**Desktop Security 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

**GENERAL REFERENCE 4**

**GENERAL GUIDELINES FOR DESKTOP 4**

**USAGE OF DESKTOPS 4**

**DIAL-UP POLICY 4**

***ENFORCEMENT 5***

**GENERAL REFERENCE**

Desktop-based systems generally refer but not confined to Intel-based computer systems, which unlike larger computer systems such as Open-platform systems (UNIX), AS/400, or the mainframe system, are contemporarily predominant up to mid-range level.

When a notebook is connected into the Organization’s internal network (LAN), it will be considered as a "desktop" since its usage is same as a desktop.

## GENERAL GUIDELINES FOR DESKTOP

* 1. Purchases of all software, hardware and peripheral components for the company’s desktops shall follow standard recommendations as established or as advised by ISD. Requisition for any non-standard item should be justified by technical or business requirements, and with ISD’s endorsement or with Management’s approval.
  2. Replacement and additional software and equipment requirements for the desktops are likewise subjected to the above controls.
  3. All systems manuals, proof of software licenses, maintenance contracts and other purchase documents should maintain and kept under custody of ISD or the local Management in the case of subsidiaries and overseas centers.
  4. Only licensed software should be installed in the company, whether for use or for evaluation. Prior authorization should be obtained from ISD or the Local IS Administrator or from Management before any such installation.
  5. Anti-virus software should be installed for all desktops. For anti-virus measures, the Company’s *Anti-Virus Policy* should be adhered to.
  6. Screen savers should be installed on desktops with time-out capacity set for 15 minutes or less, and with password protection.
  7. Only authorized vendor should carry out repair/maintenance. In the event of the hard-disk drive is required to be sent to vendor for maintenance, any of the company’s sensitive/confidential data/files within should be backed-up to another secured media (e.g. floppy, CDRW, another hard disk). The data/files should then be completely and irrecoverably deleted /sector-erased to prevent unauthorized access.

1. **USAGE OF DESKTOPS**

The company’s desktops should only be used for business purposes or work related functions only.

* 1. Users should not alter the desktop’s configuration (e.g. the computer-name, its allocated IP address) that has been put in place by ISD or the Local IS Administrator.
  2. Users are not allowed to install or use any network analyzer or scanner on the desktop. Users are also not allowed to monitor the network traffic in the LAN, which the desktop is connected to.
  3. Sharing and storing of any non-business related files such as MP3, audio-video, screen saver etc is prohibited. If file sharing or shared drive across LAN is required for business related, control must be in place to secure it. (e.g. Require authentication, file permission)

1. **DIAL-UP POLICY**

The following directives must be in place for dial-up connections: -

* 1. 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.
  2. Unauthorized installation of a modem that bypasses the company’s gateway (e.g. firewall) for direct outbound and inbound access while the desktop is connected to the LAN is strictly prohibited.
  3. Any modem use should be justified to ISD or the Management and authorization obtained prior to installation.
  4. For authorized modem connection on desktop: -
     + 1. The authorized modem and the telephone number used should be tracked and controlled by ISD or the Local IS Administrator
       2. Call back arrangement should be used for high-sensitivity data or critical applications. For data confidentiality and integrity, encryption mechanism and checksum measures should be in place
       3. At a minimum, all modem access must require identification and authentication for login
       4. In-bound dial-up or in-bound Internet privileges must not be given to third party vendors unless prior clearance is obtained from ISD in consultation to IS Security, based on the vendor’s legitimate business need for such access. These privileges must be enabled for specific individuals and only for the time period required accomplishing approved tasks
       5. For the above vendor’s access, regular and documented changing of the inbound dial-up connection contact numbers and login specifics must be put in place
       6. If the modem-installed desktop is connected to the company’s LAN, ISD should be consulted and IS Security notified for proper isolation of the desktop so as not to compromise the security of the LAN.

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.***