**Information Systems Security Policy**

Prepared By

**IT Security**

**VERSION: 4.0**

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

[*1.* *PURPOSE* 4](#_Toc43588473)

[*2.* *SCOPE* 4](#_Toc43588474)

[*3.* *OBJECTIVE* 4](#_Toc43588475)

[4. POLICY 4](#_Toc43588476)

[4.1 APPROVED USAGE OF COMPUTER 4](#_Toc43588477)

[4.2 COMPUTER SOFTWARE 6](#_Toc43588478)

[4.3 COMPUTER HARDWARE 6](#_Toc43588479)

[4.4 VOICE AND FAX SYSTEMS 6](#_Toc43588480)

[4.5 IDs, PASSWORDS, MAGNETIC / SMART CARDS IDs 7](#_Toc43588481)

[4.6 PROTECTING CONFIDENTIAL INFORMATION 7](#_Toc43588482)

[4.7 PROTECTING COMPUTER RESOURCES 8](#_Toc43588483)

[4.8 THE INTERNET 9](#_Toc43588484)

[4.9 UTILIZATION OF NON-COMPANY OWNED EQUIPMENT 9](#_Toc43588485)

[*5.* *ENFORCEMENT* 10](#_Toc43588486)

# PURPOSE

Information assets and IT systems are critical and important assets of CompanyName. Appropriate steps must be taken to ensure all information and IT systems are adequately protected from a variety of threats.

This document provides the management direction and support for information security. It set a clear direction and demonstrates support and commitment to information security through the issuance and maintenance of an information security policy across the organization. It ensures reliable and secured information assets and IT systems in order to carry out its business, fulfilling its customers’ security requirements.

# SCOPE

All employees, contract staff and third party vendors are required to comply with this policy when they use the Company's internal computer systems (including personal computers, other workstations, infrastructure, applications, devices and connections) and information (including report, emails, memorandum or other materials created by CompanyName).

Disciplinary action, including dismissal, may be taken against any CompanyName employee and/or third party vendor who fail to comply with the Information Systems Security Policy, or circumvent/violate any Security Systems and/or protection mechanisms.

# OBJECTIVE

The main objective of this policy is to outline the Information Security’s requirements to all staff, vendors, consultants, contractors, and contract staff.

# POLICY

## APPROVED USAGE OF COMPUTER

* + 1. CompanyName computer systems must only be used for conducting the Company's business or for purpose authorised by CompanyName management
    2. Storing of any non-business related files and inappropriate materials such as mp3, audio-video, screen saver, etc, is prohibited
    3. Staff should not try to access systems for which they do not have authorisation or which they do not need in order to perform their job. If access to additional functions or applications is required, the staff department head should arrange for it
    4. Usage of CompanyName information systems and resources for personal usage or on behalf of a third party (i.e., personal client, family member, political or religious or charitable or school organization, etc.) is strictly prohibited
    5. Usage of CompanyName information systems to store, process, download, or transmit data that can be construed as biased (politically, religiously, racially, ethnically, etc.) or supportive of harassment is strictly prohibited

## COMPUTER SOFTWARE

* + 1. You must have a valid licence obtained by CompanyName for all license software that you install in your computer. Never copy or duplicate licensed software, except as explicitly allowed in the license terms and conditions
    2. Personal or other licensed software cannot be used for the Company's purposes unless authorised by the Company and vice versa
    3. You are not permitted to remove/delete/deactivate any software or anti-virus*/spyware* programs installed by CompanyName in your computer or workstation
    4. You must not use *any* *software (freeware, shareware, commercial software)* for activities that may cause interruptions to business operations or internal processes
    5. You must protect the Company's data stored in computers against virus attacks by scanning all media with authorised anti-virus software before usage
    6. You must not use any *software (freeware, shareware, commercial software)* obtained from any third party unless authorised by CompanyName’s *IT Security*
    7. You must not install or direct others to install illegal or unlicensed copies of computer software into any computer system of the Company
    8. You are not allowed to use any program/script/command, or sending messages of any kind with the intent to interfere with a staff’s terminal session

## COMPUTER HARDWARE

* + 1. Every employee is responsible to help reduce the possibility of theft of CompanyName owned/leased computer workstations and the information they contain. If you are using a laptop computer, extra care such as physical lock should be taken to safeguard it
    2. You must not add, remove, replace, or substitute any computer components (including detachable) without prior written approval from the Company
    3. You must not reconfigure or change the set-up of LAN PC workstations without the knowledge and approval of CompanyName’s Information Systems Division

## VOICE AND FAX SYSTEMS

* + 1. You must never provide sensitive information over the telephone or fax to anyone without verifying the identity of the person at the other end
    2. For sensitive fax transmissions, you must ensure that the receiver is standing next to the fax machine and uses the Company’s fax coversheet

## IDs, PASSWORDS, MAGNETIC / SMART CARDS IDs

* + 1. A computer access ID, password, magnetic card/smart card or token are the primary keys to computer security. These uniquely identify you, and allow you access to CompanyName information and computer services. For your own protection, and for the protection of CompanyName's confidential information, keep your password secret, safeguard your magnetic card/smart card and do not share it with anyone else. You shall be held responsible for its use and misuse
    2. You must never use someone else’s ID, password, magnetic card/smart card or token, unless authorised by the Company. Procedures on reassignment of IDs, magnetic cards, smart cards, etc, must be adhered to
    3. All means of access (IDs, passwords, magnetic card/smart card) to information kept in the computer systems shall be taken away immediately from every staff who has tendered his/her resignation or whose services has been terminated
    4. All access shall be documented in the user Access Matrix. User Access Matrix shall be reviewed at least once every six months or whenever there are changes. All access shall be allocated based on the endorsed user Access Matrix

## PROTECTING CONFIDENTIAL INFORMATION

* + 1. Confidential data or information should not be used for purposes other than intended
    2. Confidential data or information should be classified to indicate sensitivity
    3. Confidential data that is no longer required should be erased
    4. Confidential information must be protected against unauthorised access: -
    - Information about, or lists of, CompanyName employees and customers should not be provided to parties outside the Company
* Information system controls that are in use in the Company or the way in which they are implemented should not be disclosed to parties outside the Company
* If confidential information is to be transmitted across the Internet, it must be encrypted using authorised encryption software
* Media containing confidential information must be destroyed or permanently erased (unrecoverable) before disposal
* All confidential print-outs must be properly stored
* Print-outs containing confidential information must be shredded before disposal
  + 1. The primary requirement for protecting confidential information in all computer media (e.g. *Discs (CDs or DVDs)*, print-outs, hard disk, *USB flash drive* etc) is that access to it may only be given to people on a NEED TO KNOW basis
    2. Under BAFIA, it is an offence to expose Company Customer Information to non-Company employees. Therefore, consultants, vendors, etc exposed to such information in the course of their work with CompanyName, should sign the standard non-disclosure agreement. Company Negara (BNM) must be notified before commencement of work by any consultant, vendor, etc using the standard notification process
    3. Confidential information must be protected against theft and unauthorised access during production, transmission, storage and disposal, e.g. shred print-outs before disposal, encrypt messages if left via e-mail systems, etc
    4. There must be procedures to establish the following controls for confidential information: -
       - No data may be downloaded unless authorised by the management of CompanyName
       - All data downloaded must be unto media authorised by CompanyName.
       - All downloaded data must be stored in encrypted format in any media
       - All downloaded data must not be removed from CompanyName’s premises unless explicitly authorised by the management of CompanyName
    5. A warning statement on misuse computer information and facilities must be displayed: -
* Upon successful login to a system, or
* Just before the login prompt to a system, or
* On the same screen that provides the login to a system
  + 1. The statement will read as follows:

Warning:

“Use of this system is restricted to individuals and activities authorized by the management of the CompanyName Group. Unauthorized use may result in appropriate disciplinary action and/or legal prosecution. "

The words “CompanyName Group” will be replaced by the word “organisation” for statements displayed on devices or equipments that are accessible to the public.

## PROTECTING COMPUTER RESOURCES

* + 1. Staff should protect Company’s computer resources from unauthorised access
    2. Desktops/workstations/terminals should not be left logged-on and unattended
    3. Workstation’s screen saver facility with password protection should be used
    4. Staff should backup all important data on their desktops on a regular basis to protect it from loss, corruption or destruction. The back-ups must also be stored in a safe and secure place
    5. ***Discs (CDs or DVDs), USB flash drives, external hard drives and other removable media*** containing confidential data should not be left lying around and should be kept under lock and key when not in use
    6. IT Equipment belonging to the Company should not be taken outside the Company without proper authorisation
    7. Any implementation of IT solutions must be done or co-ordinated by Information Technology Department

## THE INTERNET

* + 1. The usage of the Internet by authorised CompanyName staff must be for conducting the Company's business or for authorised purposes only
    2. CompanyName staff must not use the Company's Internet facilities to deliberately propagate any virus, worm, Trojan Horse, etc
    3. CompanyName employees must seek assistance from Legal Department and approval from Management before incorporating anything downloaded from the Internet (or any external on-line services) into a product or material CompanyName intends to distribute internally or externally
    4. You are not allowed to create web or home pages containing information related to the Company without prior approval from the Management
    5. Web page content must be in accordance with specific company directives, and the page layout must follow the guidelines defined
    6. You are not allowed to speak or write in the name of CompanyName to any News Group, "Chat Group" or any other forum on the Internet; or respond to queries/complaints unless already authorised by the Company to perform this function
    7. Network scanning, using any hardware equipment or software are strictly prohibited

## UTILIZATION OF NON-COMPANY OWNED EQUIPMENT

* + 1. The method and equipment used to access the information systems of the Company must be properly supervised and controlled in order not to compromise the integrity and privacy of the information residing in the system. For this reason, importance of proper management must be in-place
    2. Staff are not allowed to use their personal or non Company-owned computer equipment to connect and link to any system of the Company without prior approval from their superiors and IT Security Department
    3. Connections of any personal and non Company-owned computer equipment to the computer systems and network of the Company should be removed if no longer required

# ENFORCEMENT

All staffs are required to comply with this security policy and its appendices. Disciplinary actions including termination may be taken against any CompanyName staffs who fail to comply with the Company’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.

CompanyName’s staff must ensure that CompanyName’s contractors and others parties authorized by the Company using its internal computer systems, comply with this policy.

Where the role of the service provider is outsourced to a vendor, the outsourced vendor should ensure compliance with this policy.