Global Banking School
+44 (0) 207 539 3548

info@globalbanking.ac.uk

www.globalbanking.ac.uk

891 Greenford Road, London

UB6 0HE

GBS Access Control Policy

GBS Access Control Policy

Contents

Global Banking School Access Control Policy

1. Purpose and Scope

1.1 Global Banking School (GBS) recognises that information is a valuable asset and access to it must be managed with care to ensure that confidentiality, integrity, and availability are maintained.

1.2 GBS provides access to information assets, accounts, systems, and resources. This policy outlines the rules relating to authorising, monitoring, and controlling access to GBS information systems; governing the use of all IT resources across all sites on which GBS operates. It provides the guiding principles and responsibilities to ensure GBS’ access control objectives are met.

2. Roles and

Cloud Hosted Servers

End user compute devices (laptops/desktops etc.)

Mobile devices (phones, tablets etc.)

4.3 **Account Access**

4.3.1 All GBS users must be identified and authenticated as a valid user prior to access being granted to IT systems, computer resources, allowing activities performed traceable to individual account holder.

4.3.2 Identification and authentication of users and systems enables the tracking of activities to be traced to the person responsible. All GBS members shall have a unique identifier (user ID) for their personal and sole use. Shared, group and generic user IDs are not permitted.

4.3.3 All GBS members must be educated that they are not permitted to allow their user ID to be used by anyone else. They must be made aware of this and how to store them. A process must exist for issuing and revoking the user IDs. Redundant user accounts must be monitored and managed.

4.4 **Account Privileges**

4.4.1 GBS account profiles and privileges are to be restricted to the minimum required for individual account holders to fulfil their role. Access to operating systems and application management is to be restricted to designated administrators and support staff associated with the management and maintenance of the respective platforms.

4.4.2 GBS user-accounts are only to remain active for the period required for individual users to fulfil the needs for which they were granted and should consider the following:

Privileges associated with each system need to be identified.

Privileges should be allocated on a need-to-use basis.

An authorisation process and record of privileges should be maintained.

Development and use of system routines should be promoted.

5.4 **Account Restrictions**

5.4.1 In accordance with ICT

the Staff Handbook and must be followed to achieve GBS policy objectives. Reference should also be made to the, GBS Data Protection Policy, GBS Data Classification and Handling Policy, GBS Privacy Policy and GBS ICT Policy. Information on other related policies is available from GBS Academic Standards and Quality Office (ASQO).

9. Audit and Compliance

9.1 GBS Access Control Policy may be amended by GBS at any time. GBS will ensure that all staff receive appropriate training to enable them to comply with this policy. GBS will regularly test our systems and processes to monitor compliance. Any issues related to the monitoring and review of this policy, please contact asqo@globalbanking.ac.uk.

10. Data Protection and Confidentiality

10.1 GBS is registered with the Information Commissioner's Office as a Data Controller. Details of the School's registration are published on the Information Commissioners

Annex 1 – GBS Access in Special Circumstances

Special circumstances include, but are not limited to:

Special Circumstances	Detail
Information Technology (IT) Security Team	The Information Technology (IT) Security team may access accounts and user data. Some examples of when such access may be required include: Business continuity. To detect and prevent crime (including but not limited to, fraud and unauthorised access to computer systems) System security protection: Virus, malware, hacking and other infected device and account prevention. To establish the existence of facts relevant to the business of the institution (for example - where a case of suspected plagiarism is being investigated and there is sufficient evidence, the communications and/or files may be examined without prior user consent). Misuse, abuse, and illegal activity investigation. Access request must be sent to the Data Protection Officer (DPO) for review.
Regulatory Requests	A request for information to satisfy a regulatory request (e.g., Data Subject Access Request-DSAR) can be made, please refer to GBS DSAR Policy. Access request must be sent to the Data Protection Officer (DPO) for review.
Previous Account Owner	A request for information held against a previously active account by the account owner may be approved only after a careful review and on a case-by-case basis. Access request must be sent to the Data Protection Officer (DPO) for review.
Staff Account Access by Department	Requests must be sponsored and approved by the Head of Department or any member of GBS Senior Management Team

	(or recognised designate). Access request must be sent to the Data Protection Officer (DPO) for review.
Student Account Access by Department	Requests must be sponsored and approved by the Head of Department or any member of GBS Senior Management Team (or recognised designate). Access request must be sent to the Data Protection Officer (DPO) for review.
Public Authorities	Requests must be sponsored and approved by the Head of Department or any member of GBS Senior Management Team (or recognised designate). The relevant documentation must be completed. Access request must be sent to the Data Protection Officer (DPO) for review.
Medical or Deceased User Account Access	Requests must be sponsored and approved by the Head of Department or any member of GBS Senior Management Team (or recognised designate). The relevant documentation must be completed. Access request must be sent to the Data Protection Officer (DPO) for review.