Information Security Management System

Anti - Virus Policy

Document no. JMBGRP/ISMS/Pol-AV

Version no. v1.2

Document details

Classification	Internal	
Released date	28.08.2018	
Description	The objective of this documented policy is to ensure that all relevant individuals understand the key elements of virus protection.	
Custodian	Corporate IT dept.	
Approved by	Manish Jaiswal (Group CTO)	
Owner	Corporate IT dept.	

Distribution list

Name
To all locations of JMB group.

Version History

Version no.	**Version date**	**Approved by**	**Comments**	**Signature**
v1.0	28.08.2018	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	10.01.2019	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	08.02.2020	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	11.02.2021	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.1	25.03.2022	Manish Jaiswal (Group CTO)	Logo changes done in this policy	
v1.2	28.09.2023	Manish Jaiswal (Group CTO)	Changes done for acceptable AV signature is N-3	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Reviewed & no changes	

Contents

1. Purpose

1.1.The objective of this policy is to ensure that all relevant individuals understand the key elements of virus protection: why it is needed, how to keep the impact of malware to a minimum, how to protect the organization against attacks and how to ensure that virus infections can be addressed within the minimum timescale.

2. Scope

2.1.This antivirus policy is applied to all the computers on a network and safeguards from any malicious attacks This policy is met by all IT computers connected to JMBGRP's network to ensure effective virus prevention, detection, and correction.

3. Definitions

3.1.**Malware:** It refers to any type of software intentionally designed to cause damage to a computer, server, network, or device, or to gain unauthorized access to systems and steal sensitive information. Example: computer viruses, worms, trojan horses, rootkits, spyware, dishonest adware, crime ware and other malicious and unwanted software.

3.2.**Computer Virus:** A computer virus is a type of malicious software (malware) that is designed to replicate itself and spread from one computer to another it can attach itself to legitimate programs or files and infect them, causing the virus to spread when those programs or files are shared or executed. Computer viruses can be programmed to perform a variety of harmful actions, such as corrupting data, stealing personal information, disrupting system operations, or even rendering the infected computer unusable.

4. Policy Statement

4.1. Communication

4.1.1. Responsibilities for being alerted to the latest information and external bulletins relating to threats of viruses and for software update information must be formally allocated.

4.1.2. IT System and network administrators must be notified quickly of significant new malware- related risks (e.g., by e-mail). In certain extreme cases, end users and Third Parties may also need to be informed.

4.1.3. IT Service Providers and IT Infrastructure organizations must be prepared to respond quickly to such communications and be able to apply updates and fixes as necessary.

4.2. Software Installation

4.2.1. Software must be installed by authorized persons.

4.2.2. Only authorized and licensed software may be installed according to established changecontrol processes.

4.2.3. Where practicable, user workstations should be configured to prevent end users frominstalling software.

4.2.4. 'Non-Business' software must not be installed on company computers.

4.2.5. All programs received from outside sources must be checked for viruses before installationon PCs or servers.

4.3. Anti-Virus Software

4.3.1. This section applies to devices running Microsoft Windows. For all other operating systems, Group Information Security will determine the required level of anti-virus protection, considering the current level of threat, the vulnerability and the availability of anti-virus products.

4.3.2. Anti-virus software must be installed and active on all Servers and PCs, including those used for remote access. Only those Servers/PCs that would not operate properly if a/v software is installed and are not fully connected to the main company network may be exempt. Any such exemptions must be documented.

4.3.3. Anti-virus software should be set to scan boot sectors and memory on load-up and should be set to scan all executable files (including macro files in desktop software) and protected files (e.g., compressed or password-protected files).

4.3.4. All new Servers/PCs must be formatted / set-up using known 'clean' system / set-up disks.

4.3.5. For PCs, scan on create and write actions should be set permanently on. Periodic (e.g. weekly or monthly) scanning of all disks including hard disks and removable storage media (e.g. CDs, DVDs and USB storage devices) should be performed.

4.3.6. For servers, if scanning on read/write cannot be performed on a permanent basis due to performance or other reasons, scanning should be executed periodically.

4.3.7. External emails and attachments must be scanned for viruses prior to delivery into users' mailboxes. Internal emails should also be scanned if possible.

4.3.8. Vulnerable types of attachments (e.g. vbs) in emails may be blocked automatically, where considered practical.

4.3.9. Virus-checking software updates (DATS/pattern files) must be applied as soon as released by the software supplier, preferably by push technology. This will normally require checking for DAT/pattern file updates on a daily basis.

4.3.10. Anti-virus scan engines should be upgraded as required.

4.3.11. Anti-Virus protection software should be configured to:

4.3.11.1. Be active at all times;

4.3.11.2. Ensure that important settings cannot be disabled by the user;

4.3.11.3. Remove the malware and any associated files or reset system settings;

4.3.11.4. Quarantine files suspected to contain malware (e.g. for further investigation);

4.3.11.5. Provide a notification when suspected malware is identified (e.g. by producing anevent log entry and providing an alert).

4.4. **Protective Measures**

4.4.1. The following technical measures should be implemented where possible to reduce the possibility of malware being introduced:

4.4.1.1. Implement malware detection or protection systems to scan network traffic entering the corporate network.

4.4.1.2. Restrict the Web sites from which code can be downloaded by providing filtering of forbidden websites or categories.

4.4.1.3. Prevent the downloading of certain types of mobile code (e.g., those associated with knownvulnerabilities, such as unsigned ActiveX controls, Java Script and Browser Helper objects).

4.4.1.4. Configure Web browsers to block or prompt users before downloading any potentiallyunsafe content.

4.4.1.5. Allow only trusted mobile code to be downloaded (i.e., signed with a trusteddigital certificate).

4.4.1.6. Disable the Auto-Run option (for external media) in Windows.

4.4.1.7. Consider the security of computer software when procuring technical equipmentwith embedded operating systems. See Appendix 2 for further details.

4.5. Security Reviews

4.5.1. Regular checks of servers, desktop computers, laptop computers and hand-held computingdevices should be performed to ensure that:

4.5.1.1. Anti-virus software has been installed and is operating;

4.5.1.2. The configuration of anti-virus software is correct; and

4.5.1.3. Updates are applied within required timescale, signature / dat accepted as Ver. N-3.

5. Responsibilities

5.1. All Employees/users

5.1.1. Be alert to threats and avoid actions that could introduce viruses or other malware. See Appendix 1 for detailed guidance.

5.1.2. Ensure that anti-virus and personal firewall is installed on the PC and is active and up todate.

5.1.3. Report incidents or violations to the Service Desk / Help Desk.

5.2. Information Security Management

5.2.1. Produce and issue Information Security policies and procedures relating to malwareprotection.

5.2.2. Promote awareness of Information Security principles and policies among staff and thirdparties and provide advice and guidance on the implementation of policy.

6. References:

6.1. ISO 27001:2013 - 12.2.1; 12.4.1; 16.1.1; 16.1.2; 16.1.3; 16.1.6;

7. Appendix 1 – Advice for Users

7.1. How Do I Prevent a Virus?

1. **Check that anti-virus software and a firewall has been installed on your PC or system.** If the PC or system is not a company standard build the anti-virus software may need to be installed.
2. **Check that the anti-virus software on your PC is updated regularly (at least weekly).** If the Dat/signature file is more than two weeks out of date contact your Service Desk / Help Desk.
3. **Update anti-virus software on laptops used out of the office.** If your laptop is not connected to the company network for a long period it might not be updated. Try to connect to the network regularly or check to see if the system can receive updates from Internet. Contact your Service Desk / Help Desk for advice if necessary.
4. **Ensure that the anti-virus software and firewall on your PC is active.** Never switch the anti- virus software or firewall off.
5. **Do not remove or reconfigure anti-virus software.** If necessary, this should be done only by IT support staff.
6. **Check CDs, USB memory sticks, other portable devices and downloaded files for viruses before use.** Most Anti-virus products (e.g., McAfee, Trend) include facilities to scan folders and devices, typically via a right mouse click on the device or folder in Windows Explorer. Scan any media that you have used outside the company and files downloaded from the internet or from other networks.
   - **Do not allow personnel from other companies to use their storage media in company PCs for demonstration purposes without them being checked for viruses first.**
7. **Do not install unauthorized software.** Only authorized software should be used and this should only be installed by authorized administrators.
8. **Do not open or launch attachments contained in suspicious or untrusted e-mail messages.** The most likely source of viruses is attachments in unsolicited e-mails. Such e-mails are best deleted.
9. **Be careful opening MS Office documents received from external sources.** Viruses can be present in macros in Microsoft Office documents. If in any doubt, do not enable macros when prompted.
10. **Use of anti-virus software and a personal firewall at home is strongly recommended.** The home PC is even more vulnerable to malware than company PCs.

11. How can I recognize a computer virus?

Most viruses are detected by the network operations staff. Possible symptoms are:

- Very slow response by the PC;
- Unexpected or unusual responses;
- Unexpected messages displayed;
- Files or documents unexpectedly lost or corrupted.

12. What should I do if I suspect a computer virus?

- Stop whatever work you are doing on the PC and write down the symptoms that alerted you to the possible virus attack. Record any unfamiliar messages that appeared on the PC screen.
- Immediately notify the Service Desk / Help Desk. They are best placed to handle removal of the virus and protect other users in the company.
- Inform your line manager of the incident.
- Do not attempt to repair the virus yourself; follow the advice and instructions from the Service Desk / Help Desk.
- Do not forward virus warning emails from unknown external sources to other people – many such emails are hoaxes. The Service Desk will co-ordinate any required action.

8. Appendix 2 – Advice when Purchasing Technical Equipment with Built-In / Embedded Computer Software

8.1. When purchasing technical equipment, consider the following checks:

1. Is there existence of any kind of built-in/embedded computer system supplied within theequipment?
2. Who will be responsible for and who will perform computer hardware maintenance?
3. What type of installed operating system software?
4. Feasibility to keep operating system up-to-date according to the requirements of operatingsystem vendor?
5. Who will be responsible for and who will perform operating system maintenance?
6. What kind of application software is delivered?
7. Who will be responsible for and who will perform application software maintenance?
8. Does the supplier/vendor/manufacturer provide fixes for any disclosed or reported application software vulnerability?
9. Is application software web based, and if so:

a. Has application code been checked on absence of OWASP top10 vulnerabilities?

b. Can the supplier/vendor/manufacturer show results of a vulnerability test?

c. Is organization allowed to have a vulnerability test being performed and is the supplier/vendor/manufacturer willing to fix found vulnerabilities.