**Anti Virus 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 GUIDELINES AGAINTS MALICIOUS CODE 4**

**POLICY AGAINTS MALICIOUS CODE FOR ALL 5**

**POLICY AGAINTS MALICIOUS CODE FOR ADMINISTRATORS 5**

***ENFORCEMENT 5***

## GENERAL GUIDELINES AGAINTS MALICIOUS CODE

* 1. Virus protection controls can be applied through various measures: -
		+ 1. Installation of Anti-virus software
			2. Controlling of share across network
			3. Segmentising of network with access control through firewalls, routers, or switches
			4. Installation of Content Filtering software
			5. Installation of Intrusion Detection System
			6. Any other proven measures
	2. Where virus control is not through use of anti-virus software, other means of measures as above should be in place.
	3. At the minimum, anti-virus software should be installed for all desktop-based[[1]](#footnote-1) computer systems such as workstation-desktops, notebooks, network file and print servers, and email gateways.
	4. Installed anti-virus software should be configured to run in full-time at the background, and with auto-protect or similar mode. The anti-virus-related activities should be system logged.
	5. Anti-virus software should be maintained up to date with the latest virus signatures or patterns.
	6. Updating of latest virus signatures or patterns to the computer systems should be automated where possible. If automatic-process is not possible, a manual process should be in place to enable end-users’ action in the updating.
	7. A re-scan of the computer systems should be executed immediately after the signature/pattern update.
	8. All above virus protection controls should only be administrated and maintained by authorized personnel.[[2]](#footnote-2)
	9. Virus incident should be investigated by authorized personnel. A documentation of the investigation should follow after its completion.
	10. A documented virus incident response process should be in place. The process can either exist as a stand-alone process or be subsumed under a larger Incident Response Process.
1. **POLICY AGAINTS MALICIOUS CODE FOR ALL**
	1. Staffs are not allowed to intentionally write, generate, compile, copy, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software.
	2. All new software, files or mails must be scanned with the anti-virus software before use.
	3. All desktop-based removable storage media such as floppy disks, tape-cartridges, zip or other drives should be scanned with the installed anti-virus before installing into any desktop, notebook or LAN server.
	4. If a suspected virus that can not be repaired is detected by the installed anti-virus software, the computer system user must: -
		* 1. Cease all operations
			2. Disconnect the infected computer system from the network
			3. Immediately notify the authorized personnel2
			4. Document conditions and status of the environment
	5. Users must ensure the installed anti-virus software is not disabled.
	6. Users must not change the anti-virus software’s configuration, which was installed by authorized personnel.
	7. Staff should validate any virus alert received from an entrusted source[[3]](#footnote-3) with IS Security at Head Office or with the trusted anti-virus site before taking action. Until verified, such information should not be disseminated indiscriminately. This is to avoid unnecessary reaction to virus hoax at the expense of resources.
2. **POLICY AGAINTS MALICIOUS CODE FOR ADMINISTRATORS**
	1. Ensure compliance to the **GENERAL GUIDELINES AGAINTS MALICIOUS CODE** above.
	2. Be constantly informed of latest virus threats, whether directly through virus alert-service OR secondarily through the advisory alerting from Head Office support (as in the case for Local IS Administrators).
	3. Perform immediate virus signature/patterns update when available following a virus-alert notification. This process should be in addition to the regular virus update process.
	4. Perform forensic action following a virus infection in restoring the computer systems and investigating the incident.
3. ***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.***
1. *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, some mid-range servers or the mainframe system, are contemporarily predominant up to mid-range level.* [↑](#footnote-ref-1)
2. *Authorized support may be provided by outsourcer. Local authorized support may be provided by the Local IS Administrators who are appointed by Head of Departments. Outside of Head Office, for subsidiaries or overseas centers, the Local IS Administrators would be appointed by the resident manager in charge of Information Systems. Local authorized support to be advised by IT Security or other ISD support team from Head Office.* [↑](#footnote-ref-2)
3. *Except for the reference site of the installed anti-virus software or sites as informed by IS Security at Head Office, any other source of virus information should be treated as entrusted source.* [↑](#footnote-ref-3)