Global Banking School
+44 (0) 207 539 3548
info@globalbanking.ac.uk
www.globalbanking.ac.uk
891 Greenford Road, London
UB6 0HE

GBS Password Policy

Document title	GBS Password Policy
Version	V1.0
Approved by (Oversight Committee)	Information Management Group (IMG)
Policy lead (Staff member accountable)	Managing Director
Date of original approval	January 2025
Date of last review	NA
Changes made at the last review	NA
Date effective from	January 2025
Date of next review	January 2028

Related policies

- GBS ICT Policy
- GBS IT Acceptable Usage Policy
- GBS Equality and Diversity Policy
- GBS Freedom of Speech Code of Practice
- GBS Anti-Harassment and Anti-Bullying Policy – Staff, Students
- GBS Student Charter
- GBS Student Disciplinary Policy and Procedure
- GBS Staff Disciplinary Policy
- GBS Email Usage Policy
- GBS Data Protection Policy

External Reference

Password administration for system owners by National Cyber Security Centre, Accessed online at: https://www.ncsc.gov.uk/collection/passwords

Password policy: updating your approach by National Cyber Security Centre, Accessed online at: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

Three random words or #thinkrandom, Accessed online at: https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

GBS
GLOBAL BANKING SCHOOL

Contents

GBS
GLOBAL BANKING SCHOOL

Global Banking School Password Policy

1. Introduction/Policy Statement

1.1. This document outlines the Password Policy and guidance.

1.2. All GBS IT Systems use password authentication as a minimum requirement. IT systems owned by departments and faculties shall be secured by MFA wherever possible.

2. Purpose

2.1. Global Banking School (GBS) recognises the vital role of Passwords which are keys to its systems, data and information The purpose of this policy is to provide guidance to all staff, students, visitors, or any individual using GBS systems in line with best practises and industry standards for the implementation of an organisation wide Password Policy.

3. Scope

3.1. This policy applies to all GBS users, and third parties required to authenticate with GBS IT systems and services. GBS Users include staff, students, visitors, and other associate roles.

4. Terminology

4.1. Shall or Must – This term is used to state **a mandatory** requirement of this policy.

4.2. Should – This Term is used to state a **recommended** requirement of this policy.

4.3. May- This term is used to state an **optional** requirement of this policy.

4.4. Shall not or must not- This term is used to state an **absolute prohibition** requirement of this policy.

4.5. Should not- This term is used to state a **not recommended** requirement of this policy.

5. Policy

5.1. The password policy applies to:

- **GBS Staff** using **GBS IT devices** to login GBS applications/network.
- **GBS Staff** using **Personal device** to login GBS Applications/network
- **GBS Student** using **GBS Lab or Classroom IT devices** to login GBS Applications/network
- **GBS Student** using **Personal device** to login GBS Application/network

5.2. All GBS users (Staff/Students) must ensure the following for their passwords to access GBS Applications:

Guideline	**Password must be unique.**
	Password must not be revealed.
	Change Password when you know, or suspect password has been compromised.
	Must use Multi-factor Authentication (MFA) where available. MFA is must for Cloud Services
Minimum Length	**Twelve (12) characters and more.**
Maximum Length	**No maximum length.**
Account Lockout	**Ten (10) attempts post unsuccessful wrong password entry.**
Password Expiry	**No arbitrary expiry of Passwords.**
Avoid:	**Repeated Usage of password.**
	Family and pet names, username, date of births, personal information, favourite sports team.
	Same passwords for different systems and applications (email/banking/application/social media).
	Shared username/password.
Recommendation	**Use multiple words in Passwords- recommends Three Random Words.**
	Use system-based password reset option to reset password if available.

5.3. IT team will provide guidance to users to enrol into multi-factor authentication.

5.4. All GBS users, members and third party shall notify IT Services, if they know or suspect that their password has been compromised.

5.5. This policy should be read in conjunction with the accompanying guidance on passwords. Please refer to GBS – Password Guidance.

6. Exceptions

6.1. There may be additional requirements for privileged users/IT administrators as and when approved and managed by IT Services.

7. Non-Compliance

7.1. GBS User who violate this policy may face disciplinary consequences in proportion to their violation. Management will determine how severe offense is and take the appropriate action.

8. Data Protection and Confidentiality

8.1. GBS is registered with the Information Commissioner's Office as a Data Controller. Details of GBS's registration is 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)

8.2. The UK GDPR and DPA regulates the use and storage of personal information (i.e., any information which identifies a living individual) on computing systems. It is the user's responsibility to ensure that their information and computer usage complies with this law. Failure to do so could result in criminal charges being brought against both user and GBS.

9. Policy Review

9.1. This policy may be amended by GBS at any time and will be reviewed annually to ensure it is fit for purpose. Any issues related to the monitoring and review of this policy, please contact asqo@globalbanking.ac.uk.

10. Alternative Format

10.1. 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 the Academic Standards and Quality Office at asqo@globalbanking.ac.uk.

APPENDIX A - Glossary

GBS: Global Banking School

NCSC: National Cyber Security Centre

IT: Information Technology

ICT- Information and communications technology

MFA: Multi-factor Authentication

OTP: One Time Password

BYOD: Bring Your Own Device