DCU Unit4 Business World
(Agresso) User Access Management Policy
# Table of Contents

**Purpose** .................................................................................................................................................. 2  
**Scope** .................................................................................................................................................... 2  
**Policy Statement** ..................................................................................................................................... 2  
  - Active Directory (AD) ............................................................................................................................. 3  
  - DCU ICT Security policies ....................................................................................................................... 3  
  - User Protocols ....................................................................................................................................... 4  
  - Account Privileges ................................................................................................................................. 4  
  - Separation of Duties ............................................................................................................................... 4  
  - Generic Accounts .................................................................................................................................... 5  
  - Breaches .................................................................................................................................................. 5  
  - Third Parties .......................................................................................................................................... 5  
  - Account Deactivation .............................................................................................................................. 5  
  - Account Auditing .................................................................................................................................... 6  
**Document Change Management** ........................................................................................................... 6  
**Version Control** ...................................................................................................................................... 7
Purpose
This policy provides high-level information and the prerequisites required to access the Dublin City University (DCU) financial information system, Unit4 Business World (Formerly called Agresso). This policy is complemented, and should be considered in conjunction with, a series of sub-policies, procedures and guidelines which define access and security in more specific detail for the individual components of the DCU Information and communications technology (ICT) environment.

These sub-policies and related documents are published and accessible on the DCU ISS website.

The purpose of this policy is to protect Dublin City University’s financial information and Communications Technology (ICT) resources from accidental or malicious disclosure, modification, or destruction, while also preserving the open information sharing requirements of this information system.

This policy lays the foundation for a common understanding of financial information security at DCU based on the generally accepted information security principles of Confidentiality, Integrity and Availability.

- **Confidentiality** limits information access to authorised users.
- **Integrity** protects information against unauthorised modification.
- **Availability** ensures that information is accessible when needed.

Scope
This policy applies to all staff, students, and authorised third parties of the University and its subsidiary companies, who use the Unit4 Business World system. This includes all schools, research centres, learning centres, employees, consultants, contractors, agents and authorised users accessing DCU’s Unit4 Business World (Agresso) financial information system.

Within the context of this policy, financial information refers to all financial information processed, stored, used or transmitted in any medium or form.

Policy Statement
User access to Unit4 Business World (Agresso) will only be granted where there are valid business reasons. All Unit4 Business World (Agresso) access requests must originate from either the Purchase Administrator (Buyer) for their department and / or a DCU finance office authorised requestor.
Staff, Students and third parties are authorised individually to use the DCU Information and Communications Technology (ICT) environment. Accounts are created for staff and students on systems and networks as appropriate. Each user is responsible for the data entry and the use of their own account. Users are responsible for all activities carried out under their account.

Unit4 Business World (Agresso) user account creation will only occur when a person has been registered with an active staff or student ID and a corresponding Active Directory (AD) login.

Active Directory (AD)
Active Directory provides central authentication and authorisation services for DCU Windows based computers. It also allows DCU network administrators to assign policies, deploy software, and apply critical updates to networked computers.

When a user attempts to log on to a windows computer that is in Active Directory, it automatically attempts to verify the user’s password with the Active Directory server.

DCU ICT Security policies
All devices attaching to the DCU network must comply with the relevant DCU ICT security policy. These are outlined at this link.

In particular, your attention is drawn to the following security policies.

- ICT Security Policy
- Mobile Computing Security Policy
- Use of Computer Resources - Code of Conduct
- Password Policy
- Remote Access Policy

If you are connecting to the network from a remote location, please consult the Remote Access Policy.

The finance system helpdesk cannot set up any user who does not have a registered and active AD User account.

University staff requiring access to Unit4 Business World (Agresso) must submit a ticket request to do so via the Finance Systems Helpdesk (see the Finance Office Webpage).

Completion of the request will determine the type and range of access provided.
All data and information stored on DCU’s financial information systems is considered confidential and must be handled in accordance with the University’s Data Classification Policy.

User Protocols
Users are to ensure that their computer has screen protection to prevent access by another person when their computer is unattended and the user is logged into Unit4 Business World (Agresso).

Users should log out of Unit4 Business World (Agresso) modules they are not using and completely log out of Unit4 Business World (Agresso) at the end of each workday.

Account Privileges
A user will be provided with access appropriate for their role at the University. If a user’s role changes, their access may also change to reflect the requirements of their new role.

If access requirements change then it will be necessary to submit a ticket request to do so via the Finance Systems Helpdesk (see the Finance Office Webpage).

Separation of Duties
Separation of duties and responsibilities must be adhered to when creating and maintaining all Unit4 Business World (Agresso) accounts to ensure no one person has the ability to circumvent normal auditing processes.

It is the responsibility of the School, Faculty, Department, Research Centre, Company and/or Strategic Business Unit to:

- maintain clearly defined roles and permissions within each area when setting up and managing user accounts
- ensure that users' access privileges and assigned roles are approved and consistent with business needs.

The Finance systems helpdesk will apply a defined set of roles (menu structure and data access) to each user based on the information provided in the Agresso new user form. This will ensure separation of duties can be strictly controlled and adhered to.
Generic Accounts
The use of shared, guest, anonymous and other such generic user accounts will be strictly avoided where possible. If guests or shared accounts must be used to access Unit4 Business World (Agresso), they must be supported by a process that identifies the user of the account, such as a record of account allocation, as well as other compensating controls. The use/continued use of such accounts must be supported by valid business and operational reasons, in line with this policy and other policies of the University and its subsidiary companies.

Breaches
Breaches of these guidelines will be dealt with according to the ISS Access Control policy and may result in disciplinary action as provided for under the applicable Employment Agreements and ordinances.

Users must not allow other staff or third parties to use their Unit4 Business world (Agresso) user accounts.

Staff, students and associates learning of any violation of this guideline are obligated to bring this matter to the attention of an appropriate staff member within the University immediately.

Third Parties
In the normal course of events, DCU finance office may contract for ICT services. Representatives of these contracted companies and/or individuals must follow all University policies.

Schools, Departments, and all other Strategic Business Units are expected to inform all third party users of the Unit4 Business world (Agresso) user access management policy and all other relevant policies. In addition, they must also provide oversight of the contractor and contractor representatives during the time they have access to Unit4 Business world (Agresso).

All devices attaching to the DCU network must comply with relevant ICT Security policies.

Account Deactivation
Unit4 Business world (Agresso) access will be provided for the duration of a user’s employment or contract with DCU and/or its subsidiary companies.
Account deactivation shall occur upon termination of an authorised user’s relationship with DCU and/or, where appropriate, where a change in duties alters an authorised user’s access requirements.

Deactivation is initiated by an authorised member of staff within the School, Faculty, Department, Research Centre, Company and/or Strategic Business Unit submitting a ticket request to do so via the Finance Systems Helpdesk (see the Finance Office Webpage).

The Director of Finance, or nominated delegate, may revoke the access of an authorised user at any time in response to an incident, breach of DCU policy, or for risk management or moderation purposes.

Events triggering account deactivation include, but are not limited, to the following:

- Notification from Human Resources of the end of a user’s employment.
- Notification from the Purchase administrator (buyer) that a user no longer requires access and/or financial delegation.
- Review by Finance Systems Team in conjunction with HR and Payroll records.

Account Auditing

Periodic auditing of user accounts will be performed by the Finance systems helpdesk team to identify and revoke any non-active and unused accounts or to perform the re-allocation or revocation of privileges. Purchase Administrators and / or budget holders may be requested to endorse or verify an authorised user list provided as part of each audit cycle.

Document Change Management

Dublin City University believes that it is important to keep this policy current in order to ensure that it addresses security issues accurately and is up-to-date with evolving business issues and technologies. This policy is a living document that will be reviewed annually and/or updated as needed.

The Director of the DCU finance Office will draft necessary changes and have them reviewed and approved by the Executive Group of DCU as appropriate. The Director of Finance, the Deputy Director of Finance, and Finance Systems helpdesk team members will communicate changes to the DCU community. Anyone in the University can determine the need for a modification to the existing policy. Recommendations for changes to this policy should be communicated to the Director of Finance.
End.