Multi-Factor Authentication Procedure

Standard Title: Multi-Factor Authentication Procedure

Standard Category: COLLEGE ADMINISTRATIVE

Standard Number: 1

Standard Version: 1

Standard Owner: VP Digital Transformation and Chief Information Officer

Approval Date: Click or tap to enter a date.

Effective Date: Click or tap to enter a date.

Standard Approver: Technology Management Committee

Review Period: Annually and as needed

Reviewed: 1/14/2025

Revised: N/A Click or tap to enter a date.

---

1. Purpose

George Brown College (GBC) is committed to advancing the security of its Information Technology Services (ITS) resources with controls that support secure access to employee and student accounts. This procedure outlines the Multi-Factor Authentication (MFA) requirements to enhance the security of GBC's User accounts and safeguard sensitive data from unauthorized access, modification, disclosure, or misuse. Implementing MFA adds an additional layer of security that further validates user identities beyond usernames and passwords by requiring supplementary authentication information.

This procedure is designed to mitigate the risk of security breaches, deter unauthorized usage, and protect the integrity of GBC's Information Systems, ensuring a secure environment for our Users.

2. Scope

This procedure governs all Users with a GBC (GBC) account, including students, employees, consultants, contractors, sub-contractors, vendors, temporary workers, guests, trusted partners, alums, and agents of GBC.

3. Definition of Terms

Please see this link for all Cyber Security Definitions.

4. Procedure

4.1 Multi-Factor Authentication Use

4.1.1 Users must maintain a personal device, such as a smartphone or tablet, to install the College's designated authenticator application (e.g., Microsoft Authenticator) for accessing GBC's Information Systems. The College will not supply smartphones or tablets for the purpose of MFA.

4.1.2 Users may be granted time-limited exceptions for not installing the College's approved authenticator application. In such cases, users must utilize an alternative college-approved or supplied authenticator solution (e.g., hardware tokens). Users are responsible for the reasonable costs of lost, stolen, or damaged hardware tokens and must return college-provided hardware tokens upon graduation or leaving the college.

4.1.3 The VP, Digital Transformation and Chief Information Officer or their delegate may grant exceptions to using the College's chosen authenticator application based on significant demonstrated needs (not preferences) after evaluating the applicable risks and costs.

4.1.4 Users are responsible for securely managing their authentication credentials, including but not limited to usernames, passwords, smartphones/tablets, and hardware tokens.

4.1.5 Users shall not use any hardware token that does not belong to them. Any lost and found hardware tokens or other GBC-owned devices must be returned to the original owner or ITS.

4.1.6 Users shall immediately report any loss or theft of their hardware token or other GBC-owned devices to the Help Desk at (416) 415-5000 x4357.

5. Compliance

As a GBC User, you must comply with this MFA procedure, which is governed and enforced under the Acceptable Use Policy (AUP) and the broader Cyber Security policies.

The ITS department is responsible for monitoring adherence to these requirements. Non-compliance or failure to adhere to any of the provisions outlined in this procedure or aforementioned policies may lead to disciplinary actions commensurate with the severity of the offense per applicable academic and administrative codes of conduct and collective bargaining agreements.

6. Related Materials

This procedure was developed according to the ISO 27000 family of standards, specifically ISO 27001: 2022—Information Security, Cyber Security, and Privacy Protection—Information Security Management Systems—Requirements.

For more information, please refer to the MFA Frequently Asked Questions.

7. Related Policies

- Acceptable Use Policy
- Cyber Security Policy
- Employee Code of Conduct – Academic
- Employee Code of Conduct - Admin
- Employee Code of Conduct - Staff