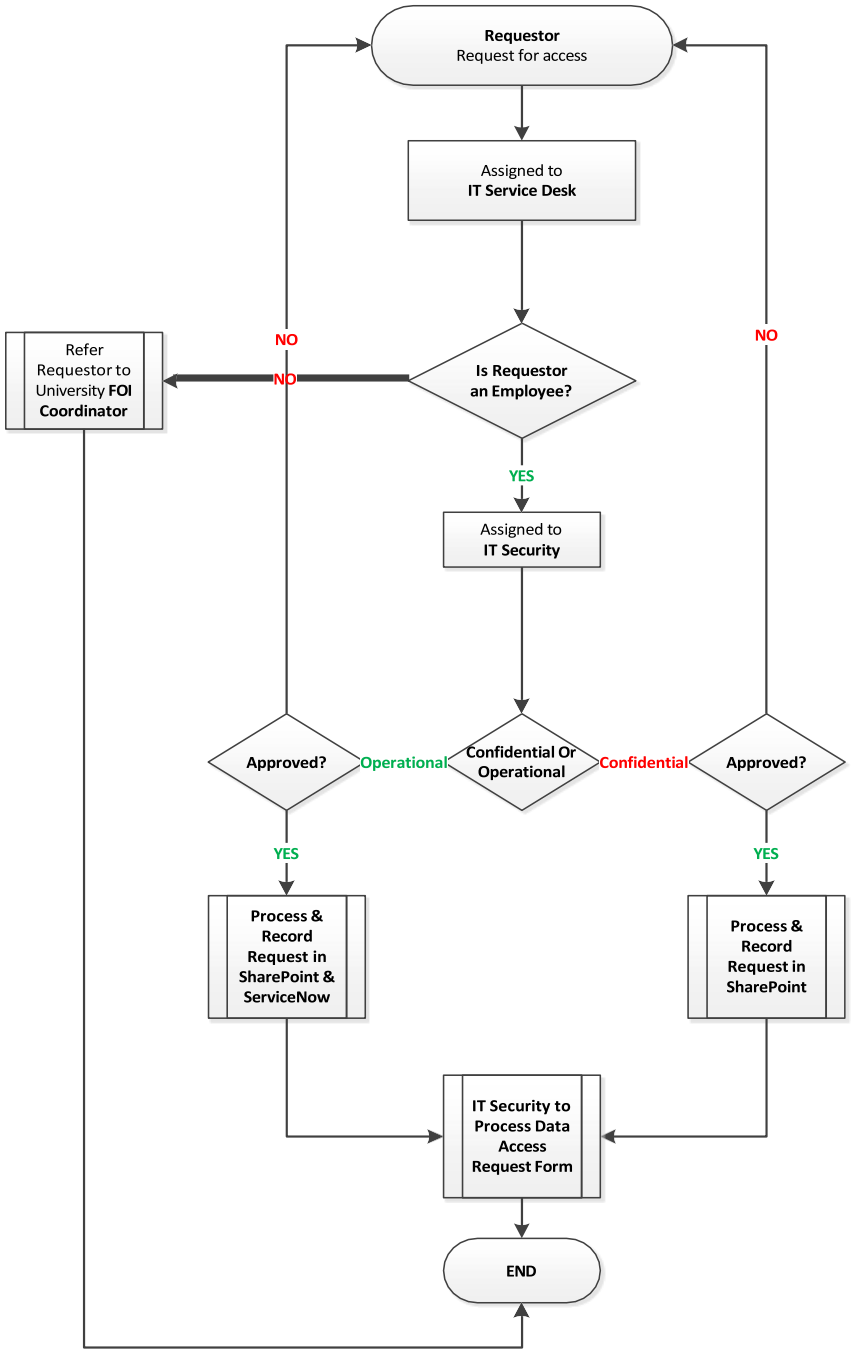
Approval Authority	Senior Leadership Team
Owner	Chief Experience Officer
Legislation mandating compliance	
Category	Primarily a function of management
Related University Legislation and Policy Documents	*D&T Conditions of Use Policy* *D&T Network Infrastructure Standard* *Information Classification Policy* *ICT Security Policy* *Password Policy* *Security Policy* *Australian Cyber Security Centre (ACSC) Essential Eight Maturity Model*
Date effective	09/02/2026
Review date	09/02/2029

Revision History

Approved/Amended	Date Approved	Resolution No. (if applicable)
Approved	09/02/2026	
Approved	19/09/2022	
Approved	27/04/2018	
Approved	20/09/2016	
Approved	02/10/2015	

Attachments

Data Access Request Process Flow



Roles & Responsibilities

Requestor
Murdoch University Dean/ Director or Above

Approver
The person who has authority to grant access to the information.

Request Method
All Data Access Request must be made via the Covert & Operational Data Access Request Form

This form is for single use/users only, each request must be submitted on a New Form

Confidential Request
This request primarily entails any Investigation including Preliminary Investigation towards Suspected/Actual Fraud, Corruptions, Misconduct or Matters regarding Legal Obligations

Operational Request
Any request for information that does not meet the criteria of Confidential Request will be Operational Requests

Approval Clarifications
If the approver cannot be clearly identified using the following rules consult University`s Integrity Officer i.e. Director, Internal Audit & Risk

Approval Authority

Confidential Request
The Approver for all confidential requests must be the Vice Chancellor of Murdoch University or their official delegate.

Operational Request
All operational request must have approval from respective School Deans or Directors AND Director People & Culture.

Chief Experience Officer or Head of IT Operations will authorize release of Information.

Written Consent must be obtained from current staff who are the subject of the request.

Note: Please fill the Form Below.

Confidential & Operational Data Access Request Form

(Single Use only, if multiple access is required submit separate forms)

REQUESTOR INFORMATION (Who is requesting this access, Requestor must be Director or Above)

Date: _____

Name (Last, first, middle initial) _____ Staff Number _____

School / Office _____ Position _____

Email address _____ Contact Number _____

STAFF/STUDENT/MAIS OTHER INFORMATION (who`s information is required)

Date _____

Current Staff/Student/MAIS Other: Yes ☐/No ☐

Name (Last, first, middle initial) _____ Staff/Student/MAIS Other Number _____

School / Office _____ Contact Number _____

Type of Request:

☐ Full Covert Access to all Data
☐ Operational Access to Person`s Email with Person`s Permission
☐ Operational access to Person`s Files with Person`s Permission

Please describe nature of request (type of information requested; Context & Justification, reasoning for the approvers, etc.) **in detail. (if required attach additional documentations**)

List all Staff (including requestor) that will have access to this information: _____

Name _____ Staff Number _____

Name _____ Staff Number _____

Access Duration & Justification for the duration:

Requestor Signature | Date

Approvals & Authorisation (Please refer to Data Access Request Flow, to determine appropriate approval. If the approval is granted via an email, please print and attach to this form).

Vice Chancellor or their Official Delegate (Full Covert Access Approval):

All Other Approvals:

School Dean`s / Director (Approval):

Director, People and Culture (Approval):

Chief Experience Officer or Head of IT Operations (Release Authorisation):

Staff Consent (For all Operation Request):

For Administrative Use Only:

Date received

Action taken:

IT Security Official signature & Staff Number | Date

Attach additional documentation, if applicable.

Please refer to the electronic copy in the Policy and Procedure Manager to ensure you are referring to the latest version.