Anti-Malware Policy

Version 2.0

15/05/2021

Document Ownership – Threat Intelligence and Vulnerability Management Team

genpact

Transformation Happens Here

NOTICE

The information contained in this document is not to be used for any purpose other than the purposes for which this document is furnished by Genpact, nor is this document (in whole or in part) to be reproduced or disclosed to other Genpact employees without a need to know, or to any third party or made public without the prior express written permission of Genpact.

Version Control

Version No.	Version Date	Type of Changes	Author	Approver	Date of next Review
1.0	03/03/2020	New Release	Shailender	Rohit Kohli	02/03/2021
2.0	15/05/2021	Added new Anti-Malware capability	Shailender	Rohit Kohli	14/05/2022

Contents

1 Introduction

Viruses and malware are a threat to the confidentiality, integrity and availability of information and can prove to be harmful to Genpact. An attack by virus or malware could result in data loss, privacy breaches, delay in delivery due to system unavailability, revenue and/ or reputation. Detection, prevention and recovery controls to protect against malware & viruses shall be implemented along with appropriate user awareness.

2 Objective

The objective of this policy is to protect Genpact information systems from potential threats from viruses and malware.

3 Scope and Applicability

All Information systems, including end user system and server shall be covered under the scope of this policy.

4 Anti-Malware Solution

- An Anti-Malware solution shall be deployed on the information system considering the risks to Genpact environment
- Anti-Malware solution shall have at minimum, but not limited to, below mentioned functionalities:
  - Perform real time analysis of all the files being processed or accessed.
  - Perform real time detection and prevention of malware.
  - Provide malware and malicious activity detection and response capability with historical data/event search.
  - Delete or quarantine all malwares, spywares, viruses etc. from the system without causing any system performance degradation; and
- Anti-Malware solution shall be evaluated and approved by Information Security Team
- Identified personnel in the team shall be assigned with responsibilities to manage the Anti-Malware solution
- Notifications shall be enabled and be sent to CDC on detection of any viruses, malware or malicious code
- Users shall not try to modify or in any way tamper with the anti-malware settings in any system
- In the event of virus outbreak, the SecOps/CDC reserves the right to temporarily contain the infected machine or remove it to safeguard other machines on the network
- Anti-malware solution shall always be automatically enabled when the system is in use with the exception to troubleshoot problem diagnosis
- Exception to stop operating anti-malware solution under any circumstances must be authorised by the head of the InfoSec or The Risk Management Committee

5 Policy Non-Compliance

Failure to comply with the Anti-Malware Policy shall result in appropriate disciplinary actions as per CAP policy.

6 Policy Exception

Any deviation to this Policy shall be treated as per the Genpact Infosec Exception Management Process.

7 Annexure

7.1 Document Reference List

Please refer to the ISMS Master List of Documents.

7.2 Abbreviations and Definitions

Please refer this Link.