# Procedure

**IT PASSWORD AND AUTHENTICATION PROCEDURE**

| | | | | |
|---|---|---|---|---|
| **Procedure Section & Number:** | | | **Effective Date:** | |
| **Policy Owner:** | Vice President Infrastructure & CIO | | **Last Revised:** | N/A |
| **Policy Administrator:** | Associate Director Information Technology | | **Review Scheduled:** | 2 years |
| **Approver:** | Executive Committee | | | |
| *The official controlled version of this document is held with the Policy & Procedure Coordinator.* | | | | |

## A. PROCEDURES

1. Access to a host computer system, network server, or networked personal computer must be approved by the systems owner who must forward a request for access to IT Helpdesk.

2. A user's manager will approve the user's access to a computer system, network, or servers by sending a request for access to IT Helpdesk.

3. IT will maintain user identifier information and keep system access requests on file.

4. IT will supply the user with an identifier and a password for first-time access.

5. Where appropriate, users will be required to use two factor authentication.

6. A user may access College Systems and Networks by providing the required authentication.

7. IT will publish password complexity standards within their knowledgebase.

8. A user must change a password immediately if he has reason to believe or suspect that it is no longer confidential.

## B. RESPONSIBILITIES

Authentication of users and applications, accessing or processing data, is a fundamental requirement of information security to ensure confidentiality and integrity of data. This procedure establishes authentication requirements for the use of Keyano College's technology resources.

### 1. Responsibility of Users

1.1 Users are responsible for keeping passwords and all other types of authentication secure and confidential, including not sharing or storing passwords in an insecure manner. Passwords should not be written down and/or left in an easily accessible location.

1.2 Passwords are confidential College information and should never be stored electronically without strong encryption.

1.3 All passwords must be changed at first issuance or use.

1.4 Passwords must not be shared for any individual accounts, including with IT support professionals, and only shared for other account types as defined in the Definitions section of this Procedure to the minimum extent required. If anyone asks a user for their password (including ITS), they are obligated to report this to the ITS.helpdesk@keyano.ca as a security incident.

1.5 For any shared passwords, whenever any person with knowledge of the password changes to a role where they no longer require knowledge of the password (i.e., leaves the College or changes positions), the password must be changed.

1.6 Passwords for Keyano systems must be unique. Users should never use their Keyano password for any third-party systems, even if used for Keyano business purposes. Users should never use the same password for privileged and non-privileged accounts.

1.7 Users must not store passwords with applications or use the "remember password" functions built into web browsers. Using a third-party password manager is highly encouraged to create strong passwords and store them securely. (Contact ITS for a list of currently recommended password managers.)

1.8 Always log out of applications or lock computers when leaving a computer to prevent unauthorized use.

1.9 Users must not attempt to circumvent College established authentication processes.

1.10 Users must follow ITS standards for authentication and password specifications. (See link to the standard https://app.procedureflow.com/flows/226404)

1.11 Authentication: All users of accounts must protect any authentication mechanisms, including passwords or other authentication factors (MFA tokens, certificates, internet cookies, etc.) to ensure only appropriate access to College data and resources. Passwords shall not be shared.

1.12 Policy: All users of accounts must follow College policies and standards, including but not limited to, the Information and Communication Technology Usage and the IT Network Security and Access Control policies.

1.13 Privileges: All accounts shall be used only for the purpose they were authorized.

1.14 Misuse: Any disclosure of an account password or suspected compromise or misuse of accounts or data must be reported immediately to the ITS.helpdesk@keyano.ca.

1.15 Accounts: All College business shall be conducted using an account associated with @keyano.ca addresses, or approved exceptions. Non-College accounts such as personal Gmail, Yahoo, etc. accounts shall NOT be used for conducting College business. To protect personal information, Student, Alumni and Retiree accounts shall not be used for conducting College business.

1.16 Communication: Official College communications may be delivered to preferred or required addresses for those with @keyano.ca addresses. Account holders must periodically check these accounts for required communication and, if forwarding is allowed, are responsible for checking the destination address. The College is not

responsible for messages forwarded to third party mailboxes. Some College business processes may require receiving messages from valid Keyano email addresses and may not accept messages from third party accounts (Gmail, Yahoo, etc.).

1.17 Third Party Accounts: Accounts created in non-College systems but used for College business must be handled in a manner consistent with the policies for accounts, including association with @keyano.ca email addresses and the current standards published by ITS.

**2. Responsibilities of Account Managers**

2.1 Authority: Managing accounts is the responsibility of Information Technology Services (ITS). All accounts must be managed in accordance with current ITS standards, including requirements for identity vetting, passwords, multifactor authentication, federation, auditing, and lifecycle (creation and termination). ITS may publish standards to supplement and enforce this policy.

2.2 Automation: Automated account management (software and/or scripts) shall be used to ensure accounts are managed as appropriate when each account user's role with the College changes according to official College records. Use of all accounts shall be monitored by automated tools to detect atypical use and take appropriate action, up to and including disabling of the account.

2.3 Access: Access granted to each account must be reviewed at least annually by appropriate data stewards or account managers to ensure all access is authorized.

2.4 Shared Accounts: Shared accounts shall not be created or assigned when an individual account access method is available. ITS will approve the use of all shared accounts.

2.5 Inactive Accounts: Built-in or automated systems shall disable any account which has been determined to be inactive. Account inactivity timeframes will be determined according to risk and published as ITS Standards, but in no case should they exceed 180 days. Exceptions can be made for accounts which are not used interactively or where active use is not expected or cannot be accurately determined.

2.6 Lifecycle: All accounts shall be maintained only if there is a documented affiliation of the account holder with the College. Accounts shall not be created until there are sufficient records to uniquely identify the account holder. Changes to College roles of the account holder require review of access granted to their accounts. This includes changing of assigned access, or up to and including account renaming or creation of a new account for the new role.

2.7 Auditing: Information systems used at the College must audit account creation, modification, enabling, disabling, and removal actions and notify the account managers or security operations team and/or log centrally.

2.8 Federation: Federated identity services for College accounts shall only be provided by ITS or ITS-approved systems or vendors. Federation shall be used by all college applications and websites or for any service used by many faculty, staff, or students.

2.9 Preferred Email: Accounts and records shall be maintained to enforce use of @keyano.ca email addresses for communication to employees or other approved individuals conducting College business. This includes publishing in the campus directory. Students, alumni, and retirees should use alternate domains or email addresses for personal or student matters to ensure their records are separate from College business that may be subject to public

records requests. Active students, enrolled in the current term, must have their preferred email address set to their @keyanomail.ca email address if they are not also a benefits-eligible employee. Individuals with multiple roles should be assigned a preferred email address based upon their primary role. Where possible, use of student and employee addresses for communication should favour role based official Keyano addresses, rather than using the preferred address.

2.10 Auto-forwarding Email: College systems shall be configured to prevent automatic forwarding of email directly, or via rule or filter, for accounts created for conduct of College business. Where not possible to prevent this configuration, automation shall be used when possible to correct the automatic forwarding and notify the user of the change. Accounts not directly, or reasonably expected, to be involved in College business, including but not limited to students, alumni, and retirees will be allowed to auto-forward email.

2.11 Account Reuse: Once an individual account has been assigned and used by a person, it shall not be assigned or re-used by any other person. This includes both the specific account, and re-use of the email address at any future date.

2.12 Privileged Accounts: Separate individual accounts shall be created and must be used for any privileged access. Use of privileged accounts shall be logged. Privileged accounts shall not be used for non-privileged functions (email, web-browsing, etc.).

2.13 Passwords: All systems and accounts shall be configured to require or meet current ITS password standards (https://app.procedureflow.com/flows/226404)

2.14 Least Privilege: When provisioning accounts, principles of least privilege shall apply. To the extent possible, accounts should be granted sufficient privileges to perform approved functions and no more.

**3. Remediation and Compliance**

Noncompliance with this policy shall be considered a violation of Keyano's Information and Communication Technology Usage Policy and will be addressed and remediated accordingly.

## C. DEFINITIONS

| | | |
|---|---|---|
| **(1)** | **Password:** | A combination of letters, numbers, symbols, and special characters that can be used to authenticate a person to an account accessing a technology resource. Long forms of passwords are sometimes called a passphrase. |
| **(2)** | **Biometric Identifier:** | Unique physical or behavioral characteristics of a person that can be analyzed to uniquely identify and authenticate a person to an account for accessing a technology resource. |
| **(3)** | **Token:** | A hardware or software device that can be cryptographically verified as unique. |

| | | |
|---|---|---|
| **(4)** | **Geolocation:** | For purposes of this policy, geolocation refers to the process of identifying the locations of a user based upon the known locations of their Internet Protocol (IP) addresses, or from data collected from their authenticated devices with built-in location detection. |
| **(5)** | **API Token:** | For purposes of this policy, an application program interface (API) token is a unique, long, token or key that may provide authentication for an application to access another service or application. |
| **(6)** | **Personal Identification Number (PIN):** | A short number or password used locally on a device as a convenient authentication alternative to typing a full password. |
| **(7)** | **Multi Factor Authentication (MFA)**: | Using two or more authentication factors: typically, passwords, biometrics, or tokens, to achieve authentication. |
| **(8)** | **Account:** | For purposes of this policy, an account is an electronic identifier used by systems and applications to authenticate and authorize users or processes to access college technology resources and to facilitate auditing of activities associated with an individual user. |
| **(9)** | **Account Types** | |
| | 9.1 Individual: | Primary account assigned to a single individual for access to technology resources, including interactive logon to computers, email, VPN, or other Keyano resources. |
| | 9.2 Shared: | Account used or shared where multiple users know the password or otherwise use the account for interactive logon. |
| | 9.3 Functional: | Account used by applications and processes and not interactively used by end users. |
| | 9.4 Privileged: | Administrative account restricted to authorized ITS staff. |
| **(10)** | **Authentication:** | Authentication is the process by which a system or application confirms that a person or device really is who or what it is claiming to be and through which access to the requested resource is authorized. Authentication factors may include something you know (e.g., password), something you have (e.g., hardware token, certificate, or software |

authenticator), or something you are (usually a biometric, like a fingerprint).

**(11) Authorization:** A process by which access to a resource is authorized based upon the authenticated identity or account.

**(12) Federated Identity:** An account which can be used across disparate technology systems or organizations, typically through a Single Sign On (SSO) service.

**(13) Single Sign On:** Use of a single account to access multiple applications or systems.

**(14) Account Manager:** An individual or system that manages accounts, assigns accounts to individuals, and grants privileges to accounts.

## D. RELATED LEGISLATION & STANDARDS

- COBIT DSS05.02 Manage Network and Connectivity Security
- *Freedom of Information and Protection of Privacy Act*
- NIST Digital Identity Guidelines

## E. RELATED DOCUMENTS

- Password Standards https://app.procedureflow.com/flows/226404_
- Information and Communication Technology Usage Policy
- IT Network Security and Access Control Policy

## F. REVISION HISTORY

| Date (mm/dd/yyyy) | Description of Change | Sections | Person who Entered Revision (Position Title) | Person who Authorized Revision (Position Title) |
|---|---|---|---|---|
| February 2021 | NEW | All | Associate Director IT | Vice President Infrastructure & CIO |
| | | | | |
| | | | | |
| | | | | |