gravyty

your force for good

Password Security Policy

Version No: 1.3

Version 1.3. | 2023

Table of Contents

1. Overview

1.1. A password is the key to sensitive private and business information. When such a key is exposed by unauthorized entities, valuable information can leak or be damaged. Therefore, passwords should be hard to guess, be well protected and be changed frequently.

2. Purpose

2.1. The purpose of this policy is to enhance the protection of Gravyty's data by following the guidelines for password construction, protection and maintenance.

3. Scope

3.1. This policy applies to all of Gravyty's systems, workstations and servers.

4. Requirements

4.1. **Change frequency**

4.1.1. All system-level passwords (Administrator, etc.) must be changed on a monthly basis, at minimum.

4.1.2. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every three months.

5. Standards

5.1. All user-level and system-level passwords must conform to the standards described below:

5.2. All users at Gravyty should be aware of how to select strong passwords: Strong passwords have the following characteristics:

- Contain at least three of the five following character classes:
- Lower case characters
- Upper case characters
- Numbers
- Punctuation
- "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)
- Contain at least eight to fifteen alphanumeric characters.

5.3. The password is NOT a word found in a dictionary (English or foreign).

5.4. The password is NOT a common usage word such as: Computer terms and names, commands, sites, companies, hardware, software. Passwords should NEVER be "Password1" or any derivations of this word.

5.5. Should not include the words "Gravyty", or any derivations of this word.
5.6. Should not include birthdays or other personal information such as addresses and phone numbers.
5.7. Should not include repetitive word or number patterns such as aaabbb, qwerty, zyxwvuts, 123321, etc.
5.8. Should not include any of the above, preceded or followed by a single digit (e.g., secret1, secret).
5.9. Try to create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation or other phrase.

6. Protective measures

6.1. System users are never to share passwords with anyone, including administrative assistants.
6.2. All passwords are to be treated as sensitive, confidential information.
6.3. Passwords are never to be written or stored online without encryption.
6.4. Passwords are never to be revealed through email, chat, or other electronic communication.
6.5. Passwords are never to be spoken about in front of others.
6.6. Passwords' formats are never to be hinted at (e.g., "my family name").
6.7. Passwords are never to be revealed on questionnaires or security forms.

7. Remote access password

7.1. Access to the networks via remote access is to be controlled using either one- time password authentication or a public/private key system with a strong passphrase.

8. Security event reporting

8.1. System users are to immediately report any attempts by another person to obtain password or other confidential information to the IT Management Group.