AFFIDAVIT OF COMPLIANCE

I HEREBY AFFIRM that I, [name] _____, am the [title] _____, and the duly authorized representative of [name of business] _____. I am over 18 years of age, of sound mind, capable of making this affidavit, personally acquainted with the facts stated in it, and I possess the legal authority to make this Affidavit on behalf of myself and the business for which I am acting.

I ACKNOWLEDGE that, in accordance with the Fair and Accurate Credit Transactions Act (FACTA), the City of Austin is required to ensure that the activities of service providers who provide the City services related to covered accounts under FACTA are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

I FURTHER AFFIRM that the aforementioned entity has in place reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

Signed this the ____ day of _____, 20__.

_____
Signature of Affiant

BEFORE ME, the undersigned authority, personally appeared _____, who being by me duly sworn, stated that the contents of this affidavit are true and correct.

SWORN TO AND SUBSCRIBED before me on the ____ day of _____, 20__.

_____
Notary Public in and for the State of Texas

My commission expires: _____

Austin Energy Data Handling Controls	
Rev. No.: 2.0	Date: October 5, 2018
Owner: Enterprise Information Security	Category: Information Security
Author: Michael Goin	SME: Mike Goin, AE Risk Management, AE Legal
	Doc Type: Contract Exhibit

CONTENTS

1. DATA HANDLING CONTROLS: SECURITY DIRECTIVES AND REQUIREMENTS

1.1. Contractor Responsibilities regarding treatment of City Data

1.1.1. The City requires that controls ("Data Handling Controls" or "DHC") be in place to manage risk to the confidentiality, integrity and availability of City Confidential Information in any form in the care, custody or control of Contractor. These Data Handling Controls represent a minimum standard for protection. Additional controls required under applicable laws, regulations, or standards governing specific forms of data (e.g., health information, credit cardholder data) may also apply.

1.1.2. Contractor agrees to comply with these Data Handling Controls in performing the Services (including information technology-based Services) and in providing the Deliverables under the Contract. Contractor accepts all responsibility and liability for the security, integrity and protection of all City Data in its custody or control, including but not limited to when City Data is received, transmitted, processed, stored, backed up, archived, returned, or as occurs otherwise during performance of Services, including that involving a subcontractor. Contractor agrees that any damages or liability arising from any violation of these Data Handling Controls, including damage to City Data as well as all work to restore City Data and its integrity, are Contractor's responsibility. Contractor agrees that compliance with these Data Handling Controls is not an affirmative defense to any losses, disclosures, corruption or other damage to City Data which may occur for which Contractor is responsible, as Contactor acknowledges and agrees that there may be situations for which the Data Handling Controls may be inadequate to reasonably protect City Data as a project matures during the term of the Contract, and Contractor agrees to use appropriate additional measures in its reasonable judgment to protect City Data in such situations.

1.2. Location Parameters

1.2.1. The authorized geographical data center region for the storage and processing of City Data under this Contract is the contiguous United States.

1.2.2. Contractor may utilize non-US based personnel but must ensure that City Confidential Information cannot be stored, viewed, downloaded, or transported outside the contiguous United States.

1.3. Specific Security Directives

1.3.1. For access to City Data, Contractor must ensure that only the minimum amount of rights is granted to an Authorized Person as required to perform Contractor's contractual duties.

1.3.2. Unless otherwise approved by the City in advance, in writing, Contractor must encrypt all City Confidential Information. Only an Authorized Person within the Secure Service Area may view unencrypted City Confidential Information.

1.3.2.1. Contractor employees and subcontractors who have provided written certification showing they meet the minimum requirements of these Data Handling Controls are allowed to view unencrypted City Confidential Information if necessary to provide the Services.

1.3.2.2. The Secure Service Area shall be designed in such a way as to prohibit the unauthorized viewing, modification, or destruction of any unencrypted City Confidential Information (including any image). Contractor may not remove City Confidential Information from the Secure Service Area unless approved by the City in advance in writing.

1.3.3. Unencrypted City Confidential Information may not be stored on any Contractor or subcontractor Endpoint Device.

1.3.4. Contractor must have in place its own internal security program that includes policies using applicable industry best practices. Contractor will provide documentation of these policies and procedures within ten business days of written request by the City.

1.3.5. Contractor must detach all removable storage media containing City Confidential Information from any device when not in use and store the media in Contractor's physically-secure location.

1.3.6. Contractor must ensure that only an Authorized Person may access devices containing City Data.

1.4. Data Disposition

1.4.1. Contractor agrees to return all City Data obtained under this Contract (including this DHC) or otherwise in its care, custody or control to the originating City department, and to delete any remaining copies from Contractor's storage/production/use/possession at the end of the engagement, including:

1.4.1.1. as stated in any scope of work and/or

1.4.1.2. at City's request, or upon

1.4.1.3. Contractor's failure to follow the compliance directives of this Data Handling Controls document.

1.5. General Compliance Requirements

1.5.1 Contractor's failure to comply with any provision of these Data Handling Controls is a material default under the Contract.

1.5.2 Contractor agrees that City or its authorized representatives may audit or review Contractor's compliance with these Data Handling Controls under Contract Section 0300, Paragraph 17, Audits and Records. Except in an emergency (including a Breach or Security Incident), such audit or review shall be conducted only during normal business hours and without disrupting normal business practice, and City shall provide reasonable advance notice of exercising its right of audit or review.

Audits or reviews may include, but are not limited to:

- system, security, application, operating system, and database logs;

- physical access logs at all data centers;

- data center location or ownership changes;

- access control procedures;

- procedures for the physical and digital destruction of media;

- environment changes that have the potential for outages;

- workplace inspections for compliance with these Data Handling Controls and review of any Vendor supplied documentation submitted to document/demonstrate compliance; and

- procedures for and evidence of routine testing and updating of systems to prevent against attacks.

1.6. Logging/Auditing Requirements

1.6.1. Contractor must create system, security, application, operating system, and database logs:

1.6.1.1. when Contractor creates, reads, updates, or deletes City Data;

1.6.1.2. when Contractor initiates a network connection;

1.6.1.3. when Contractor accepts a network connection;

1.6.1.4. at user authentication and authorization, including failed access attempts;

1.6.1.5. for user login and logout;

1.6.1.6. when Contractor grants, modifies, or revokes access rights, privilege levels, and permissions, firewall rules, and user passwords;

1.6.1.7. when Contractor makes any system, network, or services configuration changes, including installation of software patches and updates, other installed software changes, operating system and Hypervisor activity;

1.6.1.8. at application process startup, shutdown, or restart;

1.6.1.9. in the case of any application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), and in cases of failure of network services, such as DHCP or DNS, or hardware fault; and

1.6.1.10. if contractor detects suspicious or malicious activity, such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

1.6.2. Contractor will retain system activity logs (and make all such logs available to City) for a period of three years after final payment on this Contract, or three years after all forensic, audit and litigation matters are resolved, whichever is longer.

1.6.3. Contractor will review all relevant security logs for anomalies for potential Security Incidents and forensic analysis.

1.7. Media Reuse

1.7.1. Contractor must promptly Securely Erase all City Confidential Information from any permanent or non-volatile storage media:

1.7.1.1. once immediate use of such media is no longer necessary,

1.7.1.2. at City's request, or

1.7.1.3. within 30 days of termination of the Contract.

1.7.2. For all endpoint and mobile devices containing City Data, Contractor agrees to utilize full disk encryption with pre-boot authentication methodologies to ensure all City Confidential Data is encrypted at rest.

1.7.3. Contractor shall Securely Erase all City Data by destructively overwriting all City Data to ensure that even deleted files cannot be recovered from the media.

1.8. Security

1.8.1. Contractor must limit access to the Hypervisor to only those qualified and pre-approved staff who have job functions dedicated to performing work on the Hypervisor. All access logs to the Hypervisor must only be reviewed by qualified personnel approved by Contractor and City.

1.8.2.   City retains ownership over all City Data.

1.8.3.   Contractor must use industry best practices for encryption of City Confidential Information at rest and in transit.

1.8.4.   Contractor will ensure that all electronic and physical access to City Data is secured. Contractor must verify the identification, authentication, and authorization of each user and their specific role and access level, and Contractor must immediately block all physical and electronic access to City Data for any terminated employee.

1.8.5.   Contractor must use due diligence to evaluate and respond to potential Security Incidents and events that create suspicions of unauthorized disclosure, modification, or destruction of City Data. The response must restore the confidentiality, integrity, and availability of the environment(s) compromised or potentially compromised, and establish root causes and remediation steps and determine the nature and extent of the event. If Contractor determines that there has been a Security Incident involving City Data (including City Confidential Information), Contractor shall report such Security Incident to the City PM within four (4) hours of determination.

1.8.6.   Upon written request, Contractor shall make its then current key management policy for encryption keys and certificates available to the City within 10 business days.

2. DATA HANDLING CONTROLS: ADDITIONAL COMPLIANCE REQUIREMENTS

2.1. Contractor Practices

2.1.1.   In addition to any other requirements of these Data Handling Controls, Contractor agrees it shall maintain and enforce its own reasonable and adequate security procedures during the term of the Contract for the protection of City Data, which procedures must be designed to protect City Data (especially City Confidential Information) and the hosting environment from a Security Incident, including using Contractor's best efforts to avoid the unauthorized access, modification or loss during transmission and storage, including the use of data encryption techniques described herein.

2.1.2.   Contractor confirms that all use, transmission, storage, and destruction of City Confidential Information shall be in strict accordance with all terms, covenants, and conditions of the Contract and all applicable Federal, State, and local laws, rules, and regulations.

2.1.3.   Contractor agrees that City may conduct, at no extra cost to City, network penetration tests of all systems at Contractor's facilities used for the processing,

storage or transmission of City Data. City may also, at its discretion, contract out penetration testing services to a third party. City shall provide reasonable notice of each network penetration test and shall conduct each network penetration test at reasonable times. If, following any testing, vulnerabilities are identified, Contractor shall promptly document Contractor's remediation action plan and provide it to the City PM within three business days, including at a minimum:

    2.1.3.1.1.   nature of the vulnerability including scope and breadth,

    2.1.3.1.2.   potential impact to service of vulnerability and subsequent mitigation,

    2.1.3.1.3.   summary of mitigation, and

    2.1.3.1.4.   known or suspected loss of City Data and ability to recover; and

2.1.3.2.   implement the remediation action plan not later than three business days after delivery of the plan unless otherwise approved by City in writing. The implementation of remediation activity must be communicated to and approved by the City in advance, ensuring the avoidance of unplanned outages; and

2.1.3.3.   provide City with written documentation and reports on the status of all modifications to correct such vulnerabilities, including interim and final reports.

2.1.4.   Contractor shall perform appropriate background checks on its employees and subcontractors with access to City Confidential Information.

2.1.5.   Contractor shall prohibit access to City Confidential Information for Contractor employees and subcontractors who fit into any of the following classifications:

2.1.5.1.   Anyone who has been convicted of a felony offense;

2.1.5.2.   Anyone who has been convicted of a misdemeanor offense related to computer security, theft, fraud or violence; or

2.1.5.3.   Anyone who is currently awaiting trial for any of the above-stated offenses.

2.1.6.   The COA CISO may, at any time in writing, require Contractor's employees and subcontractors to submit to additional background checks. Continued access to City Data, including City Confidential Information, and secured facilities shall be contingent on the Contractor's employee's agreement to submit to a background check and the results of the background check. Refusal shall be grounds for immediate termination of the User ID and password, and where applicable, access to COA premises and networks, and any ID badge issued shall immediately be decommissioned.

2.2. Security Incident Reporting Procedures

2.2.1. Contractor must telephone the City PM and e-mail AE-Exec-Info-Sec@austinenergy.com within four business hours of when Contractor discovers, is notified of, or otherwise has knowledge of any Security Incident. Contractor must include the following information in the report emailed:

2.2.1.1. person reporting the Security Incident ;

2.2.1.2. person who discovered the Security Incident;

2.2.1.3. date and time the Security Incident was discovered;

2.2.1.4. nature of the Security Incident;

2.2.1.5. actions taken and by whom;

2.2.1.6. involved system and possible interconnectivity with other systems;

2.2.1.7. description of the information lost or compromised, or potentially lost or compromised;

2.2.1.8. storage medium from which information was lost or compromised;

2.2.1.9. controls in place to prevent unauthorized use of the lost or compromised information;

2.2.1.10. number of individuals potentially affected;

2.2.1.11. whether law enforcement or other external agencies were involved for any reason and, if so, those contacted; and

2.2.1.12. any other relevant information pertaining to the Security Incident.

2.2.2. Within four hours of discovering the Security Incident, the Contractor shall contain the Security Incident.

2.2.3. Contractor shall investigate (with City's participation, if so desired by City) the Security Incident, perform a root cause analysis, and create and provide to the City a remediation plan within seven days of becoming aware of the Security Incident.

2.3. Remediation

2.3.1. As soon as practicable, and at no additional cost to the City, Contractor will remedy the source of the Security Incident, as required by the remediation plan.

2.3.2. The Contractor shall reimburse the City for all costs to City associated with the Security Incident.

2.4. Recovery

2.4.1. Within seven days of completing the remediation plan, Contractor must provide the City reasonable written assurance declaring full system recovery, signed by an executive with proper authority, attesting that the Security Incident is remediated and shall not recur.

2.5. Lessons Learned

2.5.1. Contractor shall, at no cost to the City and as part of the Services, update policies, procedures, or enforcement methods in a manner designed to prevent similar Security Incidents from recurring and provide summary of updates to City within 14 days of declaring full system recovery.

3. Definitions

3.1.1. **Authorized Person** – Contractor personnel (including subcontractor personnel) located in the contiguous United States having successfully completed the required background check and related requirements of the Contract

3.1.2. **City Project Manager or City PM** – City of Austin project manager, or their designee, assigned to this Contract

3.1.3. **City Data** - data or information (in any form) regarding the City or its customers that is created, collected, provided, obtained, or otherwise made available in connection with this Contract to an Authorized Person. City Data may be either non-confidential information or City Confidential Information.

3.1.4. **City Confidential Information** – includes: (A) information provided by City that is marked or identified as confidential, (B) information of City including software, computer programs, documentation, processes, procedures, techniques, technical, financial, customer, personnel and other business information of a non-public nature that would reasonably be understood to be confidential whether or not marked or identified as confidential, (C) information generated by Contractor (or subcontractor) that contains, reflects, or is derived from confidential information, (D) Personal Identifying Information, (E) Sensitive Personal Information, and (F) all other information made confidential by federal, state or local law or regulation. City Confidential Information is a subset of City Data.

3.1.5. **Data Center Region** – means the authorized geographical region for the storage and processing of City Data, and is presently only the contiguous United States.

3.1.6. **Data Handling Controls** – this document

3.1.7. **Endpoint Device** – Any network-capable computer hardware device including, but not limited to desktop computers, laptops, smart phones, tablets, thin

clients, printers or other specialized hardware such POS terminals and smart meters.

3.1.8. **Hypervisor** – a piece of computer software, firmware or hardware that controls the flow of instructions between guest Operating Systems and the physical hardware such as CPU, disk storage, memory, and network interface cards within a virtual environment

3.1.9. **Personal Identifying Information** ("PII") – means any information that, either alone or in conjunction with other information, identifies an individual, including an individual's:

3.1.9.1. name, social security number, date of birth, or government-issued identification number;

3.1.9.2. mother's maiden name;

3.1.9.3. unique biometric data, including the individual's fingerprint, voice print, and retina or iris image; or

3.1.9.4. unique electronic identification number, address, or routing code

3.1.10. **Sensitive Personal Information** ("SPI") – means

A. an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

(i) Social Security Number;

(ii) Driver's License Number or government-issued ID; or

(iii) an individual's account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account, or

B. information that identifies an individual and relates to the physical or mental health or condition of the individual, or the provision of health care to the individual.

C. SPI does not include publicly available information.

3.1.11. **Securely Erase** – secure deletion of any information, including a recognized destructive delete algorithm, for example, at least seven overwrites with pseudorandom data or at least seven overwrites with zeroes

3.1.12. **Security Incident** – any actual or potential unauthorized disclosure of, or unauthorized access to, City Confidential Information; or a violation or imminent threat of violation of computer security policies, acceptable use policies, or compliance requirements under these Data Handling Controls; or violation or imminent threat of violation of industry standard security practices

3.1.13. **Secure Service Area** – a physically and electronically secured area, with secure communications, within Contractor's facility where unencrypted City Confidential Information is secured from unauthorized access