**Data Security Rider**

CONTRACTOR acknowledges and agrees that data and information to be provided to CONTRACTOR or otherwise received, stored, processed, hosted, managed, or used by CONTRACTOR during performance of this Agreement is categorized as Confidential Information under this Agreement or by laws and regulations, or otherwise is Sensitive data requiring protection from intrusion, release, breach or other exposure. The following requirements apply to applications (including Cloud applications and subscriptions, Hosted/Managed services, and web sites/interfaces) used by UTILITIES and all devices and infrastructure to be connected to the UTILITIES network or that otherwise document, contain, or process UTILITIES’ information on the UTILITIES’ network or accessed through other means:

1. **Standards**
2. Login Credentials/Passwords

CONTRACTOR agrees to align all credentials (passwords) with the minimum complexity requirements as outlined in UTILITIES’ Cyber Security Policy [and shown below]. If supported, CONTRACTOR agrees to utilize UTILITIES’ approved single sign-on capabilities when technically feasible.

Minimum credential (password) complexity requirements for all account types:

* 1. Be a minimum of 10 characters in length.
	2. Not include dictionary words (spelled forward or backward) or easily guessed sequences of characters (e.g., abcdef, QWERTY, q1w2e3, etc.).
	3. Contain at least 1 lower case letter, 1 upper case letter, and 1 number (e.g. 0-9).
	4. Not include any names (e.g., system usernames, family names), addresses, birthdays, or any other easily identifiable personal information.
	5. Passwords for all account types **must** be set to expire every six (6) months. If technological means do not exist / cannot be used to enforce a password change, the password must be manually changed every six (6) months regardless.
	6. New passwords for all account types **must** be different than the last 24 passwords used.
	7. A newly changed password will be active for at least 1 day before a change is allowed.
1. Data/Information Classification and Protection

Encryption of data and information designated or described in Agreement as Confidential or Sensitive or otherwise subject to information protection.

* 1. CONTRACTOR agrees to apply industry standard encryption protocols to encrypt UTILITIES’ data while at rest and in transit. The encryption method employed to satisfy the ‘at rest’ requirement must be sufficient to protect against unauthorized access/use of the data while the system storing/processing the information is in use (e.g. field encryption). Encryption methods designed to render unmounted/inactive data unreadable to unauthorized parties (e.g. full-disk encryption) will only satisfy the ‘at rest’ requirement for stored/offline backups.
	2. CONTRACTOR agrees to immediately disable and discontinue use of any encryption protocol, cipher, algorithm, or other method that is listed or described in any security monitoring organization’s list as compromised or suspected to have been compromised [*e.g.,* lists maintained by NCCIC, US-CERT, etc.].
	3. CONTRACTOR agrees to disable all encryption protocols, algorithms, cipher suites, or security configurations that do not meet UTILITIES’ minimum encryption and configuration requirements.
	4. CONTRACTOR agrees to protect encryption keys and all backups of UTILITIES’ data at a level equal to or exceeding the encryption level of the data being encrypted. Encryption keys shall not be stored in the same location as the data.
	5. CONTRACTOR agrees to provide UTILITIES with the encryption keys or a key escrow for all UTILITIES’ data.
	6. CONTRACTOR agrees to only use methods meeting or exceeding UTILITIES’ minimum encryption and configuration requirements (shown below):

(a) TLS version 1.2 for all SSL/TLS-based sessions

(b) AES 128 for all symmetric encryption

(c) 2048-bit keys for all asymmetric encryption

(d) IKEv2 and PFS for all IPsec VPN tunnels.

(e) X.509 standards, SHA-2 hashing, and an approved independent authority as issuer for all certificates.

1. Location of data
	1. CONTRACTOR agrees that UTILITIES’ data must remain within the continental United States at all times. CONTRACTOR may alter the specified location within the U.S. of UTILITIES’ data with ninety (90) day advance written notice to UTILITIES. Primary / alternate data centers must be geographically separated.
2. **Audits and Cyber Security Testing**
3. UTILITIES has the right to audit and/or test applications and devices delivered hereunder prior to acceptance and periodically thereafter during performance of this Agreement.
4. CONTRACTOR agrees to undergo such acceptance and periodic security audits by certified third parties occurring at least annually. Any identified issues must be resolved within ninety (90) days of the date of the audit report. UTILITIES may request, and CONTRACTOR shall provide, a copy of the results of this audit at any time during the performance of this Agreement. The initial acceptance audit requirement may be satisfied by providing a SSAE 16 or 18 or SOC 2 Type 2 report or equivalent, and such report shall also be provided to UTILITIES annually. CONTRACTOR also agrees to provide a SOC 1 Type 2 report annually.
5. In addition to audits, CONTRACTOR agrees to allow security testing and to provide valid (non-administrative) credentials, if applicable, for use during security testing. Security testing will consist of vulnerability and/or web application scans and / or manual testing conducted by UTILITIES’ cybersecurity personnel and identified issues will be communicated to CONTRACTOR for remediation or mitigation. Security testing will not consist of ‘penetration tests’ involving exploitation beyond the extent necessary to prove the presence of the identified vulnerability / security misconfiguration. UTILITIES reserves the right to determine if the remediation or mitigation measures are acceptable.
6. In addition to remediating or mitigating issues prior to acceptance, CONTRACTOR will also be responsible for remediating or mitigating any vulnerabilities or configuration issues identified through subsequent security tests conducted in accordance with this Agreement. CONTRACTOR will have fifteen (15) days from the date of testing to remediate critical vulnerabilities or issues identified as such by UTILITIES, and sixty (60) days from the date a vulnerability or configuration issue is identified to remediate/mitigate other vulnerabilities or configuration issues identified through security testing. UTILITIES reserves the right to determine if the remediation or mitigation measures are acceptable.
7. **Security-related Patches and Maintenance**

As soon as reasonably possible after they are tested and determined to be safe for installation, but not to exceed 30 days from issuance, CONTRACTOR agrees to apply patches to systems/solutions that comprise the service(s) that they provide and systems/solutions they manage on behalf of UTILITIES for “critical” software / firmware vulnerabilities that are revealed and addressed by a supported patch. CONTRACTOR will categorize the urgency of application as either “critical” or “non-critical” in nature based on industry recommendations and applicability to their product / solution. Application of “non-critical” patches, including service packs, will be implemented according to CONTRACTOR’s business standards.

1. **Breaches**

CONTRACTOR agrees to, provide Notice to UTILITIES of any access, acquisition, use, or disclosure of UTILITIES’ data in a manner which compromises the security or privacy of the data (“breach”), within forty-eight (48) hours of discovery. Notice shall be made to both UTILITIES’ Representative in the manner provided for legal Notices under this Agreement, and by email to UTILITIES Cyber Security Team.

In its initial Notice and when more information becomes available, CONTRACTOR shall state to the extent known:

(a) the details of the event that caused the breach,

(b) whether the breach involved exposure, scanning, exfiltration, destruction or modification, or other misuse/misappropriation of the data,

(c) the amount and nature of the data involved in the breach,

(d) the persons/parties who gained access to the data, to the extent known (subject to an ongoing duty of disclosure as information is developed), and

(e) the CONTRACTOR’s plan to mitigate the cause of the breach.

1. **Destruction of Data / Records / Information**

CONTRACTOR agrees to sanitize all media containing UTILITIES’ data / information in accordance with NIST SP 800-88 media sanitization guidelines [media containing UTILITIES’ Sensitive data must be sanitized by ‘Clearing’ at a minimum; media containing UTILITIES’ Confidential data must be sanitized by ‘Purging’ at a minimum] and any UTILITIES’ Records retention requirement to include exemptions for legal holds.

Upon termination, cancellation, expiration, or other conclusion of the Agreement or upon expiration of the specified retention period of any applicable laws, regulatory requirements, or retention schedules, CONTRACTOR agrees to return all UTILITIES’ data and any other information in CONTRACTOR’s custody provided to enable performance of this Agreement (such as infrastructure or context diagrams, project plans, etc.) or sanitize the media [see requirements above] containing the data / information based upon UTILITIES’ preference. Promptly after completion, CONTRACTOR agrees to provide UTILITIES with a certificate confirming the date and method of destruction of the data.

1. **Data Storage, Replication and Backup**

CONTRACTOR shall backup all UTILITIES’ data from the production server for data recover purposes. In addition, CONTRACTOR shall also backup all UTILITIES’ data to a separate geographically isolated location for disaster recovery purposes. UTILITIES’s data shall be stored for a minimum of thirty (30) days at the production facility and at the disaster recovery facility for a minimum of ninety (90) days. Upon UTILITIES’ request, CONTRACTOR shall make available to UTILITIES a copy of UTILTITIES’ data with twenty-four (24) hour advance written notification.

CONTRACTOR shall ensure that UTILTIES’ data accessed by or disclosed to CONTRACTOR is stored, processed, or maintained only to the extent required for the performance of CONTRACTOR support services under this Agreement. CONTRACTOR shall ensure that UTILITIES’ data is not replicated or stored on any unencrypted removable / portable storage devices.