IT ACCOUNT ENTITLEMENT AND RIGHTS POLICY

1. PURPOSE AND SCOPE

1.1. 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.

1.2. This policy applies to all IT accounts that are created and hosted by Cardiff University IT, and to externally created or hosted accounts that seek permission to connect to the University's IT network and services, or other services associated with Cardiff University.

2. RELATIONSHIP TO OTHER POLICIES AND PROCEDURES

2.1. 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.

3. POLICY

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.

3.1. IT accounts shall only be created when a user falls within one or more entitlement category as determined and published by the University Membership Categories and Entitlements Group (MCE). Any individual exceptions to this shall be approved by the Chair of the Information Security Operations Group (ISOG). The MCE group will consider if exceptions require an additional Category, which will in turn be approved by ISOG.

3.2. When determining entitlements, the University Membership Categories and Entitlements 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.

3.3. IT accounts shall be managed during their lifecycle and shall be suspended or deleted in accordance with the Membership Categories and Entitlements tables, 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.

3.4. 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:

3.4.1. not possible to use the existing data authority systems (Student Records Systems, HR system) to feed the central identity management system as the user does not fall within the appropriate category or;

3.4.2. 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.

3.5. 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, Admissions and Registry departments to ensure that staff and student accounts are suspended at the appropriate point following a change of status to ex-members.

3.6. Ex-member accounts shall only be extended beyond the default period if those individuals fall within the scope of 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 3.1 above.

3.7. Staff and students shall be given appropriate notice of the impending routine closure of their account. For staff this will be at least 1 month's notice (where the member of staff's contractual notice period is in excess of a month) and for students this will be at least 3 months' notice. Communications shall be embedded into existing leavers processes.

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

3.9. 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 Business Owner.

3.10. 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 additional rights, these will be maintained in the central Identity Management System with an appropriate audit trail of authorisation.

3.11. Users shall be given a unique username and email address. This is to be enforced by the identity management system. Retention of skeleton user records is required in order to ensure all usernames and email addresses are unique.

3.12. Training requirements in relation to high and medium risk specific authorised roles shall be identified and University IT shall ensure that appropriate mechanisms exist to convey an individual's responsibilities in relation to 'enhanced rights' and to capture the agreement to comply with relevant policies.

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

3.14. Wherever possible an identity should have a single login account with as few accounts as practical per identity. Each login account is to be used by the individual specified in the Identity only. The use of shared 'generic' accounts is not permitted, without a risk assessment and exception signoff by ISOG. Where privileged access to IT systems is required, such access rights may be delegated to an individually attributed service account to provide clear separation of role. For example:

3.14.1. Where an individual has access to university confidential data, that is not part of their substantive role (e.g., a Taught postgraduate working part time in registry) that access should be facilitated through clear separation of login accounts and identities.

3.14.2. Where an individual has split roles, their title displayed in the email address book shall default to their largest contracted FTE role (e.g., 0.8 School of Engineering, 0.2 School of Mathematics, would default to School of Engineering). Exceptions may be addressed through local Human Resources.

3.14.3. If the nature of relationship with the university changes, for example, a full-time member of staff becomes a full-time student, depending on risk the established account may be deprecated in favour of a new account for clear separation of responsibilities and duties.

4. BREACHES OF POLICY

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

5. ROLES AND RESPONSIBILITIES

5.1 The **Senior Information Risk Owner** is the sponsor for this policy, and responsible for approving the need to develop or substantively amend the policy, for presenting the final draft to the approving body and for ensuring that their policy-making documents comply with, and are monitored and reviewed in line with the Cardiff University Policy for the Development of Policy-making Documents.

5.2. The **Senior Information Risk Owner** is responsible for ensuring that the governance of the University Membership Categories and Entitlements Group is fit for purpose, including designating a Chair. (It is noted that the Group's remit also covers University library entitlements).

5.3. The **Chief Information Officer** is responsible for ensuring that appropriate processes and procedures are established to support this policy.

5.4. **Information Asset Owners** 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.

5.5. The **Secretary to the University Membership Categories and Entitlements Group** is responsible for ensuring that a summary of categories and associated entitlements is published and maintained.

5.6. The **IT Rights Authority Holders** are responsible for ensuring that requests for access for users who are neither staff nor students (e.g. contractors, temporary staff, research collaborators, and academic visitors) are appropriate, justified, fall within one of the approved categories and that any changes to users' circumstances impacting on their access entitlement are notified to University IT immediately.

6. DEFINITIONS

Identity means an "Identity" that should uniquely represent a real person.

Information Asset means 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.

Key Information Asset Owner means an Information Asset Owner shall be nominated by the Senior Information Risk Owner for each key Information Asset. The Information Asset Owners shall understand what information comprises or is associated with the asset, and the threats and vulnerabilities associated with it, and understand and communicate the importance and value of the asset to the University

Senior Information Risk Owner means 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

7. VERSION CONTROL

Document Name	IT Account Entitlement and Rights Policy	
UEB Policy Sponsor	Chief Operating Officer	
Policy Owner	Owen Hadall, Interim CIO	
Policy Author(s)	Helen Dennis, Senior Manager (Endpoints and Entitlements)	
Version Number	2.1	
Equality Impact Outcome and Form Submission Date	An assessment has been conducted and found no impact to protected characteristics. It noted that Welsh Language preferences are not recorded in the Identity Management System, but all communications from the system are bilingual.	11/05/2023
Privacy Impact Assessment outcome (where applicable)	A DPIA has been conducted. This policy supports maintenance of privacy by ensuring that users are allocated appropriate access rights and therefore if applied appropriate, positively supports privacy.	11/05/2023
Approval Date	25 May 2024	
Approved By	Chief Operating Officer (SIRO)	
Date of Implementation	1 June 2024	
Date of Last Review	19/02/2018	
Date for Next Review	Approved date + 3 years	
For Office Use – Keywords for search function	IT, Account, Access, Policy, Entitlements	