|  |
| --- |
| **Internal Vulnerability Assessment Report** |
| |  |  |  | | --- | --- | --- | | **Report Created By** |  | **Report Created For** | | Genpact Information Security Team |  | MHE Hyderabad PCI DSS Certification | |  |  |  | |
|  |

|  |  |  |
| --- | --- | --- |
| Testing details | Tester name and qualification details | Report date |
| Vulnerability Assessment | Threat & Vulnerability Management Team | Jan’2021 |

|  |  |
| --- | --- |
| Scan Started: | Ongoing |
| Report Release Date: | Jan’2021 |
| Retest Report Release Date: | NA |
| Credentials: | NA |
| IP Addresses |  |
| Total Hosts Scanned: | All |

|  |
| --- |
| Conclusion |
| Genpact has determined that Genpact’s internal network under scope is COMPLIANT with Genpact validation requirements. |

### ANALYSIS RESULTS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Note: The VA Analysis results cover scans for all in-scope devices. Also, the analysis has been filtered to only show vulnerabilities with ‘High’ rating. Please note exception details for high vulnerabilities open for 30 days & above.  Servers  All the server related identified vulnerability are remediated.  To address false positive vulnerabilities attached is the evidence under Internal Vulnerability Assessment section below.  Network  To address all the iOS related network device vulnerabilities DD team recommended the iOS upgrade, for which network team take a risk acceptance against risk id R160120\_101904. | | | | |
|  |  |  |  |  |
| As per the analysis, Vulnerabilities highlighted were closed by installing the relevant patches. False positive vulnerabilities & Business justification evidence also attached. |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Conclusion

Vulnerability detected in earlier quarter are not showing in subsequent quarterly scans i.e. Vulnerabilities identified in last quarter are not repeated in current quarter, also we have closed all the HIGH / Critical vulnerability observed in last quarter scan. After closure of all high vulnerabilities or taking risk acceptance, the report is now **compliant**.

|  |
| --- |
| Tester’s Note |
| Assessor observed that vulnerabilities identified during the scan as High, Medium, and Low were patched in a timely manner and found that overall VA report to be Compliant as per the PCI DSS requirement. |