Password Policy

2020-04-21

Document Number:

QMZ-PAS-01.DOCX

Prepared by: Qmuzik Technologies Technologies (Pty) Ltd

TABLE OF CONTENTS

1. Overview

Qmuzik Technologies' intentions for publishing Password Policy are not to impose restrictions that are contrary to its established culture of openness, trust and integrity. Qmuzik Technologies is committed to protecting its employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Effective security is a team effort involving the participation and support of every Qmuzik Technologies employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to ensure that only authorized users gain access to Qmuzik Technologies' information systems and to establish a standard for creation of strong passwords and the protection of those passwords.

3. Policy

To gain access to Qmuzik Technologies' information systems, authorized users, as a means of authentication must supply individual user passwords. These passwords must conform to certain rules contained in this document.

3.1 Who is Affected

This policy affects all employees of Qmuzik Technologies and it's subsidiaries, and all contractors, consultants, temporary employees and business partners. Employees who deliberately violate this policy will be subject disciplinary action up to and including termination.

3.2 Affected Systems

This policy applies to all computer and communication systems owned or operated by Qmuzik Technologies and its subsidiaries. Similarly, this policy applies to all platforms (operating systems) and all application systems.

3.3 User Authentication

All systems will require a valid user ID and password. All unnecessary operating system or application user IDs not assigned to an individual user will be deleted or disabled.

3.4 Password Storage and Protection

3.4.1 Passwords will not be stored in readable form without access control or in other locations where unauthorized persons might discover them. All such passwords are to be strictly controlled using either physical security or computer security controls.

3.4.2 Passwords must not be shared with anyone, including supervisors and co-workers. All passwords are to be treated as sensitive, company information.

3.4.3 Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication, nor revealed over the phone to anyone.

3.4.4 Passwords may be stored only in "password managers" authorized by the organization.

3.4.5 Do not use the "Remember Password" feature of applications (for example, web browsers) for user accounts that have system-level privileges such as domain logins or authentications. This feature is discouraged in as far as possible.

3.4.6 Any user suspecting that his/her password may have been compromised must report the incident and change all possible affected passwords.

3.5 Application Passwords Required

All programs, including third party purchased software and applications developed internally by Qmuzik Technologies must be password protected.

3.6 Choosing Passwords

Minimum password requirement:

- All user-chosen passwords must contain at least one alphabetic and one non-alphabetic character.
- Password length minimum 1~~0~~2 characters
- Passwords expire every ~~3~~60 (thirty) days
- The use of control characters and other non-printing characters are prohibited. All users must be automatically forced to change their passwords appropriate to the classification level of information. To obtain a new password, a user must present suitable identification. Users must use a separate, unique password for each of their work related accounts. Users may not use any work related passwords for their own, personal accounts.

Tips to enable an easy to remember, complex password:

- Use a Passphrase rather than simply a password
- Make the password at least 15 characters long. The longer the better – longer passwords are harder to crack.
- Include numbers, capital letters and symbols. Consider using a $ instead of an S or a 1 instead of an L, or including an & or % – but note that $1ngle is NOT a good password. Password thieves are onto this. But Mf$J1ravng (short for “My friend Sam Jones is really a very nice guy) is an excellent password

3.7 Changing Passwords

All passwords must be promptly changed if they are suspected of being disclosed, or known to have been disclosed to unauthorized parties. All users must be forced to change their passwords at least once every 30- (thirty) days.

3.8 Application Development

3.8.1 Application developers must ensure that their programs contain the following security precautions:

3.8.2 Applications must support authentication of individual users, not groups.

3.8.3 Applications must not store passwords in clear text or in any easily reversible form.

3.8.4 Applications must not transmit passwords in clear text over the network.

3.8.5 Applications must 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.

3.9 Multi-Factor Authentication

Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also

3.10 Password Constraints

The display and printing of passwords should be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them. After three unsuccessful attempts to enter a password, the involved user-ID must be either: (a) suspended until reset by a system administrator, (b) temporarily disabled for no less than three minutes, or (c) if dial-up or other external network connections are involved, disconnected.

3.11 Exceptions

Any exception to the policy must be approved by the Qmuzik network administrators in advance in writing detailing the situation with dates and risks involved.

4. Related Standards, Policies and Processes

Information Systems Access Policy

Incidence Report Policy

5. Definitions and Terms

6. Revision and version control

Version Number	Date	Description of Change	Changed By
1.0	2020/04/21	Creation	Tinus Kleingeld
2.0	2020/04/28	Revised	Adriaan Voges
2.1	2020/04/29	Revised 3.6 and 3.7	Tinus Kleingeld
2.2	2020/04/29	Revised	Adriaan Voges

7. Policy acceptance

The undersigned hereby agrees that this policy is valid and can be enforced.

Name	Role	Signature
Adriaan Voges	Director	