

Information Security Addendum

Hum has established and agrees to maintain a written information security and privacy program (the "*Information Security Program*") designed to comply with this Information Security Addendum and applicable law. Terms not defined herein have the meaning set forth in the DPA.

As part of its program, Hum has implemented and agrees to maintain administrative, technical, and physical security safeguards designed to protect the confidentiality, integrity, and availability of Personal Data, including but not limited to:

- **Administrative and Organizational Safeguards**

- o Hum maintains policies and procedures for the security of Personal Data, including the following:
 - Written information security policies that set forth Hum's procedures with regard to maintaining the safeguards set forth in this Information Security Addendum.
 - Incident Response Plan, which sets forth Hum's procedures to investigate, mitigate, remediate, and otherwise respond to security incidents.
- o Hum conducts regular assessments of the risks and vulnerabilities to the confidentiality and security of Personal Data.
- o Hum regularly tests and monitors the effectiveness of its Information Security Program, including through security audits, and will evaluate its Information Security Program and information security safeguards in light of the results of the testing and monitoring and any material changes to its operations or business arrangements.
- o Hum has appointed a VP-level individual to oversee and manage its Information Security Program and has designated an Incident Response Team to address any Personal Data Breach.
- o Hum maintains role-based access restrictions for its systems, including restricting access to only those Hum employees that require access to perform the Hum Services or to facilitate the performance of such Hum Services, such as system administrators, consistent with the concepts of least privilege, need-to-know, and separation of duties.
- o Hum periodically reviews its access lists to ensure that access privileges have been appropriately provisioned and regularly reviews and terminates access privileges for Hum employees that no longer need such access.
- o Hum assigns unique usernames to authorized Hum employees and requires that Hum employees' passwords satisfy minimum length and complexity requirements and be changed periodically.
- o Hum regularly provides training to employees, as relevant for their roles, on confidentiality and security.
- o Hum requires relevant Hum employees to acknowledge Hum's Information Security Program annually.
- o Hum has a policy in place to address violations of its Information Security Program.

- **Technical Security**

- o Hum logs system activity—including authentication events, changes in authorization and access controls, and other system activities—and regularly reviews and audits such logs.
- o Hum maintains network security measures, including but not limited to firewalls, to segregate its internal networks from the internet, risk-based network segmentation, intrusion prevention or detection systems to alert Supplier to suspicious network activity, and anti-virus and malware protection software.
- o Hum has implemented workstation protection policies for its systems, including automatic logoff after a period of inactivity and locking the system after a defined number of incorrect authentication attempts.
- o Hum requires multi-factor authentication on its systems for administrative users.
- o Hum conducts periodic vulnerability scans and assessments on all systems storing, processing, or transmitting Personal Data to identify potential vulnerabilities and risks to Personal Data.

- o Hum remediates identified vulnerabilities in a risk-prioritized and timely manner, including timely implementation of all high-risk mitigating manufacturer- and developer-recommended security updates and patches to systems and software storing, transmitting, or otherwise Processing Personal Data.
- Physical Security
 - o Hum restricts access to its facilities, equipment, and devices to Hum employees with authorized access on a need-to-know basis.
 - o Hum tracks the location of its equipment, devices, and electronic media and maintains a record of such locations.