University IT Account Entitlement and Rights Assignment Policy

Version Number:	2.1
Document Status:	Approved
Date Approved:	25 June 2019
Approved By:	Data and Information Management Oversight Group
Effective Date:	25 June 2019
Date of Next Review:	June 2021

1 Purpose

The purpose of the policy is to set out the principles upon which decision shall be made in respect of the creation, management, suspension and deletion of a University IT account.

2 Scope

This policy applies to all IT accounts that are created and hosted by Cardiff University and to externally created or hosted accounts that seek permission to connect to the University IT Facilities (see definitions).

3 Relationship with existing policies

This policy forms part of the Information Security Management Framework. It should be read in conjunction with the Information Security Policy and all supporting policies.

4 Policy Statement

The creation, management, suspension and deletion of IT accounts shall be managed in accordance with overarching principles which ensure that the University's resources are used effectively, that its legal obligations are complied with and that its information assets are appropriately protected in terms of confidentiality, integrity and availability.

5 Policy

5.1 IT accounts shall only be created when a user falls within one or more entitlement category as determined and published by the Information Security Operations Group (ISOG). Any exceptions to this shall be agreed by ISOG and approved by the Senior Information Risk Owner.

5.2 When determining entitlements, the Information Security Operations Group shall take into consideration how the entitlement (or modification or withdrawal of entitlement) supports the University's strategic goals, the effective use of resources, compliance with legislative and contractual obligations and the risks to security of information assets in terms of confidentiality, integrity and availability.

5.3 IT accounts shall be managed during their lifecycle and shall be suspended or deleted in accordance with the Membership Categories and Entitlements tables[1], such that when the status of the user changes there are safeguards in place to ensure that the entitlements remain appropriate or are removed at the appropriate point.

5.4 IT account creation and management shall be automated and managed via a single identity management system as far as feasible to ensure efficient operation. Where powers to create and manage accounts for entitled groups or individuals are devolved, those powers should only be used where it is:

1. a) not possible to use the existing data authority systems (e.g. SIMS or Core) to feed the central identity management system as the user does not fall within the appropriate category or
2. b) not operationally practicable to use the existing data authority systems for other reasons which are in the University's best interests.

All account creation and management, whether centrally or locally conducted shall comply with this policy and the Membership Categories and Entitlements tables.

5.5 The authoritative data source for determining each membership status shall be defined by the University IT Service and processes and procedures shall be established in liaison with the Human Resources and Registry departments to ensure that staff and student accounts are suspended at the appropriate point following a change of status to ex-members.

5.6 Ex-member accounts shall only be extended beyond the default period if those individuals fall under another Membership Categories and Entitlements table category and their rights should be modified accordingly. Any exceptions to this shall be approved in accordance with clause 5.1 above.

5.7 Staff and students shall be given appropriate notice of the impending routine closure of their account. For staff this will be at least 30 days notice (where the member of staff's contractual notice period is in excess of a month) and for students this will be at least 90 days notice. Communications shall be embedded into existing leavers processes.

5.8 No notice period is proscribed where accounts are suspended for reasons other than routine closure.

5.9 When designing authentication mechanisms to allow access to University IT resources and applications, the mechanism design should ensure that the basis for authentication reflects the relevant entitlement as set out in the Membership Categories and Entitlements tables. Where a technical solution is not possible the risk of proceeding differently should be signed off by the relevant Data Lead or Senior Systems Owner (Technical).

5.10 Users shall be given a predefined set of rights and entitlements which shall reflect their membership category entitlement as per the Membership Categories and Entitlements tables. Where specific authorised roles require 'enhanced' rights a list of who holds these shall be maintained at a local level and reviewed regularly by the Head of School/Department and nominated IT Rights Authority holder(s) (i.e. the individual who has the power to authorise the role) to determine whether the holding of those roles is appropriate in the current context. A valid list shall be signed off by the Head of School/ Department.

5.11 Training requirements in relation to IT Rights Authority holders shall be identified and IT Services shall ensure that appropriate mechanisms exist to convey an individual's responsibilities in relation to 'enhanced rights' and to capture training undertaken and the agreement to comply with relevant policies.

5.12 Suitable feedback mechanisms shall be in place to ensure that when the holders of specific authorised roles change, the users' entitlements are appropriately amended.

6 Responsibilities

6.1 The Senior Information Risk Owner is responsible for ensuring that the governance of the Information Security Operations Group is fit for purpose, including designating a Chair. (It is noted that the Group's remit also covers University library entitlements).

6.2 The Director of IT Services is responsible for ensuring that appropriate processes and procedures are established to support this policy.

6.3 The Data Leads are responsible for ensuring that any authoritative data sources required for IT account identity management purposes are kept up to date and remain fit for purpose.

6.4 The Chair of the Information Security Operations Group and Director of University IT are responsible for ensuring that a summary of categories and associated entitlements is published and maintained.

7 Compliance

Breaches of this policy may be treated as a disciplinary matter dealt with under the University's staff disciplinary policies or the Student Disciplinary Code as appropriate. Where third parties are involved breach of this policy may also constitute breach of contract.

Definitions

Information Asset: An Information Asset is information that has value to the University. Key Information Assets are the most important types of information required for achievement of the University's strategic aims.

Data Lead: Accountable for quality of data within their domain; Ensure data within the domain is fit for operational and strategic use; Determine conditions under which data may be used (taking account of any legal obligations applying to that type of data), in order to safeguard confidentiality, integrity, availability and quality; Confirm classifications of data entities within the domain; Confirm data requirements for business purposes.

Senior Information Risk Owner: The Senior Information Risk Owner for the University's overall information security objectives is designated by the Vice-Chancellor. The Senior Information Risk Owner shall ensure that the University's information security objectives are compatible with the strategic direction of the University and shall own the associated information security risks.

"IT facilities" (as per the IT Regulations) includes:

- Core services as provided by Cardiff University IT Services;
- Cardiff University College, School or Professional Services computers, computing equipment and mobile devices;
- personally owned computers, mobile devices and peripherals when connected to, or accessed from or via Cardiff University IT facilities;
- use of remote networks and services, when accessed from or via Cardiff University IT facilities;
- all programmable equipment; any associated software and data, including data created by persons other than users, and the networking elements which link IT facilities.

[1] https://intranet.cardiff.ac.uk/staff/services/technical-help-and-support/getting-help-with-it/it-access-entitlements