**Internet Usage Policy**

Prepared By

**IT Security**

**VERSION: 1.0**

All rights reserved. This document is a proprietary product of IT Security and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission from IT Security, is strictly prohibited. Any printed copy of this document is uncontrolled

**CHANGE HISTORY**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Date** | **Summary of changes** | **Author** | **Pages affected** | **Remark** |
| 1.0 |  |  |  |  |  |
|  |  |  |  |  |  |

Table of Contents

**PRINCIPLES OF INTERNET SECURITY POLICY 4**

**GENERAL POLICY FOR INTERNET CONNECTION 4**

## GENERAL POLICY FOR INTERNET USAGE 4

**EXTERNAL REPRESENTATIONS OVER THE INTERNET 5**

**EXPECTATION OF PRIVACY 5**

**USE OF INTRANET NETWORK 6**

***ENFORCEMENT 6***

# PRINCIPLES OF INTERNET SECURITY POLICY

* 1. The Internet or another organization’s network should be treated as entrusted network.
	2. Until the internal security controls are established, connection to such network should be assumed as not in compliance to the internal corporate security standards. The connection should therefore first be evaluated for information security before implementation.
	3. In recognition of the Internet as an unsecured channel for data communication, the use of it for *business transaction or processing* as versus for *exchange of information or communication purpose* should be treated with the corresponding controls and appropriate security measures.

## GENERAL POLICY FOR INTERNET CONNECTION

* 1. No private Internet Service Provider (ISP) accounts and unauthorised dial-up lines should be used unless with prior authorisation from the Management (e.g. exception for telecommuters and mobile computer users).
	2. All Internet activity must pass through the company’s established gateway so that access controls and related security mechanisms can be applied. Gateways are commonly established through use of firewalls.
	3. Where an http proxy is established in the company for browsing in the Internet, all web browsers shall be configured to use the http proxy.
	4. Automatic updating of software or information on computers from vendor's system via Internet background "push" technology is prohibited. Exception to this should be authorised by the Management (e.g. virus signature live update at the anti-virus gateways) and the security measures be put in place in the computers.
	5. ***Staffs are not allowed to connect any modems to their desktops or notebook to access the Internet or any external networks, except those approved for specific business use.***

## GENERAL POLICY FOR INTERNET USAGE

* 1. Web browsing generally must be used only for business activities. Incidental personal use is permissible so long as: -
		+ 1. It does not consume more than a trivial amount of resources
			2. Does not interfere with user productivity, and
			3. Does not pre-empt any business activity
	2. Employees should not visit websites for private commercial activities or for amusement/entertainment purposes.
	3. ***Access to Internet services that provide pornographic material or other illegal or undesirable material are forbidden.***
	4. ***Staff is individually accountable for their own behaviour and actions. Outbound communications must not be inflammatory, harassing, defamatory, disruptive to other’s operations, or otherwise reflect poorly on the organisation’s reputation or image.***
	5. ***Staff should not forward any security alert/warning or chain mail that they received from the Internet to other staff. All such alerts/warning should be forwarded to IT Security Department for verification.***
	6. ***Spamming is prohibited.***
	7. ***Sensitive, critical or value bearing information must not be transmitted across the Internet without enhanced security controls such as encryption.***
	8. No corporate resources connected to the Internet shall be used to: -
		+ 1. Download or disseminate offensive or illegal materials
			2. Unauthorized hosting of information to anyone or to any site
			3. Process data unrelated to work or upload information without authorization
			4. Scan for information or disrupt the operation another computer system, whether externally or internally
			5. Intercept data in transmission whether externally or internally, unless with prior Management’s approval
	9. Employees should comply with relevant local Internet laws and computer usage acts.
	10. Any downloading from the Internet should be carried out in a controlled environment, such as on desktop/notebook which is isolated from the LAN and which is Anti-Virus protected and monitored. Any exception to this has to be authorised by the Management.
	11. Files downloaded should be scanned, and ascertained as malicious code (virus) free before being use or being transferred to other desktops/notebooks/servers.

## EXTERNAL REPRESENTATIONS OVER THE INTERNET

* 1. Employees using corporate resources to access the Internet shall conduct themselves with the view of their affiliation with the company.
	2. Employees should therefore: -
		+ 1. Be aware that disclaiming one’s opinion as not reflecting that of the company in the messages posted in public or private discussion does not absolve their liability.
			2. Refer to the Public Affairs Department all questions and queries from the public or outside organisations on matters relating to the company and not communicate on behalf of the company unless prior authorisation is received from the Management.
			3. Comply with the company’s data classification policy on matters pertaining to releasing of internal information to the outside.
	3. Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or any company electronic communications system is forbidden.
	4. The user name, electronic mail address, organisational affiliation, and related information included with messages or postings must reflect the actual originator of the messages or postings.

## EXPECTATION OF PRIVACY

* 1. The company has the right, but not the duty, to monitor any/all aspects of its computer system, including, but not limited to, monitoring sites visited by users on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded or uploaded by users to the Internet, and reviewing e-mail sent and received by users.
	2. It may be necessary for authorised personnel to review the content of an individual employee's communications during the course of problem resolution or in an investigation. The access privilege to perform such review should be authorised by the proper approval channels as decided by the Management.
	3. Except as otherwise specifically provided, users may not intercept or disclose, or assist in intercepting or disclosing, e-mail communications. The Company is committed to respecting the rights of its employees, including their reasonable expectation of privacy.

## USE OF INTRANET NETWORK

* 1. All proprietary content posted to the Intranet is the property of the company and is for the exclusive use of authorized persons.
	2. Posting information on the Intranet or forwarding of it to third parties should comply with the Data Classification policy and must not be carried out without prior authorisation from the Management.
	3. All external party’s access to the Intranet must be Management approved and the inter-network connectivity secured in compliance to the internal corporate security standards.
	4. Although the Intranet is an informal internal communications environment, the laws for copyrights, patents, trademarks, and the like still apply.
1. ***ENFORCEMENT***

# *All staffs are required to comply with this security policy and its appendices. Disciplinary actions including termination may be taken against any Organization staffs who fail to comply with the Organization’s security policies, or circumvent/violate any security systems and/or protection mechanisms.*

# *Staff having knowledge of personal misuse or malpractice of IT Systems must report immediately to management and IT Security.*

* 1. *Organization’s staff must ensure that Organization’s contractors and others parties authorized by the Organization using its internal computer systems, comply with this policy.*
	2. *Where the role of the service provider is outsourced to a vendor, the outsourced vendor should ensure compliance with this policy.*