**Content Filter for Web and Email Access 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

**PURPOSE 4**

**SCOPE 4**

**REFERENCES 4**

**INTRODUCTION 4**

**WEB CONTENT ACCESS 4**

**EMAIL CONTENT 5**

**CONTENT FILTER APPLIANCE 5**

**ENFORCEMENT 6**

1. **PURPOSE**

The purpose of this policy is to provide an acceptable level of access for email and web content.

1. **SCOPE**

The scopes of this policy are:

* + - 1. All email bearing Organization Group address names are bounded by this policy,
      2. All web access from the computer infrastructure of Organization Group to the Internet

1. **REFERENCES**
   * + 1. Organization Group Email Usage Policy
       2. Organization Group Internet Usage Policy
2. **INTRODUCTION**
   1. When employees access inappropriate or illegal content, organizations lose productivity, expose themselves to legal liability, and experience a decrease in network performance.
   2. In addition, spyware, viruses, and, worms can be easily distributed onto the network from web sites that have untrusted contents.
   3. A web content filtering solution can alleviate all of these problems by blocking access to inappropriate web sites.
3. **WEB CONTENT ACCESS**
   1. Websites that contain profanity, seditious content, unlawful and defamatory in nature are not allowed to be accessed using corporate Internet resources.
   2. Websites containing malicious codes, unknown embedded java script and plug-ins that requires user to download must be avoided.
   3. Websites that offers online games, gambling, chat, auto surf and peer-to-peer file distribution are not allowed.
   4. Instant messaging applications (Yahoo Messenger, MSN Messenger, ICQ, Meebo etc.) that run on websites are not allowed. Using free email provider which has instant messaging capability are prohibited.
   5. Websites that offer background services (daemons) that unsecured such as IRC bots; eggdrop; BitchX; XiRCON are not allowed to be accessed.
   6. No downloading of files with below extension are allowed (not limited to):-
      * 1. Audio (e.g. .mp1, .mp2, .mp3, .mp4, real audio)
        2. Video (e.g. .mpg, .mpeg, .xing, .asf, VDOLIVE)
        3. .torrent
        4. Freetel
        5. Cooltalk
        6. H.323
        7. Backweb
4. **EMAIL CONTENT**
   1. Emails should be short and precise to save recipients storage.
   2. Sharing non-business attachments with friends and colleagues are not allowed. Chain emails are prohibited.
   3. Sending attachments that contains illegal and unlawful material e.g. profanity, seditious, defamatory in nature, advertisement are not permissible.
   4. Sending emails content which result in complaints from the recipient or from the recipient’s email provider, or which result in blacklisting of the sender’s email address or mail server are not allowed.
   5. Even though the unlawful emails not originating from the sender, the sender hold full responsibilities for every emails that the sender sent out.
   6. Spamming is prohibited.
   7. Please refer *1.009 Organization Group Email policy* for more details.
5. **CONTENT FILTER APPLIANCE**
   1. The content filter appliance blocks offensive and inappropriate content using enterprise-class policy enforcement.
   2. Content Filtering appliance policy should block based on (and not limited to):-
      * 1. Sender IP address
        2. Sender Domain
        3. Sender E-mail address
        4. Recipient Email address
        5. Attachment type
           1. Blocked attachment file extensions
           2. Block extension in archives
           3. Block password protected archives
           4. Block notification
           5. Notify sender of banned file interception
           6. Quarantined attachment extensions
           7. Quarantine extensions in archives
           8. Quarantine password protected archives
        6. Subject line content:-
           1. Subject blocking
           2. Subject quarantine
           3. Subject tagging
           4. Subject white listing
        7. Body content:-
           1. Message content blocking
           2. Message content quarantine
           3. Message content tagging
           4. Message content white listing
        8. Header content:-
           1. Header blocking
           2. Header quarantine
           3. Header tagging
           4. Header white listing
6. **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.