Effective: December 11, 2017

Administrative Procedure: Logical Access Control

Table of Contents

1.0 Access

1.0 All Access to Superior North Catholic District School Board's systems and data, including changes to access resulting from changes in responsibility or internal transfers, must be authorized by the end-user's supervisor or a higher authority, and the access request and authorization documented in a central repository. The Board reserves the right to determine the structure and type of usernames, passwords and/or other identifying authorization mechanisms used for logical access.

2.0 Least Privilege

2.1 Access to IT systems and data must be granted on the basis of least privilege. This means that access will be granted only to systems or data that a user requires to complete his or her functions at the most restrictive access level necessary to perform these functions. This enhances security of the Board's IT systems and integrity of electronic data.

3.0 Role-Based Access

3.1 Where available by system functionality, role-based access must be used to grant users access to IT systems and data. Role-based access grants users access to IT systems and data based on their roles within the Board, rather than granting access based on individual user. This simplifies the administration of user access rights by associating these rights with a limited number of standardized roles, and also assists in maintaining the principle of least privilege. The assignment of multiple roles to a single user which may combine to violate separation of duties requirements identified by the business/data owner is prohibited.

4.0 User Accountability and Responsibilities

4.1 No person other than those authorized such access shall access IT systems and data. User accounts, which allow users to access IT systems and data, are provided to individuals for their exclusive use. Users are prohibited from sharing their account(s) and/or passwords with others. An authorized user is at all times responsible and accountable for the use of their account. Use of another user's credentials is prohibited.

5.0 Changes to User Access

5.1 At times, a user's access to IT systems and data may require changes, due to circumstances such as changed responsibilities, internal transfers, etc. Changes required to user access must be authorized by the end-user's supervisor or a higher authority and documented in a central repository in accordance with the principle of least privilege as outlined above.

6.0 Termination

6.1 Termination of user access must be conveyed to IT by Human Resources so that all access associated with the terminated account can be removed.

7.0 Password Management

7.1 Passwords are required for access to all IT systems. Users have the following password-related responsibilities. A user must:

7.1.1 Not share his or her password(s);

7.1.2 Immediately report to IT the compromise of any passwords;

7.1.3 Immediately change a compromised password.

7.2 IT hardware/software products are often supplied with default vendor-set passwords. To protect against compromise of IT systems and data by means of these passwords, which tend to be publicly known or available, default vendor passwords must be changed before hardware/software is placed into production.

8.0 Compliance and Reporting

8.1 Information Technology enforces this Policy and the related Standards at all times. Anyone who has reason to suspect a deliberate and/or significant violation of this Policy is encouraged to promptly report it to the IT. Policy violations will be assessed and action taken to remediate the violation, including consequences where appropriate, subject to collective agreements and/or other contractual conditions.