Protection of United Nations Assets from Malicious Software United Nations Secretariat ICT Technical Procedure

Ref: SEC.04.PROC

Revision History

Serial	Release Description	Release	Release Date	Author(s)
1.	New document	1.0	__ Oct 2014	Endorsed by ICT Policy Committee

Approved By

Atefeh Riazi, ASG/CITO

Date:

21Oct/14

2 October 2014

Protection of United Nations Assets from Malicious Software United Nations Secretariat ICT Technical Procedure

Section 1

Purpose and Scope

1.1 The purpose of this technical procedure is to provide directions on measures that must be taken by ICT Service Providers to achieve effective protection of United Nations assets from malicious software. These measures are important to enhance the security of any United Nations network against different types of malicious software and maintain a data communications environment that is free of viruses and other forms of malicious software.

1.2 This technical procedure applies to all computers, owned by the UN, that are connected permanently or temporarily to a United Nations network. It also applies to servers not on the United Nations network but "representing" the United Nations (e.g. website hosted on the cloud).

Section 2

Definitions

2.1 The following definitions shall apply for the purposes of the present procedure:

(a) *Authorized User*: any staff member who is authorized to use information and communication technology (ICT) resources;

(b) *ICT service providers*: United Nations Secretariat organizational units that provide ICT services to one or more Secretariat entities;

(c) *United Nations network*: computer network, either wired or wireless, under the control of an UN ICT service provider.

(d) *Malicious Software (Malware)*: any software code, script, active content, or program that is designed to penetrate systems without owner's awareness and consent. This software can cause damage, disrupt computer operation, send spam, gather sensitive information, or gain access to private computer systems. There are various types of malicious software such as viruses, worms, spyware, Trojan horses, etc;

(e) *Approved standard software*: Software that has been approved as an ICT standard by the ICT service provider, and where support is provided by the ICT provider

(f) *Non-standard software*: Software that is not been supported by the ICT service provider, usually a business specific software.

(g) *Security software*: any computer program, such as anti-virus, anti-spyware, and software firewall that is designed to enhance information security;

(h) *Computers*: includes desktop and laptop computers;

(i) *Servers*: computers hosted in a data center providing services to many users via the network;

(j) *Network appliances*: hardware device with integrated software (firmware), specifically designed to deliver a limited and fixed set of network service.

(h) *Bastion Host, also known as Jump Station*: computer serving as the only gateway between a trusted and untrusted network that gives limited, authorized and auditable access to the trusted network.

Section 3

Responsibilities

3.1 Responsibilities of ICT Service Providers are:

(a) to implement this ICT Technical Procedure, and in case where there is no clear ICT service provider identified, then the responsibility shifts to the business unit owning the computer.

(b) to communicate to the authorized users the "General Guidance for Users" in Annex 1.

(c) to ensure that the authorized users:

(1) take measures to protect against malware by adhering to the policy and guidelines provided in this document;

(2) attend any security awareness training proposed by ICT Service Provider or OICT;

(3) are aware and sufficiently trained for reporting suspicious behavior related to the use of the computer or potential alterations to the network infrastructure, to the ICT service provider in due course;

(4) follow instructions from ICT Service Provider when notified about detected malware.

Section 4

General Policy

4.1 All computers connected to United Nations networks must be equipped with approved security software. This software must be active at all times, be scheduled to perform security checks at regular intervals, and have its definition files kept up-to-date.

4.2 All applicable security updates ("patches") must be installed to the operating system and to all managed software components, no later than 30 days after release by the vendor; critical updates should be deployed as soon as possible. All such updates should be tested prior to deployment. If an update cannot be deployed, e.g. due to a software incompatibility, this needs to be documented, and other mitigating measures implemented;

4.3 In the event that a computer has been infected or compromised by malware, it must be immediately disconnected from the network and isolated. ICT Service Provider must disconnect a computer that appears to be infected, without prior notice, and isolate it until verified free from malware.

4.4 Security Updates for the Operating System as well as for managed software should be started automatically on United Nations computers when attached to the network. Security updates must be tested and validated by the ICT Service provider before being applied to any computer.

4.5 All e-mail traffic should be scanned for malware. Files attachments identified as malware by the OICT and/or other ICT service providers must blocked by the e-mail system.

4.6 Security scanning and integrity checking of system files shall be performed on a regular basis to detect any malware;

4.7 All computers must be configured to limit administrative privileges to only authorized users who require such access to perform their official duties, such as technical support staff, as explained in the "Access Control for the United Nations Secretariat ICT Technical Procedure".

Section 5

Servers and Network Appliances Procedure

5.1 Servers and network appliances must follow the Logical Design of Network (Security) Zones as designed by OICT. The usage of bastion host to access the servers and network appliances must be the primary way to access the servers for admin and maintenance. Servers by default should not be accessible from

the internet. If required and justified, servers may be accessible from the internet only if in a DMZ, be protected using firewalls, only on authorized ports.

5.2 Servers and network appliances must have internet access removed, unless needed for service. Access is done via bastion host and software/firmware update is done via internal central server (or external media). A record of who accessed the network device, what occurred, and when for auditing purposes must be kept; only secure protocol must be used for accessing web based admin interface – SSH or HTTPS must be the preferred protocol; passwords should appear encrypted when viewed through the configuration file; login banners should be used as a preventive measure against unauthorized access; set idle timeouts and keep-alives to detect and close inactive or hung sessions.

5.3 Physical access must be limited to hardware maintenance. Any external media (USB key, external hard drive, CD/DVD-ROM, PCMCIA Card) to be connected to the server must be scanned manually by the operator before being connected to the server or network appliance.

5.4 Systems must be kept up-to-date with OS and application upgrades and patches. Access to the local patch server must be regulated and controlled. Monitoring can be used to validate that the machine is patched.

5.5 Whitelist applications running on server, so only essential services are running and can be run. All services which have no reason to being run must be uninstalled, or disabled if uninstallation is not possible. In the particular case of SNMP, ideally SNMP version 3 should be used as it is more secure. If not possible, for SNMP v1 and v2, Access Control Lists (ACL) must be configured to limit the IP addresses that can send SNMP commands to the device, the SNMP community strings should be treated like root passwords by changing them often and introducing complexity in them. OICT should make available guidelines/default config for basic servers (e.g. Database, fileserver,…) in a single central repository.

5.6 Default usernames and passwords for operating systems and applications must be removed, or at least changed from default. Default sample applications must be removed. In the case of SNMP, default community strings such as 'public' and 'private' should be changed. All password defined on the network devices must meet the "United Nations Password policy standard". When possible, limit the rate of login attempts and enforce a lockout period upon multiple authentication failure attempt, to restrict vulnerability to dictionary and denial-of-service (DoS) attacks.

5.7 When the function of the server has an element of interaction with external users (e.g. file server, print server, web proxy) and that running an antivirus will not impact performance, an antivirus, of a brand different from the one used on end-user computer, must be installed, unless the server platform has no antivirus software available.

5.8 Servers and network appliances logs and configuration must have protection against tampering and must be scanned daily for detection of possible irregularity. All alterations to such files should be automatically reported to security personnel. Logs retention follows "Retention Schedules for ICT

Records United Nations Secretariat ICT Technical Procedure". Automated configuration backup for Network devices must follow the UN Backup policies.

5.9 In order to detect and remove memory only malware, a memory scan and/or a periodical reboot of the server/network appliances must be conducted on a systematic but not regular schedule. All change requests shall be logged whether approved or rejected on a standardized and central system. The approval of all change requests and the results thereof shall be documented, and the procedure follows "UN change management policy".

5.10 The principle of least privilege must be applied in the configuration of services, to prevent administrator-level privileges abuse by malware. The principle of least privilege refers to configuring hosts to provide only the minimum rights to the appropriate users, processes, and hosts. Network and System Administrator accounts creation must follow established procedure: the procedure should address approval from the Section head and record the authorization level given to the new administrator and the duration of that authorization.

5.11 For servers with Security Levels 2 and 3 requirements (as defined by "Access Control for the United Nations Secretariat ICT Technical Procedure"), server-based firewalls can restrict incoming and outgoing network activity for individual servers, to stop infected hosts from spreading malware to other hosts and stop data exfiltration.

Section 6

Incident Reporting and Handling

6.1 ICT Service Providers must follow the "Security Incident Response ICT Technical Procedure" to handle and report malware incident.

6.2 All reports and log files for all security incidents shall be retained following the schedule indicated by "Retention Schedules for ICT Records United Nations Secretariat ICT Technical Procedure".

Section 7

Ongoing Revisions

7.1 This document must be reviewed by the ICT Policy Committee:

- on an ongoing basis, at least once a year,
- after a major internal security incident has taken place,
- upon major changes to the United Nations internal network.

Annex-1

General Guidance for Users

a. Connecting non UN asset to any United Nations network which is not a public guest network is prohibited.
b. All computers connected to United Nations networks must be equipped with approved security software. This software must be active at all times, be scheduled to perform security checks at regular intervals, and have its definition files kept up-to-date. Users may not attempt to either alter or disable security software installed on any computer connected to any United Nations network without the express consent of the ICT Service Provider.
c. Security Updates for the Operating System as well as for managed software are started automatically on United Nations computers when attached to the network. Any action to disrupt or prevent updates is prohibited. For all non-standard software that users may require to install on United Nations computers, users are responsible to update security patches, no later than 30 days after release by the vendor, in collaboration with the ICT Service Provider.
d. Any activities with the intention to create and/or distribute malware onto the United Nations network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.
e. Users must report immediately to their ICT Service Provider (through Help Desk) about any incident or suspected incident of malware infection. Some signs of possible malware infection are malware warnings, unusual system or software behavior, and degradation in system performance. Users must not attempt to destroy or remove malware, or any evidence of that malware, without prior consultation from the ICT Service Provider.
f. In the event that a computer has been infected or compromised by malware, it must be immediately disconnected from the network and isolated. ICT Service Provider will disconnect a computer that appears to be infected, without prior notice, and isolate it until verified free from malware.
g. ICT Service Provider reserves the right to inspect Internet traffic including that which is transmitted via secure connections.
h. Always run the standard security software approved by United Nations.
i. Do not open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.
j. Exercise due diligence with e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (e.g. .exe) file disguised as a link. Do not click on any link sent to you if you were not expecting a specific link. If there a link you want to use, please retype or copy and paste the URL of the link, but do not click on it. Forward these types of messages to the local ICT provider so that they can take preventative measures to block the access to these links.
k. Do not open suspicious e-mail file attachments, even if they appear to come from known senders (e.g. a co-worker) if you were not expecting a specific attachment from that source. If an unexpected attachment is received, contact the sender (preferably by a method other than e-mail, such as phone) to confirm that the attachment is legitimate.

l. Do not respond to any suspicious or unwanted e-mails asking to reply, send personal information or unsubscribe from a mailing list. Response to such emails confirms the existence and active use of that e-mail address, potentially leading to additional attack attempts.
m. Do not copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.
n. Avoid direct disk sharing with read/write access. Always scan removable media, such as memory stick, portable hard drive, CD, and DVD, for malware before opening any file.
o. If instructed to delete e-mail messages believed to contain malware, be sure to also delete the message from your Deleted Items or Trash folder.
p. Back up critical data and systems configurations on a regular basis and store backups in a network file server or any other location indicated by the ICT provider.
q. Regularly update virus protection on personally-owned home computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.
r. Always login to your computer with regular user of limited privileges. Use admin accounts only if authorized to and when it is not possible to perform the action with a regular account.
s. Never connect UN-owned computers to the internet by bypassing the official means of connection (e.g. do not use a private 3G stick or personal hotspot, do not use private VPN or TOR or equivalent)

--- End of Document ---