User Account Lifecycle Policy

Responsibility of: IT Services
Approval Date: 21st May 2019
Review Date: May 2020
Approved By: IT Steering Group
Introduction

1. Definitions and Purpose

1.1. A user account is a set of credentials and associated data that allows a specific person to log in to one or more University services. The account is used both to authenticate the person (confirm who they are) and to authorize them (confirm what University services and data they should have access to).

1.2. The lifecycle of a user account is the set of processes that control the creation, modification, and decommissioning of the account.

1.3. Controlling access to University data and systems is an essential part of protecting their confidentiality, integrity, and availability.

1.4. The lifecycle depends on the person and their affiliation with the University. For the purposes of this policy, we identify three very broad classes of user accounts:
   - Students
   - Employees – both full and part-time
   - Contingent workers – Contractors, temps, and third parties who have a formal relationship with the University that requires a user account.

1.5. It is important to note that within these broad classes there are different types of user accounts with different requirements, properties, and associated operational processes. This policy necessarily takes a high-level view.

1.6. Some accounts are not user accounts as they are not associated with a specific person. For example, service accounts are used by IT systems to log in to other IT systems. Such accounts are out of scope for this policy.

1.7. Some individuals may fall into multiple classes; in this case they should have multiple separate accounts.

1.8. Some user accounts are privileged, meaning they have been granted additional permissions beyond what is normally given. There are additional controls applied to privileged accounts. See the privileged account policy for more details.

2. Provisioning

2.1. New accounts for students are automatically provisioned based on their status in the Student Records System.

2.2. New accounts for employees are provisioned by IT Services when they receive notice of a new hire from HR Services.

2.3. New accounts for contingent workers are provisioned by IT Services when they receive notice of a new hire from the responsible manager.

2.4. Responsible managers must, when requesting a user account for a contingent worker, specify an end date for that account. If an extension to the account is required, they should notify IT Services. If the end date is not known, it should default to one year from the contingent employee’s start date, and the responsible manager should review access and request extensions accordingly.

2.5. Provisioning should normally follow the Account Provisioning processes which are published on the IT Services processes section of SharePoint. Exceptions may be made with ITMT approval.

3. Deprovisioning

3.1. Accounts for students are automatically deprovisioned based on their status in the Student Records System.
3.2. Accounts for employees are deprovisioned by IT Services when they receive notice from HR Services that the employee has left.

3.3. Accounts for contingent workers are deprovisioned by IT Services when they receive notice from the responsible manager that the employee has left.

3.4. Deprovisioning should normally follow the Account Deprovisioning processes which are published on the IT Services processes section of SharePoint. Exceptions may be made with ITMT approval.

3.5. If IT services believe a user account is no longer required, but they have not yet received notification, they may suspend the or block the account for security reasons. However, full deprovisioning will not occur until appropriate notice is received.

4. Data stored in individual-specific areas

4.1. Some data is stored by individuals in areas set aside for their own use, such as the contents of their email mailbox or OneDrive cloud storage.

4.2. In order to comply with data protection and privacy regulations, this individual data will only be retained for a brief period of time after the user account is deprovisioned. UWL does not always have control of this timing if the data in question is being stored in cloud-based storage services such as Office365.

4.3. It is the responsibility of students to ensure any individual data the University needs to retain after their course ends is secured beforehand.

4.4. It is the responsibility of the employee and their line manager to ensure any individual data the University needs to retain after the employee leaves the University is secured beforehand.

4.5. It is the responsibility of the contingent employee and their responsible manager to ensure any individual data they need to retain after the contract or formal relationship with the University ends is secured beforehand.

5. Changes to the details of accounts

5.1. User accounts have various meta-data associated with them, such as the user’s name and contact details.

5.2. Changes to the details of a student account should be made in the Student Record System, from which they will automatically be synchronized to the student’s account.

5.3. Changes to the details of an employee account should be made to HR, who will update their records and then pass the request onto IT Services.

5.4. Changes to details of a contingent worker account should be sent to IT Services by the responsible manager.

6. Changes to the access levels of user accounts.

6.1. Requests for changes to access levels should be made either by the data owner or by the line or responsible manager with the approval of the data owner.

7. Review of accounts and access levels

7.1. On a quarterly basis IT Services will review a sample of user accounts to confirm that they should exist and that they have the correct access levels assigned, following the User Accounts Review process which is published on the IT Services processes section of SharePoint.