**Software Security Rider**

 VENDOR acknowledges and agrees to the following terms for any acquisition of software (to include trials, freeware, etc.) that is installed or run on an Electronic Asset connected to UTLIITIES’ network. “Electronic Assets” are further defined as endpoints to include, but not limited to laptops, servers, desktops, mobile devices, networking / infrastructure devices that are connected to UTILITIES’ internal network behind UTILITIES’ firewall. These terms are applicable to acquisitions of goods and services which are not primarily software in nature, but also include a software component. These terms are not applicable to Software-as-a-Service (SaaS) offerings unless the solution includes a locally installed component.

**A. Terms**

**1. Transmission of Data**

* VENDOR acknowledges and agrees that their software does not transmit UTLITIES’ data to a location outside UTILITIES’ network to include, but not limited to, synchronization of data to third parties (e.g. Box, AWS, etc.). Synchronization of data is permitted only if VENDOR has agreed to UTILITIES’ Data Security Rider in addition to this Software Security Rider.
* VENDOR’s software may be installed / used on Electronic Assets if both of the following conditions are met:

a) The functionality to transmit UTILITIES data to a location outside UTILITIES’ network has been disabled.

b) No UTILITIES’ data is transmitted outside UTILITIES’ network as a result of the installation of the software.

* VENDOR may collect aggregate technical data regarding the software, it’s usage, and environment provided that such information does not include any data that could potentially identify a specific individual (e.g. username, ID, etc.) or attributable information from the resident host (e.g. hostname, private IP address, etc.) UTILITES reserves the right to filter / block this communication and expects VENDOR’s software to function without it.

**2. Vulnerability Management**

* VENDOR acknowledges and agrees that any software provided to UTILTIES is, to the best of their knowledge, free from known material defects or weaknesses that exposes the software or resident system / network to a threat (collectively, a “Vulnerability”) at the time of UTILITIES acquisition and will be subject to ongoing Vulnerability detection mechanisms which may interfere with the operation of the software.
* If the installation of VENDOR’s software introduces material Vulnerabilities which cannot be reasonably mitigated to an acceptable level or remediated, VENDOR’s software will be removed from all Electronic Assets. UTILITIES reserves the right to determine in its reasonable opinion whether the mitigation/remediation is acceptable.
* In the case where material Vulnerabilities introduced due to the installation of VENDOR’s software cannot be reasonably mitigated to an acceptable level or remediated, VENDOR agrees to refund the cost(s) paid by UTILITIES for VENDOR’s solution equivalent to the time period remaining for the software license(s) purchased and the value of purchased products if the removal of the software renders such products inoperable or significantly degraded.

**3. Software Updates**

* VENDOR acknowledges and agrees that their software does not automatically download and install updates.
* VENDOR software may be installed / used on Electronic Assets if one of the following conditions are true:

a) Automatic updates are integral to the core functionality of the software. Examples include software packages that rely on real-time updates (e.g. anti-virus programs) to provide the value of the software. UTILITIES reserves the right to determine in its reasonable opinion whether or not automatic updates are integral to the core functionality of the software.

b) Automatic updates can be disabled such that user intervention is required to manually apply updates.

* All software updates must use reasonable measures to ensure the integrity of software updates to include both:

a) verification of the identity of the server providing the update (e.g. using cryptography for non-repudiation).

b) verification of the integrity / validity of the update (e.g. using file hashes / digital signatures).