Multi-Factor Authentication Policy

Purpose

George Brown College is committed to advancing the security of its Information Technology (IT) resources with controls that support secure access to employee and student accounts.

Background

The College issues accounts to users, including employees, students and others. Accounts provide user access to College IT resources, such as e-mail and secure file storage.

Access to accounts can create a risk of fraudulent account use and a risk to the confidentiality of information that can be accessed via those accounts.

Multi-factor authentication (MFA) is a method of authentication in which a user is granted access to an IT resource only after successfully presenting two or more pieces of evidence as part of the authentication mechanism. MFA has become an important security control, used widely by educational institutions and other organizations, to provide enhancements in the security of access to accounts, data, and resources.

George Brown College is adopting MFA as part of its ongoing efforts to ensure the safety and security of its community while minimizing its cost and administrative burden.

Scope

This Policy governs all users' access to accounts and College information technology resources.

Definitions

User: An individual with access to George Brown College information and/or information systems, such as students, employees, board members, contractors, consultants, and temporary workers.

Policy

1. The College shall implement and maintain MFA for all College information technology resources that Users can access over the internet except those information technology resources that are deemed exempt by Cybersecurity.
2. Cybersecurity shall conduct a documented risk assessment for every exempt IT resource at least annually and, as part of the analysis, create and oversee the implementation of an appropriate risk mitigation plan.
3. The College has decided to implement MFA by using an authenticator application that is to be installed on User devices. The College shall not collect or use any data from the application and shall explain to Users how they may access information that describes the application developer's privacy practices.
4. Users shall access College information technology resources by way of the College's chosen authenticator application. Cybersecurity or Human Resources may grant an exception to individuals who establish a significant demonstrated need (and not preference) and after weighing any such need against the applicable risks and costs. Exceptions are ordinarily to give individuals time to comply and ordinarily will be time-limited. The process to apply for an exception can be found on GB Community.
5. The College may require Users who are granted exceptions to leverage an alternative means of authenticating via MFA and to bear responsibility for the reasonable costs of lost, stolen and damaged hardware.

Related Policies

Acceptable Use Policy

Employee Codes of Conduct

Information Technology Policy

Student Acceptable Use (of Technology) Policy

Student Email Policy