

Anti-Virus Policy

- Reference:** CNS-P-I-ANTIVIRUS **Revision:** A
- Supersedes:** None
- Purpose:** CNS is to provide a computing network that is virus-free. The purpose of this policy is to provide instructions on measures that must be taken by AUB employees to help achieve effective virus detection and prevention.
- Source:** Computing and Networking Services (CNS).
- Approved by:** Nabil Bukhalid, Director of CNS **on:** August 28, 2007
Peter Heath, Provost **on:** Pending
- Applicability:** This policy applies to all computer users.
- Background:** A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event to computer software, data and/or the network. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, USB disks, and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to AUB in terms of lost data, lost staff productivity, and/or lost reputation.
- Scope:** This policy applies to all computers that are connected to the AUBnet network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both AUB owned computers and personally-owned computers attached to the AUBnet network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, and servers
- All employees are subject to this policy and required to abide by it.
- Policy:**
1. **Currently, AUB standard anti-virus for Windows OS clients and servers is based on McAfee anti-virus solution (<http://www.mcafee.com/>). McAfee agents are licensed with every newly purchased Windows OS system. Licensed copies of McAfee anti-virus can be purchased separately online via AUB iProcurement.**

2. All computers attached to the AUBnet network must run standard and supported anti-virus software. This anti-virus software must be active all the time and must be configured to perform on-access real-time checks on all executed files and scheduled virus checks at preset regular intervals. The virus definition files must be kept up to date all the time
3. Any activity intended to create and/or distribute malicious programs onto the AUBnet network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) is strictly prohibited.
4. If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, he/she must report such incident to the CNS immediately by e-mailing cns.helpdesk@aub.edu.lb. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.
5. No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from CNS.
6. Any virus-infected computer will be removed from the network until it is verified as virus-free.

Guidelines: Best Practices for Virus Prevention:

1. Always run the standard anti-virus software provided by AUB.
2. Never open files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.
3. Never open files or macros attached to an e-mail from a known source (even a coworker) if you were not expecting a specific attachment from that source.
4. Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.
5. AUB mail system scans all attachments for virus infections and blocks any trapped virus from being transmitted to client systems. McAfee anti-virus-shield on the client machine scans all email attachments for virus infections. Also, and by default AUBede e-mail client, Microsoft Outlook, blocks attachments with critical file extensions (see Appendix-A for details). AUBnet users should not alter the default email client configuration to override the security setup and send/receive banned extensions. A workaround to send/receive such business-critical files is to compress the file using a file compression utility.

6. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.
7. Avoid direct disk sharing with read/write access. Always scan any removable media for viruses before using it.
8. If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.
9. Back up critical data and systems configurations on a regular basis and store backups in a safe place.
10. 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.

The following activities are the responsibility of Computing & Networking Services:

1. CNS is responsible for maintaining and updating this Anti-Virus Policy. Copies of this policy will be posted on AUB web site. Check one of these locations regularly for updated information.
2. CNS will keep the anti-virus products it provides up-to-date in terms of both virus definitions and software version in use. AUBede McAfee EPO server is scheduled to check the McAfee update site every one hour for updates and to auto update both the virus definition file and the software version. AUBede McAfee client configuration is set to check the EPO on a daily basis for updates and to auto update and report success and failures. CNS will invest adequate efforts to identify AUBede clients who did not attempt to update their virus definitions file for more than 3 months and will take appropriate remedial actions.
3. CNS will apply any updates to the services it provides that are required to defend against threats from viruses.
4. CNS will install anti-virus software on all AUB owned and installed desktop workstations, laptops, and servers.
5. CNS will assist employees in installing anti-virus software according to standards on personally-owned computers that will be used for business purposes. CNS will not provide anti-virus software in these cases.
6. CNS will take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, CNS may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.

7. CNS will perform regular anti-virus sweeps on all AUBede managed and active computers every first Tuesday of the month.
8. CNS will check the EPO logs on a daily basis for detected viruses that are not quarantines by McAfee anti-virus software and take appropriate remedial actions.
9. CNS will attempt to notify users of AUBnet systems of any credible virus threats via e-mail and AUB online bulletin. Virus reports will not be acted upon until validated. Employees should not forward these or any virus warning messages in order to keep network traffic to a minimum.

The following activities are the responsibility of AUB departments and employees:

1. Departments must ensure that all departmentally-managed computers have virus protection that is in keeping with the standards set out in this policy.
2. Departments that allow employees to use personally-owned computers for business purposes must implement virus protection processes and procedures that are in keeping with the standards set out in this policy.
3. Departments who don't employ staff with enough technical know-how to ensure compliance with this policy should seek the assistance of CNS to do so.
4. Departments' compliance with this policy shall be subject to audit.
5. All employees are responsible for taking reasonable measures to protect against virus infection.
6. Employees must not attempt to either alter or disable anti-virus software installed on any computer attached to the AUBnet network without the express consent of CNS and for a strictly limited period not to exceed in any case one working day.

Enforcement: Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Appendix-A

Attachments file types blocked by default by AUB official email client (Outlook).

File extension	File type
ade	Access Project Extension (Microsoft)
adp	Access Project (Microsoft)
app	Executable Application
asp	Active Server Page
bas	BASIC Source Code
bat	Batch Processing
cer	Internet Security Certificate File
chm	Compiled HTML Help
cmd	DOS CP/M Command File, Command File for Windows NT
com	Command
cpl	Windows Control Panel Extension (Microsoft)
crt	Certificate File
csb	csb Script
exe	Executable File
fxp	FoxPro Compiled Source (Microsoft)
gadget	Windows Vista gadget
hlp	Windows Help File
hta	Hypertext Application
inf	Information or Setup File
ins	IIS Internet Communications Settings (Microsoft)
isp	IIS Internet Service Provider Settings (Microsoft)
its	Internet Document Set, Internet Translation
js	JavaScript Source Code
jse	JScript Encoded Script File
ksh	UNIX Shell Script
lnk	Windows Shortcut File
mad	Access Module Shortcut (Microsoft)
maf	Access (Microsoft)
mag	Access Diagram Shortcut (Microsoft)
mam	Access Macro Shortcut (Microsoft)
maq	Access Query Shortcut (Microsoft)
mar	Access Report Shortcut (Microsoft)
mas	Access Stored Procedures (Microsoft)
mat	Access Table Shortcut (Microsoft)
mav	Access View Shortcut (Microsoft)
maw	Access Data Access Page (Microsoft)
mda	Access Add-in (Microsoft), MDA Access 2 Workgroup (Microsoft)
mdb	Access Application (Microsoft), MDB Access Database (Microsoft)
mde	Access MDE Database File (Microsoft)
mdt	Access Add-in Data (Microsoft)

File extension	File type
mdw	Access Workgroup Information (Microsoft)
mdz	Access Wizard Template (Microsoft)
msc	Microsoft Management Console Snap-in Control File (Microsoft)
msi	Windows Installer File (Microsoft)
msp	Windows Installer Patch
mst	Windows SDK Setup Transform Script
ops	Office Profile Settings File
pcd	Visual Test (Microsoft)
pif	Windows Program Information File (Microsoft)
prf	Windows System File
prg	Program File
pst	MS Exchange Address Book File, Outlook Personal Folder File (Microsoft)
reg	Registration Information/Key for W95/98, Registry Data File
scf	Windows Explorer Command
scr	Windows Screen Saver
sct	Windows Script Component, Foxpro Screen (Microsoft)
shb	Windows Shortcut into a Document
shs	Shell Scrap Object File
tmp	Temporary File/Folder
url	Internet Location
vb	VBScript File or Any VisualBasic Source
vbe	VBScript Encoded Script File
vbs	VBScript Script File, Visual Basic for Applications Script
vsmacros	Visual Studio .NET Binary-based Macro Project (Microsoft)
vss	Visio Stencil (Microsoft)
vst	Visio Template (Microsoft)
vsw	Visio Workspace File (Microsoft)
ws	Windows Script File
wsc	Windows Script Component
wsf	Windows Script File
wsh	Windows Script Host Settings File