ICT SECURITY POLICY

Policy Statement

This policy seeks to protect the confidently, integrity, and availability of information and ICT Facilities through the use of established IT security processes and practices. It should be read in conjunction with the ICT Acceptable Use Policy.

Scope

This policy is applicable to all users of ICT facilities and acceptance of the terms of this policy is a condition of using those facilities. This policy applies regardless of the location from which a user gains access to the facilities.

Eligible INSEARCH students and staff are also provided with a range of ICT facilities offered by the University of Technology Sydney. Use of those services is subject to University policy. Refer http://www.gsu.uts.edu.au/policies/itfacilities.html

Definitions

User(s)	Means any person provided with access to the INSEARCH ICT facilities, including but not limited to students, staff, contractors, consultants, Board members and affiliates.
Project Manager	Means the person responsible for managing the change to the ICT Facilities. It is often, though not necessarily an ICT Project Manager, particularly in relation to Shadow IT.
ICT Facilities	Means : • All network services, computer equipment and software, owned, leased or used under license by INSEARCH; and • Computer facilities maintained by other bodies but available for use through an agreement or agreements with INSEARCH; and • ICT systems and solutions used inside organizations without explicit organizational approval; and • ICT systems specified and deployed by departments other than the ICT.
Computer	For the purposes of this policy, computer means any form of desktop, laptop, tablet, mobile phone or similar emerging technologies.
Mobile Code	Mobile code is any program, application, or content capable of movement while embedded in an email, document or website.
Privileged Access	Certain designated staff members have privileged access to the resources of the ICT Facilities because their job responsibilities require such access. Typically, such staff members are responsible for providing administrative services on the designated computer(s), services such as system maintenance, data management and user support. The term "privileged access" covers a range, from wider access than that given to an ordinary system user, up to and including complete access to all resources on the ICT Facilities.
Acceptable Use	Means use of the ICT Facilities as defined in the INSEARCH Acceptable Use of ICT Facilities Policy.
Wired Network	Refers to connecting to the ICT Facilities by plugging a computer into a wall socket in an INSEARCH building.
Wireless Network	Refers to connecting to the ICT Facilities by connecting a computer to the “INSEARCH Secure” wireless network.
User Account	Means a unique account name and password that permits an individual to login into

	the ICT Facilities via the wired network, wireless network or remote access.
Access Rights	Mean the systems, functions within systems and information that the user is permitted to access and/or modify.

Policy Principles

Principle	Responsible
ASSET MANAGEMENT	
1. Rules for the acceptable use of information and assets associated with information processing facilities must be identified, documented and implemented.	ICT
HUMAN RESOURCES SECURITY	
2. Approved background verification checks on candidates for employment, contractors and external parties must be conducted in accordance with relevant laws and regulations and be proportional to the classification of the information accessed and the perceived risks.	HR
EQUIPMENT SECURITY	
3. Equipment, information and software must not to taken off-site without authorisation.	ICT
COMMUNICATIONS AND OPERATIONS MANAGEMENT	
4. Changes to information processing facilities and information systems must be appropriately controlled in accordance with ICT Change Management Policy and Procedure.	Project Manager
5. Separate development, test and production facilities must be in place to manage sensitive and critical information and systems.	Project Manager
6. Appropriate detective, preventative and corrective measures, in conjunction with user awareness procedures, must be implemented on information processing facilities and systems to protect against viruses and malicious code.	ICT
7. Security controls must be implemented to govern the use of mobile code and to prevent the execution of unauthorised mobile code.	ICT
8. Networks must be managed and controlled to provide appropriate protection from threats and to maintain security for the systems and applications using the network, including information in transit.	ICT
ELECTRONIC COMMERCE SERVICES	
9. The integrity of information made available on publicly accessible INSEARCH systems must be protected to prevent unauthorised modification.	Project Manager
MONITORING	
10. The security controls of information systems must be formally and periodically tested based on risk.	ICT

Principle	Responsible
NETWORK ACCESS CONTROL	
11. Appropriate security controls must be in place to segregate INSEARCH networks in the accordance with the relevant security standards and security architecture.	ICT
12. Network access from external parties to any INSEARCH network must be restricted to only allow access required to perform agreed services.	All
13. Any computer, in conjunction with a valid user account, may connect to the guest wireless network.	ICT
14. The wired network is used to access a range of INSEARCH services and information and is reserved for computers that are owned and managed by INSEARCH.	ICT
OPERATING SYSTEM ACCESS CONTROL	
15. All users must be assigned a unique identifier, traceable to their identity, to access information systems, for their personal use only.	ICT
16. User accounts are allocated access rights based on the user's role and responsibilities at INSEARCH.	Manager
17. Passwords must not be shared with anyone, including members of ICT, assistants, colleagues whilst on personal leave.	All
18. The manager(s) is/are responsible for initiating a review of access rights whenever the staff member changes roles.	Manager
19. Access rights must be removed immediately upon termination of the user's employment or contractor agreement. In the case of contractors and other users who are not recorded in the payroll system, the manager who authorised access is responsible for timely advice of the termination date to the ICT service desk.	Manager / ICT
20. The use of utility programs capable of overriding system and application controls must be restricted and secured appropriately.	ICT
21. Effective anti-virus software must be deployed throughout the ICT Facilities.	ICT
EMAIL FILTERING	
22. INSEARCH reserves the right to refuse email from reported spammers. This may occasionally block email from companies or persons with whom INSEARCH does business, particularly, though not necessarily, agents and potential students in developing countries.	ICT
23. Head ICT has the authority to allow email from reported spammers for a period of up to 30 days to provide time for the reported spammer to resolve the issue. Such approval will not be given where the email is, or is suspected of being malicious.	Head ICT
SECURITY IN DEVELOPMENT PROCESSES AND SUPPORT PROCESSES	
24. The implementation of changes must be controlled by the use of the ICT Change Management Policy and Procedure.	Project Manager
25. When operating systems are changed, key applications must be appropriately tested to ensure there is no adverse impact on organisational operations or security.	Project Manager
26. Risks associated with the modification of vendor supplied software packages must be appropriately controlled and authorised.	Project manager and ICT

Principle	Responsible
USER RESPONSIBILITIES	
27. Users remain responsible for any inappropriate access or security breaches performed at unattended and unlocked computers.	All
28. Users must be made aware of their responsibilities regarding the selection, use and storage of passwords. User logons and passwords represent an individual's access to ICT Facilities and must not be shared with any other person.	ICT All
29. Accounts that have system-level privileges must have a unique password from all other accounts held by that user.	Privileged Users
30. Any user suspecting that his/her password may have been compromised must report the incident to the ICT Service Desk and change it immediately.	All
31. Password cracking or guessing will be initiated on a periodic and random basis by the Head of ICT.	Head ICT
BUSINESS CONTINUITY MANAGEMENT	
32. Business continuity and disaster recovery processes must address information security and risk requirements.	
33. Risks that can cause interruption to business processes must be identified, assessed and managed.	
34. Business continuity and disaster recovery plans must maintain or restore operations and ensure availability of information at the required level following interruption or failure of critical business processes.	Governance Manager / Head ICT
35. A single framework of business continuity and disaster recovery must be maintained to ensure it consistently addresses information security requirements and to identify priorities for testing and maintenance.	
36. Business continuity and disaster recovery plans must be tested and updated at regular annual intervals to ensure that they are up to date and effective.	
37. The ICT department is responsible for putting in place backups of all business systems and data so that systems and data can be restored in line with the Disaster Recovery Plan.	
38. All major systems within the ICT Facilities are backed up on a regular basis. ICT must have a Backup Strategy which details the frequency of backups. Users must save business information and documents to the network drive to ensure it is backed up.	ICT
39. Actual or suspected security incidents will be managed as Priority 1 incidents until proven otherwise, at which point they will be downgraded in accordance with ICT prioritisation criteria.	ICT
COMPLIANCE	
40. All relevant legal, statutory, regulatory and contractual requirements must be explicitly defined, documented and kept up to date for each information system.	Project Manager
41. Deviations from this Standard and supporting standards, architectures, processes and procedures must be approved by the Chief Operating Officer for all information and systems unable to meet the requirements for this Policy.	COO

Supporting Documents

- Staff Privacy Policy
- ICT Acceptable Use of Information Technology Facilities policy
- Student Acceptable Use of Information Technology Facilities policy
- ICT Change Management Policy
- ICT Change Management Procedure
- Change of Responsibility Procedure
- Password Construction Guidelines

APPROVAL		
Signature: Name: Alex Murphy	Managing Director	Date: 24 Nov 2016
Policy Title	ICT Acceptable Use and Security	
Policy Owner:	Chief Operating Officer	
Policy ID	PO/ICT/03/16	
Effective Date:	2 December 2016	
Endorsed by the Audit and Risk Committee		Date: 2 December 2016