Authentication and Password Policy

Category: Operations
Approval: PVP
Responsibility: Associate Vice President, IT
Date: July 13, 2020

Definitions:

Username: A username is a string of characters that are assigned to a user to uniquely identify them on a computer system.

Password: A password is a string of characters that is only know to a user. Combined with their username, a password is characterized as "something you know" that would allow a user access to university systems.

Multi-Factor Authentication (MFA): MFA is an account security protection that helps protect accounts from potential compromise by requiring more than just a username and password to prove one's identity during login. In addition to something you know (your password), MFA utilizes one or more additional factors to include: something you have (such as a hardware token) and/or something you are (such as your fingerprint) before granting access.

Hardware Token: A hardware device such as a USB key or a number generator, which can be physical or in the form of a mobile application, that is used in MFA.

Highly Sensitive Data: Data, Information, or intellectual property in which the University has a legal interest or ownership right and is intended for only limited dissemination. Such materials, if compromised, could cause significant and/or long-term harm to the University. Please refer to the Highly Sensitive Information Policy for more detail.

Credentials: A unique combination of username and password that allows a user to access any university system for which they have been granted authorization.

System Level Privileges: In computing, a **system level privilege** is defined as the delegation of authority to perform security-relevant functions on a computer system. A privilege allows a user to perform an action with security consequences. Examples of various privileges include the ability to create a new user, install software, or change kernel functions.

Group Memberships: In computing, the term **group** generally refers to a grouping of users. In principle, users may belong to none, one, or many groups. The primary purpose of user groups is to simplify access control to computer systems.

Application: A program or group of programs designed for end users.

Application Developer: An Application Developer creates or writes programs for a particular operating system, the web or a device

Purpose/Reason for Policy:

The purpose of this policy is to ensure that enhanced account security is enabled for all user accounts to help protect against unauthorized access to personal, private, and confidential information.

Scope of this Policy:

This Policy applies to all administrators, faculty, students, staff, volunteers, authorized third party agents, contractors, and students employed, or contracted by, Trent University ("the University"), and its affiliates, who, as part of their role and responsibilities have Trent credentials to access any of our systems.

Policy Statement:

Account and Username Allocations:

1. Accounts are issued as per the university's Account Privileges Policy.
2. Usernames are defined and distributed by the university's IT department.
3. Usernames issued by the university should not be used as usernames on any systems or services not in the control and custody of the university. If an assigned university e-mail must be used on an external system as a username, then a different password than the one used for the university account must be used.

Passwords:

1. Password Creation
    a. All user-level and system-level passwords must conform to the ***Password Construction Guidelines*** published and enforced by the IT department.
    b. Users must use a unique password for their university account and passwords should never be reused.
    c. User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
2. Password Change
    a. Passwords need to be changed when there is reason to believe a password has been compromised. In the event that a compromise has been identified through IT, notice will be sent to the user and the account may be disabled or have the password reset as a means of preventing further compromise.
    b. Automated password strength testing may be performed on a periodic or random basis by the university's IT department or its delegates. If a non-conforming password is discovered during one of these scans, the user will be required to change it to be in compliance with the ***Password Construction Guidelines***.
    c. Users must change their password using the ***Change Password*** functionality offered through the university's portal.
    d. Users must populate an alternate e-mail address and/or mobile number, through the university's portal, to utilize the university's ***Forgotten Password*** functionality.
3. Password Protection

a. Passwords should not be shared with anyone, including supervisors and co-workers. All passwords are to be treated as Highly Sensitive Data as per the University's policy on Handling Sensitive Information.
b. Passwords must not be inserted into email messages, through text messaging applications, or any other form of unencrypted electronic communication.
c. Passwords must never be entered in response to an e-mail purporting to be from the university's IT department. The university's IT department will NEVER ask you to enter your credentials or update your password through an e-mail link.
d. Passwords should not be written down.
e. Passwords may be stored only in "password managers" authorized by the university and using MFA.
f. Do not use the "Remember Password" feature of applications (for example, web browsers).
g. Any user suspecting that his/her password may have been compromised must report the incident to the university's IT department immediately and promptly change all passwords. Further actions may need to be taken by the user as directed by IT.

Application Development:

Application developers must ensure that their programs contain the following security precautions:

1. Applications must support authentication of individual users, not groups.
2. Applications must not transmit passwords in clear text over the network.
3. Applications must not store passwords in an easily reversable form and must comply with protection requirements as determined by IT.
4. Applications must provide for some sort of role impersonation, such that IT support can run processes with the same access and permissions that the user would have.
5. Applications must integrate into the Trent Single Sign On (SSO) when used for internal users.

Use of Multi-Factor Authentication (MFA):

1. MFA will be utilized as mandated through the university's IT Department.
2. MFA will not be utilized globally but will be situational based on a combination of; the user accessing the system, the system being accessed, and the conditions of access. Conditions of access may include, but are not limited to; geography of access, time of access, access device trust status, or access that falls outside of the user's normal access patterns.
3. The university's IT department will consult with a subcommittee of IT Steering before mandating the different scenarios of MFA use.
4. The technologies utilized for MFA will be defined by the university's IT department and may utilize hardware tokens and/or mobile devices.

Exceptions

Requests for exceptions to the Policy must be submitted to the Associate Vice President, IT.

Non-Compliance

Departments and users who act in good faith and execute their responsibility with a reasonable standard of care shall not be subject to disciplinary action in the event of a data security breach resulting from an account breach.

Breaches arising from intentional disregard of this policy will be subject to sanctions determined by the AVP-IT, in consultation with the employee's department head, Dean, or VP. Sanctions may include the suspension of computing privileges and account access. For unionized employees, any disciplinary action resulting from intentional violation of this policy will be consistent with collective agreement provisions and will be imposed in accordance with procedural requirements of the collective agreement and all rights thereunder shall be preserved.

Reporting

In the event of an actual or suspected data breach stemming from an account compromise, the user must inform both the IT Department and the University's Access and Privacy Office. If the breach involved research data, the Office of Research must also be informed.

Contact Officer:

Associate Vice President, IT

Date for Next Review:

Related Policies, Procedures & Guidelines

a) Password Construction Guidelines
b) Account Privileges Policy
c) Handling Sensitive Information Policy
d) Computing Resources Acceptable Use Policy

Policies Superseded by This Policy:

a) Guidelines for Use of Information Technology