Yukon University

Policy Title:	**Passwords**
Policy Approver:	President's Office
Policy Holder:	IT Director
Category:	Operational
Original Date:	December 2014
Last Revised:	April 2015
Next Review:	December 2019

Policy Statement

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Yukon University's resources. All users, including contractors and vendors with access to Yukon University systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Approval Statement

With the consent of the Senior Executive Committee and approval of the President of Yukon College, this policy is hereby deemed in effect the 29th day of April, 2015.

Karen Barnes   April 29, 2015

_____   _____
President, Yukon College   Date

Yukon University

1. Purpose of Policy

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

2. Governing Legislation and Relevant Documents

N/A

3. Scope

The scope of this policy includes all users who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Yukon University facility, have access to the Yukon University network, or store any non-public Yukon University information.

4. Policy

4.1 Password Creation

4.1.1. All user-level and system-level passwords must conform to the following guidelines.

Parameter	Standard	Comments
Length	At least 8 characters	
Complexity	At least 1 lower case character At least 1 upper case character At least 1 numeric character At least 1 special character	At least 3 of these 4 standards must be met
Prohibited Content	Password MUST NOT contain User ID	
Password Change Frequency	Passwords will be reset annually at a minimum	Some divisions require more frequent Intervals (i.e. IT Services, Finance)
Password History	No reuse of last five passwords	

4.1.2. It is recommended that users not use the same password for Yukon University accounts as for other non-Yukon University access (for example, personal Internet Service Provider (ISP) account, option trading, benefits, and so on).

4.1.3. Where possible, users must not use the same password for various Yukon University access.

4.1 Password Protection

4.1.1 Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential Yukon University information.

4.1.2 Passwords must not be inserted into email messages or other forms of electronic communication.

4.1.3 Passwords must not be revealed over the phone to anyone.

4.1.4 Do not reveal a password on questionnaires or security forms.

4.1.5 Do not hint at the format of a password (for example, "my family name").

4.1.6 Do not share Yukon University passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.

4.1.7 Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

4.1.8 Do not use the "Remember Password" feature of applications (for example, web browsers) to non-University sites/resources.

4.1.9 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

5. Policy Compliance

5.1 Compliance Measurement

The IT Services team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by IT Services in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Other Related and/or Accompanying Documents

Addendum A - Policy Communication Checklist

ADDENDUM A - Policy Communication Checklist

Policy Name: Passwords
Number: SS 12.0
Submitted by: Colleen Wirth

List those consulted with in preparation of this policy:

Name	Department	Date
Lynda Pattie	IT consultant	March-April 2015
Mike Barwell	IT Services Manager	

The order for communication and/or consultation for a new or revised policy is as follows:
1. SEC – initial review and recommendations from SEC membership;
2. Identified stakeholders within Yukon University in order of priority – see below;
3. SEC – to be briefed on any issues arising out of stakeholder consultations;
4. Staff – SEC members to bring policy to their staff for feedback (*SEC member introducing this policy is responsible for sending to SEC, requesting that it be circulated to their staff for feedback*);
5. SEC – final draft supported by SEC membership and approved by the President.

This checklist must be completed prior to the final draft of a policy being presented to SEC for presidential approval.

Body	Communication Planned	Completed	Comments
SEC	December 17, 2014		
Student Union	n/a		
Employee's Union	n/a		
Occupational Health and Safety	n/a		
Academic Council	n/a		
Board or a Board subcommittee	n/a		
YC Staff	April 2015		
Other			
SEC for Final Review	April 29, 2015		