UNIVERSITY OF
WEST LONDON

Privileged Account Policy

Responsibility of:	IT Services
Approval Date:	May 2020
Review Date:	May 2021
Approved By:	IT Steering Group

1 Introduction

1.1 A privileged account on an information system is one which has additional permissions above and beyond what is provided to a "normal" account on the system.

1.2 Privileged accounts, by their nature, attract a higher level of information security risk, and must be protected accordingly.

1.3 This policy applies to privileged accounts on both IT-managed information systems and business-managed information systems.

1.4 Changes to existing privileged accounts must be made with care. IT Services will bring all IT-managed privileged accounts in line with this policy by July 2020.

2 Principles

2.1 The use of privileged accounts must be kept to an absolute minimum. In particular, they must never be used to perform tasks that can be accomplished using a non-privileged account.

2.2 Privileged access to systems must be traceable to an individual.

2.3 Individuals with privileged access have been placed in a position of trust, and must at all times follow all applicable laws, regulations, policies, and procedures. Abuse of privileged accounts will be regarded as a serious disciplinary matter.

3 Privileged account lifecycle

3.1 Approval for the creation of a new privileged account must be given by the business owner of the information system.

3.2 Privileged accounts must always use strong, unique passwords, in accordance with the University password policy.

3.3 Privileged accounts should be reviewed regularly, and at least once a year, to confirm that they are still required.

3.4 Privileged accounts which are no longer required must be disabled immediately.

4 Segregation of privileged accounts

4.1 Privileged accounts should not be used to perform normal tasks. When a user needs to use a system to perform both privileged and non-privileged activity, they should either:

- Have two separate accounts, one privileged and one not.
- Have an account that normally runs without privilege but can have its permissions temporarily elevated when performing privileged tasks, for example by using the Microsoft Windows User Account Control (UAC) feature or the UNIX sudo command.

5 Local admin rights to user machines

5.1 Exceptionally, it is sometimes necessary for a user to have local administrator access to their University issued computer.

5.2 Requests for local admin rights must be made in writing and include a detailed justification. Such requests must be approved by both the user's Dean of College, Head of School, or Head of Central Service Department, as well as by IT Services.

5.3 Users who have been granted local admin rights are responsible for ensuring they follow the Acceptable Use of IT Assets policy and that they do nothing to compromise the security of the UWL network and IT infrastructure. For example, they must not:

- remove or modify UWL provided anti-malware software
- remove or modify features which permit IT Services to manage devices
- make changes to network configuration settings without IT approval.

5.4 IT Services will revoke local admin rights when necessary to protect the security of the UWL network and infrastructure.

5.5 IT Services themselves have a local admin account created on each user machine, for use only when a domain account cannot be used to administer the machine. Each account has a randomly generated password that is reset after each use and automatically every 5 days.

6 Active Directory

6.1 Privileged accounts in Active Directory are among the most critical to secure. For these accounts the University has implemented Microsoft's recommended practice of further segregating them into three tiers.

6.2 Tier 0 accounts, indicated with the prefix da, have direct control of enterprise identities. They can only log on interactively to Tier 0 assets such as domain controllers. Minimum password length is 20 and passwords must be changed every 60 days.

6.3 Tier 1 accounts, indicated with the prefix sa, have control of enterprise servers and applications, and can only log on interactively to these Tier 1 assets. Minimum password length is 15 characters and passwords mush be changed every 60 days.

6.4 Tier 2 accounts, indicated with the prefix wa, have control of user workstations and devices, and can only log on interactively to these Tier 2 assets. Minimum password length is 15 characters and passwords mush be changed every 90 days.

6.5 Active Directory administrative accounts are always separate from normal user accounts and in particular do not have mailboxes. All administrator accounts must have Multi Factor Authentication (MFA) enabled using the Microsoft Authenticator app (and not SMS messaging). Based on the nature of their work, some members of staff may require administrative accounts in more than one tier. These accounts must be separate and have unique passwords.

6.6 Creation of new administrator accounts must be approved by the ICT Change Request Board or by the CIO. If a temporary administrator account is needed, it must have an expiry date set. Changes to administrative accounts will be monitored and notification made of any such change to the Information Security Manager.

6.7 The built-in Active Directory administrative account is Tier 0. It is only to be used in an emergency, must be kept disabled at all other times, and the password should not be known by any member of staff, but instead randomly generated, written down, and stored securely in a safe. This will be flagged as a “honeypot” account, and the Information Security manager notified of any instance of its use.

7 Default/generic privileged accounts

7.1 Many information systems are supplied with pre-defined, generic privileged accounts, such as "admin", “superuser” or "root”.

7.2 If possible, these should be disabled and separate privileged accounts, assigned to named administrators, used instead.

7.3 Where these accounts must be kept active, their password must be immediately changed from the default, and if possible, the user name should also be changed.

7.4 Passwords for shared or generic privileged accounts must be encrypted when at rest and in transit.

7.5 When a user who has had access to the password of a shared or generic privileged account leaves the organization, that password must be immediately changed.

8 Monitoring & Reporting

8.1 Where technically possible, privileged account usage shall be logged, and the logs stored in a location which the privileged account does not have access to.

8.2 The Information Security Manager will report to the IT Management Team (ITMT), at least yearly, on the usage of privileged account in UWL.