Windsor-Essex Catholic District School Board

Section: Information Technology

ADMINISTRATIVE PROCEDURE

PR IT:01C PASSWORDS FOR INFORMATION TECHNOLOGY RESOURCES

NUMBER:	PR IT:01C
EFFECTIVE:	May 25, 2016
AMENDED:	Replaces H:17, H:18, SC:03
RELATED POLICIES:	See References
REPEALS:	
REVIEW DATE:	2019-2020

1.0 OBJECTIVE:

1.1 To provide details about the creation and use of passwords for Information Technology Resources.

1.2 To align password configuration parameters with industry standard best practices.

2.0 GUIDELINES:

2.1 All user access requests (forms or emails) from Human Resources should be formally documented, approved and communicated to System Owners / System Administrators for appropriate action (refer to Administrative Procedure PR IT:01B User Access Management, 4.0).

2.2 Passwords play a key role in preventing unauthorized access to Information Technology Resources.

3.0 PROCEDURE:

All Windsor-Essex Catholic District School Board employees with access to the Information Technology Systems that are accessed by Board Login must follow the procedure outlined below to ensure maximum password security. It is recommended that users follow these password guidelines for all systems.

3.1 The password must be eight (8) characters or longer.

3.2 The password must contain numbers (0 through 9).

3.3 The password must contain lowercase letters (a through z).

3.4 The password must contain uppercase letters (A through Z).

3.5 The password may optionally contain special characters (!#$%^&*()_=<>,-{}?~).

3.6 The password should be changed at least once per year.

3.7 Accounts will be suspended after a specific number of failed login attempts. The account lockout threshold and account lockout duration are not disclosed for security reasons.

3.8 Passwords shall be memorized and never written down or recorded.

3.9 Do not share your password with anyone.

3.10 Do not use the same password for personal use and for work use.

3.11 Immediately change your password if you suspect it has been compromised and contact the System Owner / System Administrator.

3.12 Always log out or close any system when finished using your account.

3.13 Staff can change their Board Login password using the self-service Board Login Password Changer web application.

3.14 Accounts are created / modified / removed as requested from the Human Resources Department.