Keyano COLLEGE

Policy

IT PASSWORD AND AUTHENTICATION POLICY

Policy 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. POLICY STATEMENT

One important part of computer security is the safeguarding of personal and confidential information of all individuals and organizations affiliated with Keyano College. Properly chosen passwords by College system users will assist in the control of access to systems and data.

Consistent with the College's requirements for identity and access management, users must protect the integrity of their authentication methods. Generally, all Keyano IT resources require some form of authentication, and systems will be secured as appropriate for the level of risk. Access to College systems and data must be provided in a way that such access can be audited and uniquely tied to the individual and their role with the College.

1. Guiding Principles

1.1 There is management approval on file for the specific system access granted to every individual.
1.2 Only personnel authorized to access the computer system, network, or servers are granted access.
1.3 Where possible, all activity on the system, network, or servers may be traced to an individual.
1.4 User authentication passwords are kept securely.
1.5 An individual may be held accountable for all activity logged against his or her user identifier.

2. Exceptions

2.1 Exceptions to this policy may be submitted to the Systems Owner in writing. If approved, they will forward the request to the Associate Director of Information Technology who will assess the risk and make a recommendation to the Vice

President Infrastructure & CIO. Exceptions must be reviewed for reauthorization on no less than an annual basis.

B. DEFINITIONS

(1)	**Policy:**	means the IT Password and Authentication Policy.
(2)	**College:**	means Keyano College.
(3)	**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.
(3)	**Authentication:**	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 identifier, like a fingerprint).
(4)	**Systems Owner:**	refers to the dean, director or manager of a department that controls and is the main user of that system.

C. RELATED POLICIES

- Information and Communication Technology Usage Policy
- ITS Information System Owner Policy
- IT Password and Authentication Procedure

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

- None

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