Information Security Policy

2021-02-25

Document Number:

QMZ-IS-01.DOCX

Prepared by: Qmuzik Technologies Technologies (Pty) Ltd

Submitted to:

TABLE OF CONTENTS

1. Overview

Information assets of Qmuzik Technologies, in all their forms and throughout their life cycle, will be protected through information management policies and actions that meet the legal requirements and support best business practices. The purpose of this policy is to identify and disseminate Qmuzik Technologies' framework and principles that guide business actions and operations in generating, protecting, and sharing business data.

2. Purpose

The purpose of this policy is to protect Qmuzik Technologies' information resources from accidental or intentional unauthorized access, modification or damage. This policy governs management of devices, resources, and user access to Qmuzik Technologies' owned hardware and data. All employees with access to company data is subject to – and has responsibilities under this policy.

3. Policy

1. Information Security 3 (three) main Objectives

- **Confidentiality**. Only individuals with authorization can and should access data and information assets.
- **Integrity**. Qmuzik Technologies strive to keep data intact, accurate and complete and supporting IT systems are kept operational.
- **Availability**. Users are able to access information and/or systems when needed.

2. Authority and Access Control Policy

- A hierarchical pattern applies. Senior managers have the authority to decide what data can be shared and with whom. The security policy have different terms for a senior manager vs. a junior employee.
- Network security policy—Qmuzik Technology users are only able to access company networks and servers via unique logins that demand Domain Level authentication. We are looking to investigate Two-Factor Authentication (2FA) for additional security in the near future . All login attempts are automatically logged by the domain controllers. Also see the Qmuzik Password Policy (QMZ-PASS-01)

3. Data Classification

Qmuzik Data is classified into three (4) categories, namely public, confidential, secret and top secret. This is to ensure that sensitive data cannot be accessed by individuals with lower clearance levels.

- Public data is available to anyone. For example Qmuzik Technologies training videos on Youtube.
- Confidential data is limited to company employees and selected stakeholders only. This include company policies, email etc.
- Secret data is limited to Managers and those that "need to know" to perform their duties. This may include our Development team and their managers that develop new systems and applications for our clients.
- Top secret data is limited to the company Directors.

4. Data Support and Operations

1. Data protection regulations (systems that store personal data, or other sensitive data) must be protected according to organizational standards, best practices, industry compliance standards and relevant regulations. Most security standards require, at a minimum, encryption, a firewall, and anti-malware protection. Qmuzik Technologies employs a Fortigate monitored firewall hosted by our hosting company PC Maniacs to monitor our incoming and outgoing network traffic. Emails are routed through Mimecast and Microsoft Office 365, which encrypts and protects our incoming and outgoing emails against known email attacks including malware, phishing and other malicious attacks. Also see the Qmuzik Remote Access Policy (QMZ-RAP-01)
2. Data Backups are done locally via Veeam Backups and encrypted and stored on a Network Attached Storage device (NAS) that is hosted at our hosting company PC Maniacs. Cloud storage (Redstor) is also used to backup high priority servers. These backups run on a daily and weekly schedule.

5. Security Awareness and Behavior

From time to time Qmuzik Technologies implements and updates our internal company Policies. These are communicated to employees and the relevant stakeholder or clients as needed via email. This is done to inform employees of Qmuzik Technologies security procedures and mechanisms, including data protection measures, access protection measures and overall network security awareness.

- Social engineering attacks are most often encountered in the form of phishing emails and as such employees are made responsible for noticing, preventing and reporting such attacks. Our Mimecast email management system filters most of these attacks, but on occasion a suspect email might come through. By being aware, employees and users will know not to trust these emails but to immediately report and delete these malicious mails.
- Qmuzik Technologies runs a Clean Desk Policy. Laptops are locked with cable locks and must be neatened by the end of the day to reduce clutter and clear of all paper.
- Acceptable Internet usage is setup up and managed by our Internet Service Provider EOH. Qmuzik Technologies is a software development company that requires various online tools to assist our developers and as such we do not block social media (Facebook, Youtube, etc) however we do block sites that are marked as suspicious. We also block gaming websites, gambling and pornographic sites as unsuitable for the workplace.

6. Personal and Mobile Device Management.

Using personal computing devices, such as laptops, smartphones etc introduces a new risk into the workplace. Qmuzik Technologies will address this risk by only allowing Company-owned devices on the network, unless with prior approval from the IT Manager. The wireless network needs to be split into 2 (two) networks, one that forms part of the corporate LAN and another that is only connected to the Internet for guest users. This will be done in due course.

7. Security Incident Response Plan

Once an incident has been identified, it needs to be addressed. The Security Incident Response Plan will be used to respond to the incident.

8. SaaS and Cloud policies

With Cloud computing becoming more and more used by clients and business partners, Qmuzik Technologies are looking to make the move to certain Cloud products as well. Together with this consideration, we will look to draft and implement new Cloud Policies.

4. Revision and version control

Version Number	Date	Description of Change	Changed By
1.0	2020/04/21	Creation	Tinus Kleingeld
1.1	2021/02/25	Updated	Tinus Kleingeld

5. Policy acceptance

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

Name	Role	Signature