**Name : Leng Sopharot**

**Room 209**

**Sex M**

**Antivirus and Malware Policy**

**1 Policy Statement**

To meet the enterprise business objectives and ensure continuity of its operations,  XXX shall adopt and follow well-defined and time-tested plans and procedures, to ensure the protection of IT assets from malware and virus attacks. IT assets must be employed in ways that achieve the business objectives of XXX. IT assets shall be protected in a way that ensures that they are resistant to virus and malware attacks and that all preventive and protective measures shall be used to resist such malware attacks. The policy and respective procedures, guidelines and forms such as facilities allocation forms shall be available to the CEO,  GMs,  AGMs, managers, and CISO of XXX.

**2. Purpose**

The purpose of this policy is to promote the use of anti-virus and other anti-malware software and educate the employees regarding the policies that are widely followed to use an anti-malware effectively. Besides, this policy provides direction to ensure that legal regulations are followed.

**3. Scope**

**3.1 Employees**

This policy applies to all  Employees, Contractors, and Third Party Employees, who have access to IT assets of XXX and may be bound by contractual agreements.

**3.2 IT Assets**

This policy applies to all workstations and servers that are owned or leased by XXX.

**3.3 Documentation**

The Policy documentation shall consist of Anti-malware Policy and related guidelines.

**3.4 Document Control**

The Anti-Malware Policy document and all other referenced documents shall be controlled. Version control shall be used to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purpose.

**3.5 Records**

Records being generated as part of the Anti-Malware Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

**3.6 Distribution and Maintenance**

The Anti-Malware Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the CISO and system administrators.

**4 Privacy**

The Anti-Malware Policy document shall be considered as “confidential” and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

**5 Responsibility**

The CISO / designated personnel is responsible for the proper implementation of the Policy. The Virus/malware Prevention Policy applies equally to all individuals that use any XXX Information Resources.

**6 Policy**

FCI shall adopt certain practices to prevent malware/Virus problems:  
i. All workstations whether connected to XXX network, or standalone, must use XXX- approved anti-virus and anti-malware software and configuration.  
ii. The anti-virus and anti-malware software must not be disabled or bypassed.  
iii. The settings for the anti-virus and anti-malware software must not be altered in a manner that will reduce the effectiveness of the software.  
iv. The automatic update frequency of the anti-virus and anti-malware software must not be altered to reduce the frequency of updates.  
v. Each file server attached to XXX network must utilize XXX-approved anti-virus and anti-malware software and set up to detect and clean malware that may infect file shares.  
vi. Every virus/malware that is not automatically cleaned by the anti-virus and anti-malware software constitutes a security incident and must be reported to the Help Desk.  
vii. The organization shall adopt suitable controls to prevent and detect the introduction of malicious code and unauthorized mobile code.  
viii. The information system automatically updates malicious code protection mechanisms e.g. automatic updates of anti-virus and anti-malware software.  
ix. Each E-mail gateway must utilize XXX-approved e-mail anti-virus software and must adhere to the ISMS rules for the setup and use of this software.

**7 Enforcement**

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy.