# Intel Payment Card Industry (PCI) Addendum

## Supplier PCI Compliance Acknowledgement

This Appendix applies in addition to the Intel Information Security Addendum If the Supplier (or subcontractors) is/are involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. It also applies if the Supplier (or subcontractors) store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

As one of the suppliers identified as having now or in the future (either directly or through its subcontractors) access to, handling and/or system interaction with payment card relevant systems on behalf of Intel Corporation, we would appreciate if you could confirm your' and your subcontractors' current compliance relating to payment type security requirements, such as the Payment Card Industry Data Security Standard (PCI DSS 3.2. (or current standard as applicable) ) through this written acknowledgement.

The PCI DSS 3.2 (or current standard as applicable) compliance clause below is hereby included and made part of any Master Service Agreement and/or relevant Statements of Work.

## PCI Compliance.

a. PCI Compliance. Supplier acknowledges that it has read the requirements of PCI DSS 3.2 (or current standard as applicable) and is required to be PCI DSS 3.2 (or current standard as applicable) compliant according to the standard, and/or to provide Intel with quarterly updates on its PCI DSS compliance status until it is achieved and annually thereafter. Supplier further agrees to maintain compliance with PCI DSS 3.2 (or current standard as applicable) and to continue to adhere to those terms and conditions required of an entity with access to cardholder data, as described in PCI DSS 3.2 (or current standard as applicable) .
b. Supplier acknowledges and agrees to be responsible for the security of cardholder data in its possession. Supplier further maintains it shall monitor and be responsible for the PCI DSS 3.2 (or current standard as applicable) compliance of any/all sub-contractors for the contracted service.
c. Supplier further agrees that such data will only be used for assisting the parties in completing a transaction, supporting a loyalty program, providing fraud control services, client support, or for uses specifically required by applicable law.
d. Supplier further agrees that in the event of a major disruption, disaster, or failure - the Supplier has an appropriate Business Continuity and Disaster Recovery plan (BCDR), and will maintain continuity of its services.
e. Supplier shall immediately notify Company (Intel Corporation) in the event of any breach. Supplier further ensures that an Intel PCI DSS representative, or a PCI DSS approved third party will be provided access and full cooperation to conduct a thorough security review after a security

intrusion. Any security review will be used solely for the purpose of confirming Supplier's compliance with PCI DSS 3.2 (or current standard as applicable)

f. The complete PCI DSS 3.2 (or current standard as applicable) shall be incorporated by reference in this agreement (including all its requirements and sub requirements) unless specifically described below.

g. Right to Audit. Included in Intel's Master Service Agreement and language that allows Intel's right to audit.

As referenced, please find below the minimum groupings expected for your PCI DSS compliance requirements.

| **Requirements** |
| --- |
| All PCI DSS requirements must be adopted and maintained throughout the terms of the services agreement.<br><br>[Reference https://www.pcisecuritystandards.org/document_library for the latest version of PCI DSS Requirements, and a listing of All PCI Requirements the partner must meet based on services provided] |