Downes Murray International (DMI) Acceptable Use Policy

Author
Issue date
Next revision date

Table of Contents

1 Introduction

DMI IT team's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to DMI's established culture of openness, trust and integrity. Rather the DMI IT team is committed to protecting DMI's 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, are the property of DMI. These systems are to be used for business purposes in serving the interests of the company, and of our clients in the course of normal operations.

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

2 Purpose

The purpose of this policy is to outline the acceptable use of Information Technology in all its forms at DMI. These rules are in place to protect the employee and DMI. Inappropriate use exposes DMI to many different risks such as virus attacks, compromise of network systems and services, and legal consequences.

3 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct DMI business or interact with internal networks and business systems, whether owned or leased by DMI, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at DMI are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with DMI policies and standards, and South African laws and regulations. Exceptions to this policy are documented in section 5.2

4 Policy

4.1 General Use and Ownership

4.1.1 DMI proprietary information stored on electronic and computing devices whether owned or leased by DMI, the employee or a third party, remains the sole property of DMI.

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of DMI proprietary information.

4.1.3 You may access, use or share DMI proprietary information only to the extent it is authorized and necessary to fulfill your assigned duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use, and if there is any uncertainty, employees should consult their manager.

4.1.5 For security and network maintenance purposes, authorized individuals within DMI may monitor equipment, systems and network traffic at any time.

4.1.6 DMI reserves the right to audit networks, devices 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 DMI network must comply with this Policy.

4.2.2 System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure access to passwords, is prohibited.

4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4 Postings by employees from a DMI email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of DMI, unless posting is in the course of business duties.

4.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware and other threats such as phishing.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate responsibilities (e.g. systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of DMI authorized to engage in any activity that is illegal under South African law while utilizing DMI-owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which 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. This includes but is not limited to the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by DMI.

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 DMI 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 DMI business, even if you have authorized access, is prohibited.

4. Introduction of malicious programs into the DMI network (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. 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.

6. Using a DMI computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or other legislation.

7. Making fraudulent offers of products, items, or services originating from any DMI account.

8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

9. 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.

10. Port scanning or security scanning is expressly prohibited unless prior notification to DMI IT team is made.

11. 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 duties.

12. Circumventing user authentication or security of any host, network or account.

13. Introducing honeypots, honeynets, or similar technology on the DMI network.

14. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

15. 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.

16. Providing information about, or lists of, DMI employees to parties outside DMI.

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".

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 other means, 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 DMI's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by DMI or connected via DMI's network.

7. Posting the same or similar non-business-related messages to any service.

4.3.3 Blogging and Social Media

1. Blogging by employees, whether using DMI’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 DMI’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate DMI’s policy, is not detrimental to DMI’s best interests, and does not interfere with an employee's regular work duties. Blogging from DMI’s systems is also subject to monitoring.

2. Employees are prohibited from revealing any DMI confidential or proprietary information, trade secrets or any other material when engaged in blogging.

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of DMI and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments

when blogging.

4. Employees may also not attribute personal statements, opinions or beliefs to DMI 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 DMI. 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, DMI's trademarks, logos and any other DMI intellectual property may also not be used in connection with any blogging activity.

5 Policy Compliance

5.1 Compliance Measurement

The DMI IT team will verify compliance to this policy through various methods, including but not limited to, ad hoc and periodic monitoring, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the DMI IT team in advance.

5.3 Non-Compliance

An employee who becomes aware of any aspect of non-compliance with this policy, whether by themselves or another employee, whether accidental or through any other cause, must report this incident to the DMI CEO.

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

- Data Classification Policy
- Social Media Policy
- Minimum Access Policy
- Password Policy

7 Source and Definitions

The primary source of this DMI Acceptable Use Policy (AUP) is SANS Institute (www.sans.org) and is based on their example AUP as at June 2014.

The definition of terms used in this policy can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/