KAI !GARIB MUNICIPALITY

KAI !GARIB
MUNISIPALITEIT-MUNICIPALITY

ANTIVIRUS MANAGEMENT POLICY

Antivirus Management Policy
Approval and Version Control

Approval Process:	Position:	Date:
Recommended by CFO	J. KRAPOHL	29-06-2015
Recommended by IT Steering Committee	J. KRAPOHL	29-06-2015
Approved by Council		29-06-2015
Effective		
Review Frequency: One a year (i.e. Annually)		
Version Number		

KAI IGARIB
Munisipaliteit/Municipality
29 JUN 2015
REGISTRASIE
REGISTRY

TABLE OF CONTENTS

1. OVERVIEW

This Policy establishes certain requirements which must be met by all computers connected to the Kai !Garib Municipality network to provide the Kai !Garib Municipality with a trusted and secure network infrastructure to support the effective delivery of IT resources and mechanisms to help the organisation realise its goals and objectives in maintaining a secure IT environment. It attempts to set standards in terms of antivirus software management.

2. PURPOSE

The purpose of this policy is to:

- To create awareness across the municipality of the importance of installing antivirus software.
- To establish requirements which must be met by all computers connected to Kai !Garib Municipality network to ensure effective virus detection and prevention.
- To provide a secure network environment for Kai !Garib Municipality's automated applications, staff, business partners and contractors.
- To provide a resilient set of IT resources that maintains acceptable and agreed levels of confidentiality, integrity and availability.
- To ensure that all computer devices connected to the Kai !Garib Municipality network have proper virus-protection software with current virus-definition libraries.

3. SCOPE

This policy applies to all computers used on the Kai !Garib Municipality network. This includes, but is not limited to; staff and third party desktop and laptop computers, file/ftp/ proxy servers, and any computing equipment. Computers that are not physically connected to the Kai !Garib Municipality network must also abide by this policy.

4. DEFINITIONS

Vulnerabilities - weaknesses in software that can be exploited by an entity to gain elevated privileges is authorised to have on a computer or system. Not all vulnerabilities have related patches. These situations require workarounds to attempt to mitigate "un-patched" vulnerabilities.

Threats - A circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, data modification, and/or Denial of Service (DoS).

CERT - CERT is the Internet's official emergency team. CERT focuses on security breach and incidents, providing alerts and incident-handling and avoidance guidelines. CERT also conducts an on-going public awareness campaign and engages in research aimed at improving security systems.

5. POLICY

5.1. All Kai !Garib Municipality computers must have Kai !Garib Municipality's standard, supported antivirus software installed and scheduled to run updates on a daily basis.

5.2. The antivirus solution must come with sufficient licenses for all users and devices attached to the network. The licenses will be renewed annually and updates and patches shall be scheduled to run daily.

5.3. The antivirus software and the virus pattern files must be kept up-to-date.

5.4. Virus-infected computers must be removed from the network until they are verified as virus-free.

5.5. The IT Officer is responsible for creating procedures that ensure antivirus software is run on a daily basis and that computers are verified as virus-free.

5.6. Any activities with the intention to create and/or distribute malicious programs into Kai !Garib Municipality's networks (e.g., viruses, worms, Trojans, e-mail bombs, etc.) are prohibited, in accordance with the End User Security Policy and ICT Security Policy.

5.7. 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 IT Officer immediately via e-mail or by telephone. The user must report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material, or simply stating that you believe that a computer has an electronic viral infection.

5.8. No employee should attempt to destroy or remove a virus, or any evidence of that virus.

6. ANTIVIRUS SOFTWARE

6.1. Antivirus software installation and IT Officer Responsibilities

6.1.1. Antivirus software must be installed on all desktops, servers and laptops by the IT Officer. The antivirus software must be active at all times.

6.1.2. The IT Officer is responsible for maintaining and updating this Antivirus Management Policy. Copies of this policy will be posted on the internal web site and can be obtained from the IT Officer. Check the internal website on a regularly basis for updated information.

6.1.3. The IT Officer will keep the antivirus product up-to-date in terms of both virus definitions and software version in use.

6.1.4. The IT Officer will invest adequate efforts to identify clients who did not attempt to update their virus definitions file for more than 1 week and will take appropriate remedial actions.

6.1.5. The IT Officer will apply any updates that are required to defend against threats from viruses.

6.1.6. The IT Officer will take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the IT Officer may be required to disconnect a suspected computer from the network or disconnect an entire segment of the network.

6.2. Antivirus software monitoring and updates

6.2.1. New virus definitions should be automatically downloaded and the system should be configured to update on a daily basis on all client machines.

6.3. Review of antivirus logs

6.3.1. Antivirus logs/exception reports must be reviewed monthly by the IT Officer. (Refer to the Monthly Activity Monitoring Checklist, Appendix B, in the Activity Monitoring Policy and Procedure).

7. Best Practices for Virus Prevention

7.1. Always run the standard antivirus software provided by the municipality.

7.2. Never open files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.

7.3. Never open files or macros attached to an e-mail from a known source (even a co-worker) if you were not expecting a specific attachment from that source.

7.4. Be suspicious of e-mail messages containing links to unknown Websites. 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.

7.5. The municipality's email system scans all attachments for virus infections and blocks any trapped virus from being transmitted to client systems.

7.6. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.

7.7. Avoid direct disk sharing with read/write access. Always scan any removable media for viruses before using it.

7.8. Regularly update virus protection on personally-owned computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.

8. End User Responsibilities

8.1. Users must ensure that all computers have virus protection that is in keeping with the standards set out in this policy.

8.2. Users departments that allow employees to use personally-owned computers for business purposes, if applicable, must implement virus protection processes and procedures that are in keeping with the standards set out in this policy.

8.3. All employees are responsible for taking reasonable measures to protect against virus infection.

8.4. Employees must not attempt to either alter or disable antivirus software installed on any computer attached to the municipal network without the express consent of the IT Officer.

9. Enforcement

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