



Acceptable Use Policy

2021-05-25

Document Number:

QMZ-AUP-01.DOCX

Prepared by: Qmuzik Technologies Technologies (Pty) Ltd

Submitted to:

Table of Contents

1.	OVERVIEW.....	3
2.	PURPOSE.....	3
3.	SCOPE.....	3
4.	POLICY.....	3
	4.1 GENERAL USE AND OWNERSHIP.....	3
	4.2 SECURITY AND PROPRIETARY INFORMATION.....	4
5.	POLICY COMPLIANCE.....	6
	5.1 COMPLIANCE MEASUREMENT.....	6
	5.2 EXCEPTION.....	6
	5.3 NON-COMPLIANCE.....	7
6.	RELATED STANDARDS, POLICIES AND PROCESSES.....	7
	6.1. DATA CLASSIFICATION POLICY.....	7
	6.2. DATA PROTECTION STANDARD.....	7
	6.3. SOCIAL MEDIA POLICY.....	7
	6.4. MINIMUM ACCESS POLICY.....	7
	6.5. PASSWORD POLICY.....	7
7.	DEFINITIONS AND TERMS.....	7
	7.1. BLOGGING.....	7
	7.2. HONEYPOT.....	7
	7.3. HONEYNET.....	7
	7.4. PROPRIETARY INFORMATION.....	7
	7.5. SPAM.....	7
8.	REVISION AND VERSION CONTROL.....	7
9.	POLICY ACCEPTANCE.....	8

1. Overview

Qmuzik Technologies' intentions for publishing an Acceptable Use 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.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP or cloud based-computing and storage, are the property of Qmuzik Technologies. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

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 outline the acceptable use of computer equipment at Qmuzik Technologies. These rules are in place to protect the employee and Qmuzik Technologies. Inappropriate use exposes Qmuzik Technologies to risks including virus attacks, compromise of network systems and services, and legal issues.

3. SCOPE

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Qmuzik Technologies business or interact with internal networks and business systems, whether owned or leased by Qmuzik Technologies, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Qmuzik Technologies and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Qmuzik Technologies policies and standards, and local laws and regulation. Exceptions to this policy are documented in [section 5.2](#)

This policy applies to employees, contractors, consultants, temporaries, and other workers at Qmuzik Technologies, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Qmuzik Technologies.

4. POLICY

4.1 GENERAL USE AND OWNERSHIP

4.1.1 Qmuzik Technologies proprietary information stored on electronic and computing devices whether owned or leased by Qmuzik Technologies, the employee or a third party, remains the sole property of Qmuzik Technologies. Microsoft Bitlocker is used to encrypt all laptop storage to protect proprietary information in accordance with Data Protection Standards.

4.1.2 Employees have a responsibility to promptly report the theft, loss or unauthorized disclosure of Qmuzik Technologies proprietary information.

4.1.3 Employees may access, use or share Qmuzik Technologies proprietary information only to the extent it is authorized and necessary to fulfil your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within Qmuzik Technologies may monitor equipment, systems and network traffic at any time, per Qmuzik Technologies' Audit Policy.

4.1.6 Qmuzik Technologies reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 SECURITY AND PROPRIETARY INFORMATION

4.2.1 All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy. The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- 1.** Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Qmuzik Technologies.
- 2.** Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Qmuzik Technologies or the end user does not have an active license is strictly prohibited.
- 3.** Accessing data, a server or an account for any purpose other than conducting Qmuzik Technologies business, even if you have authorized access, is prohibited.
- 4.** Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

- 5** Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- 6** Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- 7.** Using a Qmuzik Technologies computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- 8.** Making fraudulent offers of products, items, or services originating from any Qmuzik Technologies account.
- 9.** Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- 10.** Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- 11.** Port scanning or security scanning is expressly prohibited unless prior notification to Qmuzik Technologies is made.
- 12.** Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- 13.** Circumventing user authentication or security of any host, network or account.
- 14.** Introducing honeypots, honeynets, or similar technology on the Qmuzik Technologies network.
- 15.** Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- 16.** Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- 17.** Providing information about, or lists of, Qmuzik Technologies employees to parties outside Qmuzik Technologies.

4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

- 1.** Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- 2.** Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- 3.** Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Qmuzik Technologies's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Qmuzik Technologies or connected via Qmuzik Technologies's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3.3 Blogging and Social Media

1. Blogging by employees, whether using Qmuzik Technologies's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Qmuzik Technologies's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Qmuzik Technologies's policy, is not detrimental to Qmuzik Technologies's best interests, and does not interfere with an employee's regular work duties. Blogging from Qmuzik Technologies's systems is also subject to monitoring.
2. Qmuzik Technologies's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by the **Confidential Information policy** when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Qmuzik Technologies and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Qmuzik Technologies's **Non-Discrimination and Anti-Harassment policy**.
4. Employees may also not attribute personal statements, opinions or beliefs to Qmuzik Technologies when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Qmuzik Technologies. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Qmuzik Technologies' trademarks, logos and any other Qmuzik Technologies intellectual property may also not be used in connection with any blogging activity.

5. Policy Compliance

5.1 Compliance Measurement

The Qmuzik Technologies team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exception

Any exception to the policy must be approved by the Qmuzik Technologies team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

6.1. Data Classification Policy

6.2. Data Protection Standard

6.3. Social Media Policy

6.4. Minimum Access Policy

6.5. Password Policy

7. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
<https://www.sans.org/security-resources/glossary-of-terms/>

7.1. Blogging

7.2. Honeypot

7.3. Honeynet

7.4. Proprietary Information

7.5. Spam

8. 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

9. Policy acceptance

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

Name	Role	Signature