Threat and Vulnerability Management Policy

Version 2.0

15/05/2021

Document Ownership – Threat Intelligence and Vulnerability Management Team

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	Initial Release	Shailender	Rohit Kohli	02/03/2021
2.0	15/05/2021	Annual Review-No Change	Shailender	Rohit Kohli	14/05/2022

Contents

1 Introduction

Threat and Vulnerability Management is the practice of identifying, assessing, classifying, remediating, and mitigating security weaknesses. A vulnerability assessment exercise helps to identify and categorize vulnerabilities, whereas penetration testing allows for exploitation of vulnerabilities identified by assessors.

2 Objective

The objective of Threat and Vulnerability Management Policy is to provide guidance for conducting vulnerability assessment and penetration testing on identified systems; thereby pro-actively discovering the extent to which the security of information systems is threatened by attacks. This shall also address the vulnerabilities before they can be exploited to compromise Genpact resources.

3 Scope and Applicability

Threat and Vulnerability Management Policy shall be applicable to all Genpact Information Systems.

4 Vulnerability Assessment and Penetration Testing

Vulnerability assessment and penetration testing are two complimentary proactive approaches to assess the security posture of information systems. The Vulnerability Assessment shall be conducted to test the security posture of the information systems both internally and externally. Penetration Testing (PT) is the process to run exploits on the known vulnerabilities with the purpose to gain additional information or access on the targeted systems.

4.1 Vulnerability Assessment

- Genpact shall identify, prioritise, and categorise the Information Systems to plan and conduct vulnerability assessment on a periodic basis
- Application assessment shall be performed on a need basis or as per business requirement
- Prior to conducting the VA, relevant stakeholders shall be informed
- Vulnerability scanning shall be performed by using a tool-based vulnerability scanner
- Reports shall be extracted from the vulnerability scanning tool which shall include details relevant to vulnerabilities identified including the recommendations
- The report shall be validated to eliminate the false positives from the remediation process
- The remediation actions shall be discussed and agreed with the designated stakeholders who shall be responsible for mitigating the risks
- Post remediation, report shall be published to the relevant stakeholders and closure shall be tracked

4.2 Penetration Testing

- Penetration testing shall be performed prior to exposing Genpact or client application, API, or infrastructure services on the internet
- Genpact shall identify, prioritise, and categorise the Information Systems to plan and conduct penetration testing on a periodic basis

- The relevant stake holders shall be informed, and approval shall be taken before conducting penetration testing to avoid any unplanned business downtime
- Relevant information shall be gathered from trusted internal sources as applicable for white box and black box testing
- Probable impact of exploiting a vulnerability shall be assessed to avoid any unplanned outages
- Identified vulnerabilities shall be exploited to the extent where no damage/data leak is caused, however a PoC shall be established
- The report of penetration testing shall be published to the relevant stakeholders and action plan on remediations shall be discussed

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.