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

Document title	GBS Access Control Policy
Oversight Committee	Executive Board
Policy lead (Staff member accountable)	Managing Director
Approved by	Executive Board
Approval date	February 2022
Date effective from	February 2022
Date of next review	February 2025
Version	1.0

Related GBS policies

- GBS Student Code of Conduct
- GBS Student Charter
- GBS Student Disciplinary Policy
- GBS Equality and Diversity Policy
- GBS Records Management and Retention Policy
- GBS Anti-Harassment and Anti-Bullying Policy
- GBS Data Protection Policy
- GBS Data Classification and Handling Policy
- GBS Privacy Policy
- GBS IT Security Policy

External Reference Points

1. Information Commissioner’s Office, Accessed online at: https://ico.org.uk/
2. UK Public General Acts, *Data Protection Act 2018*, Accessed online at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

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 Responsibilities

2.1 GBS Senior Management Team: Responsible for ensuring that systems are in place to meet all of GBS' legal obligations, including the establishment and monitoring of systems of control and accountability. They must ensure staff are made aware of this policy and must develop and encourage good information handling practices within their areas of responsibility.

2.2 All GBS Members: (including staff, academics, associates, contractors, temporary staff, and any students who are carrying out work on behalf of GBS) must abide by relevant GBS IT policies. All GBS members must only use their account and access in accordance with GBS ICT Policy, secure their credentials and be responsible for the systems, services, and data within their control.

2.3 Line Managers: Responsible for ensuring that their staff are aware of this policy and comply with its requirements. All line managers must only permit access requests that have adequate and appropriate justification based on the requester's business need and must document access requests.

2.4 Information Asset Owners/Technician: Responsible for periodically reviewing access to their assets and investigating any anomalies. Review periods are based on the risk rating of a given asset.

2.5 GBS Academic Standards and Quality Office (ASQO)[1]: Responsible for monitoring and review of this policy. They must ensure that this policy is kept up-to-date and that it is relevant to the needs and obligations of GBS and can be contacted on asqo@globalbanking.ac.uk.

3. Legislation and Compliance Framework

3.1 It is important that access to data, information, and records created and held at GBS are managed with the appropriate level of access as set out in this policy.

3.2 Compliance with this policy enables consistent controls to be applied throughout GBS practices, minimising exposure to security breaches, whilst allowing systems and security administration and technical support staff to conduct their activities within the framework of the law. This policy aims to ensure that, by having the appropriate access controls in place, the right information is accessible by the right people at the right time and that access to information, in all forms, is appropriately managed and periodically audited.

4. User-Access Management

4.1 GBS controls access to information assets based on business requirements and compliance. The objective is to prevent unauthorised access to information systems. User access management covers all stages of user access, from initial registration, through to changes in role, to deregistration and revocation of access. The security of systems, networks, applications, and databases is heavily dependent on the level of protection of user IDs, passwords, and other credentials that provide access to it. Hence, protecting the credentials that provide access to information is indirectly protecting the information.

4.2 Account Creation

4.2.1 User accounts for any GBS IT system will only to be created on the correct authority. It is the responsibility of the IT system technician who is creating user accounts to confirm that the correct level of authority has been granted. IT systems refers to:

- Physical Servers
- Virtual Servers

[1] *Formerly known as GBS Quality Assurance Team*

- 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[2] 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.

[2] *A “privilege” is any facility in a multi-user system that enables one user to override system or application controls.*

- Development and use of system routines should be promoted.
- Privilege identifiers should be different from that for normal business use.

5. Security and Access

5.1 Appropriate levels of security must be in place to prevent the unauthorised or unlawful use and disclosure of information. All records in any format must be held in accordance with GBS ICT Policy and GBS Data Protection Policy. Records must be stored in a safe and secure physical and digital environment, taking account of the need to preserve important information in a useable format enabling access commensurate with frequency of use.

5.2 GBS Data Classification and Handling Policy describes five information classifications to help staff identify the level of security the information requires. The five classifications include: Public, Restricted, Private, Internal and Confidential. Please refer to Annex 2 - Information Classifications for a brief outline on these.

5.3 Monitoring Access and Use

5.3.1 Systems will be monitored to detect deviation from GBS Access Control Policy and record events to provide evidence in case of security incidents. The Information Asset Owner/Technician must establish the logging and monitoring requirements for business auditing purposes.

5.3.2 Designated staff members responsible for the following areas must establish the logging and monitoring requirements for the relevant purposes:

- Security
- Incident investigations
- Audit
- Fraud
- Legal

5.3.3 A process for capturing logging and monitoring requirements must be developed. Audit and event logs will need to be adequately secured, possibly centrally and separately from privileged-level employees (separation of duties).

5.4 **Account Restrictions**

5.4.1 In accordance with ICT Policy all GBS members must not attempt to access systems, applications, or data which their user account does not naturally provide access to and for which they have not been granted specific permission.

5.4.2 All GBS members may only use IT systems and computer accounts that have been officially authorised to use. Using a computer for which staff have not been given permission to use could potentially constitute an infringement under the Computer Misuse Act 1990. Account holders must not divulge their logon credentials to anyone else or allow any other person to use their computer account at any time, regardless of whether the other person is a member of GBS. Any misuse of a computer account may be attributed to the account holder in the first instance.

6. Access Reviews

6.1 Internal GBS user privileges are to be reviewed on a regular basis with an annual access control audit and withdrawn where the circumstances of those who have been granted privileges no longer warrant such access. It is recommended that where an access review identifies an access anomaly, it will be treated as a potential incident and investigated by the asset owner/technician and information security team.

7. Access in Special Circumstances

7.1 There are special circumstances where extra or privileged access is needed. For all cases, access to any GBS information contained within an account or information pertaining to the activity of an account, is carefully restricted and must only be carried out with the appropriate authorisation and safeguards in place. Please refer to Annex 1 which outlines the approach taken for special circumstances.

8. Related Policies

8.1 Access Control Policy does not exist in isolation. It connects to functions such as management of personal information for compliance with the Data Protection Act, Information Security, and Information Assurance. This policy is accompanied by 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 website. GBS as a Data Controller shall implement appropriate technical and organisational measures to ensure that processing of personal information is performed in accordance with the UK General Data Protection Regulations (UK GDPR) and under the Data Protection Act 2018 (DPA).

10.2 All GBS staff and students should be clearly informed about the limits of confidentiality in terms of information sharing in line with data protection law. Please refer to GBS Data Protection Policy for further guidance.

11. Alternative Format

11.1 This policy can be provided in alternative formats (including large print, audio and electronic) upon request. For further information, or to make a request, please contact:

- **Name:** Welfare Management Team
- **Position:** Welfare Officer/Manager
- **Email:** welfare@globalbanking.ac.uk

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.

Annex 2 – GBS Information Classifications

GBS has five information classifications to help staff identify the level of security the information requires. The five classifications include: Public, Restricted, Private, Internal and Confidential.

CLASSIFICATION	DEFINITION
Public	Data that can be freely disclosed to the public. Examples include GBS contact information, location, job descriptions and prospectus.
Restricted	Highly sensitive internal data. Disclosure could negatively affect operations and put GBS at financial or legal risk. Restricted data requires the highest level of security protection by everyone working at GBS from staff to students to partners etc. For example, Committee papers and documents marked for the attention of a specific reader.
Private	Private information is typically a classification of information that individuals use for themselves. It is a broad and general term that is more ambiguously used than other privacy terms. For example, emails to colleagues regarding work buffets or quizzes etc.
Internal	Data that has low security requirements, however, is not meant for public disclosure such as marketing research, academic handbooks.
Confidential	Confidential information is information shared with only a few people, for a designated purpose and can be shared with others within GBS. The person who is

	receiving the information from you, the receiver, generally cannot take advantage and use your information for their personal gain, such as giving the information out to unauthorised third parties. These can include documents prepared for publication or unpublished research data.