User ID and Password Policy

1.0 Overview

In order to control access to REVGEN systems and data, all contractors requiring access are issued individual user accounts. These user accounts, which dictate the level of access any given user has, are accessed via individual user IDs and passwords.

As access to systems and data is therefore controlled via user IDs and passwords, it is imperative that they are issued, implemented and maintained in a strong manner. For example, their effectiveness is significantly reduced if care is not taken to protect passwords or easy to guess passwords are used, or if old and obsolete user IDs and passwords are left on the system in an active state. This policy is therefore aimed at providing the rules that govern the issuance and use of user IDs and passwords.

2.0 Purpose & Scope

The purpose of this policy is to establish the rules for user IDs and passwords used throughout the REVGEN systems environment, regardless of the operating system or application concerned. In addition, it gives best practice guidance for their use in client environments.

3.0 Policy

3.1 User ID Policy

- All access to REVGEN systems and data shall be via a unique user ID and password. In general, shared, group or generic user IDs shall not be permitted.

    - Exception: Sharing of individual user IDs and passwords is strictly prohibited unless it has been approved by the Senior Consultant in Managed Services or above to test the use of an email account, etc.

- All user IDs shall have an associated profile that defines those elements of the system that the user in question has access to. Users shall be given access to only those parts of the system that they require in order to carry out their job duties.

- User ID profiles shall be formally requested by the manager responsible and shall be subject to the approval of the data or system owner and implemented by the Security Officer using the security tools installed.

- User IDs shall be deleted from the system or disabled as and when contractors no longer perform service for the company. In sensitive cases, management may require the disabling or deletion of user IDs ahead of the contractor actually finishing work for REVGEN.

- The Security Officer shall audit network user IDs bi-annually to ensure that all inactive and unwanted user IDs are deleted.

- Service accounts shall be used for processing batch production work.

3.2 User ID Standards

- Personal REVGEN User IDs
  - These shall be issued to all contractors to enable them to log on and perform day-to-day operations as per the associated security profile.
  - These user IDs are unique and shall be based upon the user's name and shall be a combination of the first letter of the users first name followed by the last time. For example: jsmith, or smarks

- Web Application User IDs
  - These user IDs are used for the web applications that are often outside the direct control of REVGEN and therefore no specific standard is applied. However, by design they shall be unique.

- External Support User IDs
  - These are support user IDs, usually used as part of an email address and published on the REVGEN website or in documentation.
  - User IDs used for this purpose shall be generic rather than individual. For example support@ or info@.

3.3 Password Policy

- Initial passwords for new user IDs shall be set to expire after the first logon so as to ensure that the user changes them.

- For user IDs belonging to a specific individual, the password shall not be set to expire as long as it follows the general password construction in section 4.1.

- For system IDs such as those running production applications, the passwords shall be set to never expire. The Security Officer will ensure passwords contain at least 12 randomly generated characters.

- All default passwords supplied by vendors shall be changed prior to the software or device being implemented in production. The password strength should be commensurate with that of administrator passwords.

- Only the Security Officer or delegate shall access network devices, such as switches, routers, firewalls, etc, using a complex password that contains at least 12 randomly generated characters.

- Only secure password vault software shall be used to store passwords.

- Where a session has been idle for more than 15 minutes, the password shall be required to reactivate the session.

- User IDs shall be locked out of the system if the password is entered incorrectly 3 times within the space of 30 minutes. The account shall remain locked for a period of 15 minutes.

- All passwords are considered confidential and shall not be written down or stored unencrypted on disk or given to others for their use. When it is suspected that the confidentiality of a password has been breached the password shall be changed immediately.

- The Security Officer shall be empowered to periodically run password cracking routines to ensure compliance with this policy.

3.4 Password Standards

The following rules and standards shall be applied to passwords related to contractor user IDs:

3.5 Application Development Standards for user IDs/Passwords

Due to the confidential and sensitive nature of data held on REVGEN systems, designers and developers shall ensure that their applications provide facilities that enable the users of these systems to control access to their data. Applications design therefore takes into account the following policy:

- Applications shall be designed to use user IDs and passwords that are in line with these user ID and password standards.

- Applications must use unique user IDs for authentication.

- Applications shall enforce password features including required alpha, numeric and special character combinations as well as minimum length and shall be encrypted using AES-256.

- Applications shall support an automatic account and system lockout after 5 invalid attempts to login with the wrong password.

- Applications shall support giving users different levels of security permissions thereby restricting access and functionality on a ‘needs only’ basis.

- Applications shall support restriction of all export features to users with the highest security level.

4.0 Guidelines

4.1 General Password Construction

Passwords are used for various purposes in REVGEN, such as, user accounts, email accounts, screen-savers, etc. Since almost all of these do not use dynamic single use passwords, it is important that the passwords used are strong. The following guidelines are given for the construction of strong passwords:

- Passwords shall be a minimum of 12 characters in length and contain a mix of upper and lower case letters, numbers and special characters.

- Passwords shall not reference anything personal about the user, such as family names, birth dates, addresses, etc.

- Passwords shall not reference anything regarding the company, such as its name, a department name, manager name, etc.

- Passwords shall not contain common computer references, such as vendor names, websites, application names, etc.

- As much as possible, real words should be modified to use special characters. For example: instead of special, use Sp3c1@L.

- Passwords shall not be letter or number patterns, such as, qwertyuiop, or 123454321.

- As passwords shall never be written down, they should not be so complex that they cannot be remembered. One method for creating a complex yet memorable password is to base it on a song or film title, or phrase. For example; the phrase ‘Up the creek without a paddle’ might be formed as ^Cr3@rk<aPdl.

4.2 Password Protection Guidelines

- Do not use the same password for REVGEN accounts as for external business accounts, or private and personal accounts such as personal ISP accounts.

- Do not use the same password for different user IDs.

- Remember, REVGEN passwords are strictly confidential and must not be shared with anyone, including work colleagues and family members. If someone demands a password, refer him or her to the Security Officer and/or this policy.

- The following shall be adhered to at all times:

  - Do not reveal a password in an email message.
  - Do not reveal a password to your manager or supervisor.
  - Do not talk about a password in front of others.
  - Do not hint at the format of a password (e.g., "It's a place").
  - Do not reveal a password on questionnaires or security forms.
  - Do not share a password with family members.
  - Do not reveal a password to co-workers.

5.0 Enforcement

Any deviation from this policy is considered to be a threat to the security of REVGEN systems and data and as such is viewed as extremely serious. Contractors found in breach of this policy will be subject to disciplinary action up to and including the possible termination of their contractor agreement.

6.0 Exceptions

Microsoft 365 Office apps with MFA enabled, systematically enforces its own password policy that does not align with this policy. See the IT Policies Procedures and Standards, Section 3.5 for the Microsoft Office 365 apps password policy.

7.0 Revision History

The following table maintains the history of changes to this policy.

Rev	Date	Author	Description
1.0	12/5/18		Initial Content
1.1	6/24/19	Steven Martin	Contractor version