# IT Incident Response Policy

**2020-04-24**

**Document Number:**

**QMZ-IRP-01.DOCX**

Prepared by: Qmuzik Technologies ~~Technologies~~ (Pty) Ltd

~~Submitted to:~~

## TABLE OF CONTENTS

1. Overview ..... 3
2. Purpose ..... 3
3. Policy ..... 3
    1. Confirmed Incident ..... 3
    2. Work with Forensic Investigators ..... 4
    3. Develop a Communication Plan ..... 4
4. Ownership and Responsibilities ..... 4
    1. Sponsors ..... 4
    2. Information Security Administrator ..... 4
    3. Users ..... 4
    4. Incident Response Team ..... 4
5. Enforcement ..... 4
6. Definitions and Terms ..... 54
    1. Encryption or Encrypted data ..... 54
    2. Plain text ..... 5
    3. Hacker ..... 5
    4. POPI Act ..... 5
    5. PII 5
    6. Protected Data ..... 5
    7. Information Resource ..... 5
    8. Safeguards ..... 5
    9. Sensitive Data ..... 5
7. Revision and version control ..... 5
8. Policy acceptance ..... 6

# 1. Overview

This Policy mandates that any individual who suspects that a theft, breach of exposure of Qmuzik Technologies' data, albeit IP of source control or any sensitive or protected data has occurred must immediately provide a description of what occurred to his or her immediate Manager or the IT department, who in turn must take it up with Senior Management without delay. The IT Manager and Team will investigate all reported incidents to confirm if a theft, breach or exposure has occurred. If a theft, breach of exposure has occurred, the IT Manager will follow the appropriate procedure in place.

# 2. Purpose

The purpose of this policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (eg. To enable prioritization of the incidents), as well as reporting, remediation and feedback on mechanisms. The policy shall we be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

Qmuzik Technologies' Information Security's intentions for publishing an Incident Response Policy are to focus significant attention on data security and data security breaches and how Qmuzik Technologies' established culture of openness, trust and integrity should respond to such activity. Qmuzik Technologies' Information Security is committed to protecting the Company's employees, partners and itself from illegal and/or damaging actions by individuals, either knowingly or unknowingly.

# 3. Policy

This policy applies to

- -all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of or otherwise handle personally identifiable information as described in the POPI Act, which aims to encourage the protection of personal information that is processed by both public and private bodies.
- a breach of all Qmuzik owned protected and sensitive data, owned software and sourcecode of any kind, or such software or data under supervision of Qmuzik protected under an agreement of a third party.

**Formatted:** List Paragraph, Bulleted + Level: 1 + Aligned at: 0.8 cm + Indent at: 1.44 cm

Qmuzik Technologies strives to meet the conditions of the requirements that businesses must comply with when processing personal information.

### 1. Confirmed Incident

As soon as a theft, data breach or exposure containing Qmuzik Technologies' protected data or sensitive data is identified, the actual incident must be confirmed and the process of removing all access to that resource will begin.

The Executive Director will chair an incident response team to handle the incident. Team will include members from:

- IT Infrastructure and applications (Internally)
- IT Suppliers (if applicable)
- Finance and HR (if applicable)

- Legal (if applicable)
- Any additional individuals as the Executive Director deems necessary

**2. Work with Forensic Investigators**

If the incident is serious enough to warrant further investigation, Qmuzik Technologies will make use of the services of Forensic Investigators and experts that will determine how the incident occurred, the types of data involved, the number of internal/external individuals and/or organisations impacted and analyse the incident to determine the root cause.

**3. Develop a Communication Plan**

Depending on the severity and the impact that the breach may have, the~~T~~he stakeholders will draft a communication plan and decide on the most effective way to communicate the incident to a) internal employees, b) the public (if necessary) and c) clients and any other stakeholders identified.

## 4. Ownership and Responsibilities

**1. Sponsors**

Those members of the Qmuzik Technologies community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any Company Executive in connection with their administrative responsibilities or by die actual sponsorship, collection, development or storage of information. The Sponsor role will thus differ depending on the information resource whether it be specific product, company or customer related information.

**2. Information Security Administrator**

That member of the Company community, designated by the Director, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to information resources in consultation with the relevant Sponsors.

**3. Users**

Virtually all members of the Qmuzik Technologies community, to the extent that they have authorised access to information resources. This may include staff, trustees, contractors, consultants, interns, temporary employees, students or volunteers.

**4. Incident Response Team**

The Incident Response Team shall be chaired by Senior Management who will appoint team members from the following departments: IT, Human Resources, Finance, Communication, Legal and others as deemed necessary, or representatives thereof.

## 5. Enforcement

Any Qmuzik Technologies personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party / partner company found in violation may be subject to litigation and have their access to Company systems terminated.

# 6. Definitions and Terms

1. **Encryption or Encrypted data**

The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text.

2. **Plain text**

Unencrypted data

3. **Hacker**

A person who uses computers to gain unauthorized access to data.

4. **POPI Act**

The Protection of Personal Information Act (or POPI Act) is South Africa's equivalent of the EU GDPR. It sets some conditions for responsible parties (called controllers in other jurisdictions) to lawfully process the personal information of data subjects (both natural and juristic persons).

5. **PII**

Personally Identifiable Information is any data that could potentially identify a specific individual.

6. **Protected Data**

See **POPI Act** and **PII**

7. **Information Resource**

The data and information assets of an organisation, department or unit.

8. **Safeguards**

Countermeasures, control put in place to avoid, detect, counteract or minimise security risks to physical property, information, computer systems or other assets. Safeguards help reduce the risk of damage or loss by stopping, deterring or slowing down an attack against an asset.

9. **Sensitive Data**

Data that is encrypted or in plain text and contains POPI or PII data

# 7. 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 |
| 3.0 | 2020/05/15 | Revised | Adriaan Voges |
| | | | |

| | | | |
|---|---|---|---|
| | | | |
| | | | |

## 8. Policy acceptance

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

| Name | Role | Signature |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

| | | |
|---|---|---|
| | | |