Document title	GBS Access Control Policy
Version	V1.1
Approved by (Oversight Committee)	Board of Directors
Policy lead (Staff member accountable)	Managing Director
Date of original approval	February 2022
Date of last review	December 2024

Contents

1. Purpose and Scope 4

2. Roles and Responsibilities 4

3. Legislation and Compliance Framework 5

4. User-Access Management 5

5. Security and Access 7

6. Access Reviews 8

7. Access in Special Circumstances 8

8. Related Policies .... 8 Data ProteSf....

9. Audit and Compliance 9

10. Data ProteSf874 0Ut an

Global Banking School Access Control Policy

1. Purpose and Scope

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 madi must be 7ng (0.00000887d)-3(7

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

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

Annex 1 GBS Access in Special Circumstances

Annex 2

	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.