ADMINISTRATIVE PROCEDURE
141

MANAGEMENT OF ADMINISTATOR ACCOUNTS

General Administration

August 2016

Purpose/Background

To ensure security and management of RVS technologies, application owners are required to comply with the following procedures.

Procedures

1. System-level passwords
   1.1 Where applicable, all system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed at least once a year.
   1.2 User accounts that have system-level access must have a unique password from all other accounts.
   1.3 All systems/application owners shall be responsible for ensuring their users follow best practice guidelines for passwords outlined in AP 140 Responsible Technology Use Agreement.

2. Security
   2.1 Application owners must ensure their programs contain the following security precautions.
      2.1.1 Shall support authentication of individual users, not included in Active Directory;
      2.1.2 Shall not store passwords in clear text or in any easily reversible form; and,
      2.1.3 Shall provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
   2.2 Application owners must regularly review site security measures to ensure they conform to the Division IS027001 security controls.
   2.3 An Internet privacy statement must be posted on all Division websites.

3. Use of Passwords and Passphrases for Remote Access Users
   3.1 Remote access to the Division Network is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

4. Passphrases
   4.1 Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access. Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks." A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good

passphrase might be "The Rain in Spain falls mainly on the plain" which translates to Tr1sfm@tp. All of the rules above that apply to passwords apply to passphrases. (NOTE: Do not use this example as a passphrase!)

5. Application owners (for applications that use or store personal information):

5.1 Manager of Systems and Networks: E-directory, Corporate Plone, Follett, IDM, SysAid, Wireless, NDS, VPN, Outlook, Nirex and Commvault

5.2 Director of Communications: School Bundle Web Portal

5.3 Director of Finance: SRB, Atrieve, SchoolCash.net, TRIM, ATB Business online, ATB Tax File, MyBudgetFile, FTP, Moneris, Merchant Direct, Grand and Toy online, SchoolDude, ROE Web, LAPP, ATRF, CSB, Industrial Alliance, OpenVMS

5.4 SIS Project Manager: PowerSchool, Edulink, Extranet, PASI

5.5 21st Century Team: All other Educational Technologies as per the listing at: http://www.rockyview.ab.ca/professional-learning/educational-technologies

- Director of Learning: IPPS and eLSTR as well as any other learning support databases used to test or track students.
- Director of Transportation: EDULOG

References:

- RVS AF141 eLSTR Access Request