Controls against Malware Policy

Vishwakarma University

Internal

Title: Control Against Malware Policy	**Doc No.:**
Approval Date: 18-07-2020	**Review:** Annual
Effective Date: 19-07-2020	**Department:** System and Technology

Ver. No	Release Date	owner	Approved By	Change details
1.0	19-07-2020	CISO	Vice Chancellor	Initial

Table of Contents

1. Purpose

This document describes the measures taken by the VU to counter computer viruses and identifies the responsibilities of individuals. Information security department will be ensuring the security of the VU against viruses and other vulnerabilities. This policy applies to all devices connected to the VU's network.

2. Scope

Computing platforms (including but not limited to: desktop workstations, laptops, hand-held, personal digital assistants, servers and network devices) are integral elements in the operations of the VU and as such are vital to the VU mission.

This policy will help ensure that all vulnerable computing platforms on premises are guarded against vulnerabilities and protected by antivirus software at all times.

3. Objectives

The principal concern of this computer virus protection policy is effective and efficient prevention of all network virus outbreaks and network security attacks involving all computers associated with VU. The primary focus is to ensure that VU-affiliated users (Staff) are aware of and take responsibility for the proper use of the VU provided and Technology and Network Services-supported virus protection software.

This policy is intended to ensure the integrity, reliability, and good performance of VU's computing resources; that the resource-user community operates according to a minimum of safe computing practices; that the VU's licensed Antivirus virus software is used for its intended purposes; and that appropriate measures are in place to reasonably assure that this policy is honored.

4. Policy Statement

- Any computer, server or network devices connected to the VU's network shall be protected by antivirus software from malicious electronic intrusion.
- All computers or networked devices shall have applicable operating system and application security patches and updates installed prior to initial connection to the network.
- A policy shall be established for prohibiting the use of unauthorized software.
- A formal policy shall be prepared to protect against risks associated with obtaining files and software either from or via external networks or on any other medium, indicating what protective measures should be taken.
- In case of requirement to connect Personal devices to VU network, Device shall have antivirus software installed and configured as per the "BYOD policy" for effective operation prior to their connection to the premises network.
- Logs of scan shall be periodically reviewed.
- Reducing vulnerabilities that shall prove to be exploited by malware,
- Conducting regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorized amendments shall be formally investigated by the VU.
- All the files shall be scanned that are received over networks or via any form of storage medium, for malware before use.
- All files shall be scanned, received in form of electronic mail attachments and downloads for malware before use.
- Web pages shall be scanned for malware.

- Procedures and responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks shall be established.
- Websites and newsletters that provide details regarding to new malware would be subscribed by the VU.
- Isolating environments where disastrous impacts may result.
- A business continuity plan shall be prepared for the recovery from any sort of malware attack. This includes all data and software backups.
- Implementation of procedures shall be verified relating to malware information, and ensuring that the warning bulletins are accurate and informative.

5. Enforcement

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

6. Reference Document

- Business Continuity Plan
- Technical Vulnerability Management Policy
- BYOD policy
- HR IT policy

7. Distribution List

The following users have access to this policy:

- All staff of Vishwakarma University

8. Acronyms

- VU**:** here it refers to Vishwakarma University.
- BYOD Policy: Bring your own device policy
- Malware: malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems