Information Communication and Technology Access and Account Management Procedures

Intent

These Procedures have been developed to support the Information Communication Technology (ICT) Acceptable Use Policy and will further the intent of that Policy by:

- Expressing the commitment of the University to maintaining secure, effective and reliable University ICT Services;
- Governing the provision, maintenance and termination of accounts giving access to University ICT Services;
- Outlining the provision, modification and removal of access to University ICT Services; and
- Ensuring that the University provides its account holders with secure and timely access to the online services and resources necessary for undertaking their work and study.

Scope

These Procedures apply to all Authorised Users of the University ICT Services managed by the University or third party providers on behalf of the University, both on and off campus.

Definitions

Defined terms in the ICT Acceptable Use Policy have the same meaning in these ICT Access and Account Management Procedures.

Account means a user name or other identifier which, with or without a password, allows a user to access University ICT Services.

Asset Owner means an individual or collective group with accountability and authority for University ICT Services.

College/Directorate Representative means a person appointed by a College or Directorate whose role is to control use of University ICT Services allocated to their College or Directorate. (where applicable)

Delegate Account means an external account that is control by an account manager. The account manager can change the account's name, occupancy dates and password.

General Access Teaching Computer Facilities Labs (GATCF) means the computing labs and equipment provided by the University.

Generic Account means an Account that is not linked to personal identity (e.g. a University staff or student).

ICT News Bulletins means information supplied by ICT either by email, automatically output on a workstation or on the web-based University news boards.

Outside User means a person or organisation, external to the University.

Privileged System Access means access to administrative roles within operating systems, databases and applications, for example, root access in a Linux system.

Research DMZ means a portion of the network, built at or near the campus or laboratory's local network perimeter that is designed such that the equipment, configuration, and security policies are optimised for high-performance research applications rather than for general-purpose business systems or enterprise computing.

Table of Contents

Introduction

These procedures are designed to support the operational nature of the ICT Acceptable Use Policy by providing detailed access management procedures.

University ICT Services are the property of the University.

Procedure

1. Creation of Staff Accounts

1.1 Information and Communication Technology will follow the Staff Pre-Boarding and Off-Boarding procedure and will ensure

a. User Accounts are automatically created upon information updated by Human Resources via the Alesco HRMIS.
b. All staff Accounts are provided with access to University ICT Services including:
   i. University email,
   ii. Wireless network access (eduroam),
   iii. Corporate applications and
   iv. Access to common file shares (where appropriate)

1.2 Account details are updated to the staff member or nominated supervisor and suggest changing the password upon first login

2. Creation of Student Accounts

2.1 Student Accounts are created when the student is entered into the University system for offering the student a place at the University.

2.2 Prospective undergraduate and postgraduate students who have accepted offers will:

a. Obtain the University computer account details (login, password and email address) from Get Started @ JCU. Students will need their 8 digit University student number, supplied to them by the University Admissions included in the letter of offer to a course to log in.

b. Change their password on first login

3. Requesting Additional Access

3.1 Authorised Users can request additional access to University ICT Services, including file shares and applications.

3.2 If a staff member requires a level of access different to that usually given to Staff in their relevant area, the respective Director must authorise the level of access required and submit that authorisation to Information and Communication Technology via electronic mail or using ServiceNow incident reporting tool.

3.3 The procedure to provide such additional access will be following Change of IT access procedure

4. Requesting Generic Accounts

4.1 Information and Communication Technology from time to time to meet the University's operational needs manually create generic Accounts. Generic Accounts are not permitted for access to student, financial or personal identifiable information.

4.2 The staff member will submit the request for Generic Account(s) to the respective Director

4.3 The Director will decide whether to approve the Generic Account(s) and access in accordance with applicable University policies and procedures; and approved, forward the request to the ICT Help Desk.

4.4 Information and Communication Technology will:

a. Create the Generic Account and notify the owner of the account of the account details; and

b. Manually delete the Generic Account upon expiry, or at the request of the person responsible for the Generic Account.

5. Passwords

5.1 Authorized Users must:

a. Select passwords that comply with the University password requirements;

b. Change their passwords at regular intervals; and

c. Maintain security of their password.

5.2 Information and Communication Technology will implement a baseline tiered password policy based on user group, as defined in Table 1 below.

Table 1 – Password Requirements

Requirement	User Group				
	Undergraduate, Postgraduate and Research Students	**Staff, Generic, Delegate and External Accounts**	**ICT Staff Secondary Administrative /Domain Accounts**	**Service Accounts (e.g. application to database)**	**System Accounts (e.g. root in Linux)**
Null passwords	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed
Minimum length	8 characters	8 characters	15 characters	16 characters	20 characters
Maximum length	System maximum	System maximum	System maximum	System maximum	System maximum
Repeating characters (AAA) of adjoining characters (ABC)	Not allowed	Not allowed	Not allowed	Not allowed	Not allowed
Complexity **(8-14 characters)**	Contain at least 1 number (0 - 9), 1 uppercase character (A - Z) and 1 lowercase character (a - z)	Contain at least 1 number (0 - 9), 1 uppercase character (A - Z) and 1 lowercase character (a - z)	NA	NA	NA
Complexity **(15 or more characters)**	Contain 1 number (0 - 9) or 1 uppercase character (A - Z) or 1 lowercase character (a - z)	Contain 1 number (0 - 9) or 1 uppercase character (A - Z) or 1 lowercase character (a - z)	Contain 1 number (0 - 9) or 1 uppercase character (A - Z) or 1 lowercase character (a - z)	Contain 1 number (0 - 9) or 1 uppercase character (A - Z) or 1 lowercase character (a - z)	Contain 1 number (0 - 9) or 1 uppercase character (A - Z) or 1 lowercase character (a - z)
Password change (8-14 characters)	365 days	365 days	365 days	As required.	180 days (or upon departure of ICT

					staff with knowledge of the password)
Password change (15 or more characters)	No change	No change	365 days	As required.	180 days (or upon departure of ICT staff with knowledge of the password)
Account lockout after nominated unsuccessful attempts	Yes	Yes	Yes	Recommended	Recommended
Stored in encrypted format	Yes	Yes	Yes	Yes	Yes

5.3 Where systems do not support the above requirements, ICT will:

a. Identify the system and conduct a risk assessment on the proposed solution to identify mitigating controls; and
b. Implement the mitigating controls or make recommendations to the Asset Owner.

5.4 Administrative staff responsible for the Research DMZ will:

a. Implement and maintain security guidelines for the Research DMZ; and
b. Comply with the above password policy. Where compliance with the above password policy is not feasible, implement mitigating controls based on the results of a risk assessment.

6. Resetting Forgotten Passwords

6.1. Authorised Users who have forgotten the password for their Account must submit a request for password changes to the ICT
6.2. ICT will maintain a manual password reset process by confirming the Authorised User's identity and provide a one-time password to the Authorised User's pre-registered contact details to be changed on first login.

7. Modification of Staff Access When Their Relationship With the University Changes

7.1. The relevant Director must notify Human Resources of any change in the relationship between a staff member and the University that might affect the staff member's entitlement to University ICT Services.
7.2. The Director, Human Resources will ensure that the appropriate position changes are updated to ICT via electronic mail or via ServiceNow incident reporting tool.
7.3. Information and Communication Technology will modify the staff members' access to University ICT Services by following the Change of IT access procedure

8. Additional Requirements for ICT staff

8.1. Staff working in ICT who are enrolled in University courses or programs will not usually be granted access to University ICT Services where that access enables them to change their or others' academic results.
8.2. The Senior Manager, Information and Communication Technology, must:

a. Maintain oversight of those staff who may also be registered as students of the University and ensure that access controls are sufficient to ensure that Information and Communication Technology staff cannot modify student related records; and
b. Implement processes (e.g. supervision) to ensure that Information and Communication Technology staff members do not modify academic results or material. Information and Communication Technology staff members will not:

i. view course material for any course, before that material is made available for viewing by students enrolled in the course, unless they have written permission from the staff member, lecturer, tutor, teacher or instructor who prepared the material, or from the course coordinator or relevant Dean of College;

ii. take any action that would result in them or any other person gaining an academic advantage over other students;

iii. access any personal, academic or confidential information about anyone else unless required in the course of their University duties; or

iv. perform any other action that is inappropriate for or unauthorised by their position or duties.

9. Disabling and Deletion of Staff Accounts

9.1. If the Staff relationship with the University ends (e.g. retirement, resignation, termination or end of contract), the Human Resources notifies ICT on the Staff contract end date to remove privileged access and disable the staff account.

9.2. Upon receiving the notification, ICT will update the case to ServiceNow incident reporting tool for records management.

9.3. Staff members who have multiple relationships with the University (such as an account holder who is both student and staff member) who cease only one of their relationships will only have the access related to the terminating relationship removed

10. Suspending Accounts

The Deputy Vice Chancellor, Director Human Resources or Director Student Services or Director ICT, may authorize suspensions of Accounts under certain conditions. Situations under which suspension of Accounts would be considered include (but are not limited to):

a. Threats to the University ICT Services; or

b. Inappropriate use of University ICT Services, systems or software.

Related Policy Instruments

This policy should be read in conjunction with other relevant University policies and procedures including:

ICT Acceptable Usage Policy
ICT Acceptable Use Procedures
ICT Asset Management Policy
Financial Regulations
Disposal Plant and Equipment

Related Documents and Legislation

Singapore Statutes

The Computer Misuse and Cyber security Act (Cap 50A)
Copyright Act (Cap 63)
SPAM Control Act (Cap 311A)
Undesirable Publications Act (Cap 338)
Personal Data Protection Act 2012

Administration

Approval Details

Approval Authority:	Head of Campus Singapore
Approval Date:	02/01/2018
Version No:	V1.1
Date for Next Review:	31/12/2020

Revision History

Version	Revision Date	Description of Changes	Author
1.0	01/04/2017	Process established	Vijay Shreenivos
1.1	15/12/2017	Change Approval Authority from Deputy Vice Chancellor to Head of Campus Singapore.	Vijay Shreenivos

Contact Person/Unit

Contact Person/Unit:	Vijay Vikram Shreenivos / Senior Manager, ICT

Keywords

Keywords:	ICT, Access and Account Management Procedure