

FACTA AFFIDAVIT OF COMPLIANCE

I HEREBY AFFIRM that I, [name] _____, am the [title] _____, and the duly authorized representative of _____ (“Company”). 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 Company.

I ACKNOWLEDGE that, in accordance with the Fair and Accurate Credit Transactions Act (FACTA), the City of Austin (“City”) is required to ensure that the activities of entities that contract with the City to provide the City services related to the billing accounts of the City’s utility customers, are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

I ACKNOWLEDGE that, the City has provided the Company with a list of red flags that the City has identified as potential indicators of unauthorized access to consumer information and malicious account activity. A list of the red flags is attached here as Exhibit A.

I FURTHER AFFIRM that, to the extent applicable to the services provided to the City by the Company, the Company 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

CITY OF AUSTIN
PURCHASING OFFICE
ATTACHMENT A: FACTA AFFIDAVIT OF COMPLIANCE
RFP 1100 ELF3000, MANAGED CONTACT CENTER COMMUNICATIONS & INFRASTRUCTURE SOLUTION

My commission expires: _____

EXHIBIT A – LIST OF APPLICABLE RED FLAGS

- Documents provided by a customer or potential customer to verify identification appear altered or forged.
- The photo or physical description on an identification document (“ID”) is not consistent with the appearance of the customer.
- Other information given to open the account is not consistent with the ID of the customer
- An application or supporting document appears to have been forged or altered, or gives the appearance of having been destroyed and reassembled.
- The ID is inconsistent with external information sources; i.e., the address does not match a consumer report, or a social security (SS) number has not be issued or is listed on the SS Administration Death Master File.
- The ID provided is associated with an existing identity theft case on file.
- The SS number is the same as customers opening other accounts (or previously used to open an account when the customer states that they have not previously had an account.)
- The customer fails to provide all personal identification information upon request.
- The ID is inconsistent with existing records.
- Change of billing address is followed by multiple change requests to the account.
- Payments are made in a manner associated with fraud. For example, a deposit or initial payment is made and no payments are made thereafter.
- Existing account with a stable history shows irregularities.
- An account that has been inactive for a reasonable period of time is suddenly used.
- The utility is notified of unauthorized changes or transactions in connection with an account.

| | |
|---|--|
| 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

Contents 1

1. Data Handling Controls: Security Directives and Requirements 2

 1.1. Contractor Responsibilities regarding treatment of City Data 2

 1.2. Location Parameters 2

 1.3. Specific Security Directives 2

 1.4. Data Disposition..... 3

 1.5. General Compliance Requirements 3

 1.6. Logging/Auditing Requirements 4

 1.7. Media Reuse 5

 1.8. Security 5

2. Data Handling Controls: Additional Compliance Requirements..... 6

 2.1. Contractor Practices 6

 2.2. Security Incident Reporting Procedures 8

 2.3. Remediation 8

 2.4. Recovery 9

 2.5. Lessons Learned..... 9



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 Contractor 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 as 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



Network Connection Agreement

Austin Energy Network and Systems Access

PART I

This Network Connection Agreement for Network and Systems Access ("Agreement") is entered into as of [ENTER MONTH, DAY, YEAR] (the "Effective Date"), by and between

AUSTIN ENERGY, the Electric Utility Department of the City of Austin ("Austin Energy")

and

[ENTER COMPANY NAME] ("Consultant" or "Company").

Part II of this Agreement sets forth the terms and conditions under which Austin Energy is willing to permit Consultant access to Austin Energy's corporate computer network (the "Network") and one or more Austin Energy information and computer systems (the "Systems").

Austin Energy has, at substantial cost, developed the Network and Systems to provide information services to itself and other City of Austin departments. The Network and Systems perform vital functions for these departments. The unwarranted or unauthorized access or use of the Network or Systems could put Austin Energy and these departments at significant risk of damage, including power plant power outages, interruption of electric utility service, interference with statewide power grids, danger to life and property, destruction of data, and the unwanted disclosure of sensitive or private information.

Consultant (and/or its subcontractors) has requested access to some or all of the Austin Energy Network and Systems, to facilitate the performance of its obligations to Austin Energy relative to the following project or contracted service:

[ENTER PROJECT OR SERVICE NAME]

For the purpose of clarification, the terms of this Agreement apply to the Consultant's access or Consultant's subcontractors' access to Austin Energy via Anywhere Outside Connect (AOC). "Consultant" includes Consultant's subcontractors wherever that term is used in this Agreement.

Austin Energy is willing to permit such access based on the level of risk to Austin Energy's physical and information assets and Consultant's assurance that it will abide by the terms and conditions as defined in Part II of this Agreement.



Network Connection Agreement

Austin Energy Network & Systems Access

PART II: Terms and Conditions

1. SCOPE OF ACCESS

Consultant shall use this access to the Network and Systems solely for the purpose of performing services associated with the project or contract at Austin Energy as specified in Part I of this Agreement. Consultant shall limit its access to the means and method approved by Austin Energy, as further described below in Section 6, *Specific Connections*.

Austin Energy may terminate or otherwise curtail Consultant's access to the Network or Systems at any time without notice to Consultant. However, Consultant will be relieved of any obligation to perform implementation or services as required by Austin Energy to the extent the termination was without cause, and access by Consultant was necessary to perform such obligation.

Consultant shall comply with the terms and conditions set forth in this Agreement, and with any security procedures, guidelines or alerts issued by Austin Energy from time to time. Austin Energy may, upon written notice to Consultant, require modification or supplementing of any of the terms and conditions contained in this Agreement, and Consultant agrees to abide by those terms.

2. DEFINITIONS

| | |
|-----------------------------------|--|
| Computer system | The complete, working computer. Includes not only the computer, but also any software and peripheral devices that are necessary to make the computer function. |
| Information System | The business application that operates on a computer system. Includes the database, application programs, and machine procedures. |
| Network | The system that transmits any combination of voice, video and/or data between users. Includes all supporting hardware, such routers and switches, the cables connecting them, client and server machines, and network operating systems. |
| Consultant Executive | Consultant's executive who is authorized to and signs this legally binding agreement. This executive is expected to be the Company's President, a Vice President, Legal counsel, or equivalent role. |
| Consultant Delegated Agent | Consultant's point of contact to Austin Energy who administers the day-to-day operations of the project/program, such as Program Manager or Team Supervisor. Written notice is required for replacements (see Section 7, <i>Delegation of Authority</i> for requirements). |



3. CONSENT TO MONITORING

Austin Energy may monitor and record any access to the Network and Systems at any time without notice to Consultant. Consultant consents to this monitoring and recording, and Consultant will ensure that all persons obtaining access to the Network and Systems through Consultant consent to this monitoring and recording.

4. CONSULTANT RESPONSIBILITIES

4.1 Consultant Personnel

Consultant shall limit access to the Network and Systems to those employees of Consultant ("Consultant Personnel") who need to have such access. Consultant shall provide a copy of this Agreement to all Consultant Personnel requiring remote access and shall require each person to review and sign the individual Consultant Remote Access Request form acknowledging such. Consultant agrees it shall be entirely responsible for the acts and omissions of any person to whom it authorizes access.

4.2 Login IDs and Security Tokens

4.2.1 Personal Token Login IDs

Austin Energy may elect to issue a personal Login ID and security token to authorized Consultant Personnel to be used during login. Consultant Personnel assigned a token are responsible to keep said token secure. Only the authorized individual is permitted to use his or her assigned Login ID and token passcode.

Austin Energy may request the return of the token at any time. A fee of \$100 will be paid by the Consultant if the token is not returned or, upon return, is not in working order.

4.2.2 Shared Token Login IDs

Austin Energy may assign a shared Login ID to a pool of Consultant Personnel who are authorized to access Austin Energy Systems for the purpose of intermittent technical support. A shared security token for the Consultant Personnel shall be issued to an authorized Austin Energy contact, who shall serve as the token custodian. Consultant must contact the Austin Energy token custodian in order to gain a passcode for single session access.

4.3 Consultant Systems

Consultant shall be responsible for all systems that Consultant uses to access the Network and Systems. Consultant shall ensure that its systems include up-to-date antiviral software reasonably acceptable to Austin Energy to prevent viruses from reaching the Network and Systems through Consultant's systems. Consultant shall take reasonable precautions to prevent unauthorized access to the Network and Systems through Consultant's systems.

Consultant assumes full responsibility for any systems it uses to access the Network or Systems, notwithstanding a specification or direction from Austin Energy. Consultant is expected to back up its own files, maintain firewalls, and take such other precautions as will minimize the impact of any malfunction or computer error on its own systems.



4.4 Notice of Breaches

Consultant shall IMMEDIATELY notify Austin Energy upon learning of any security breach by contacting the Austin Energy Technology Control Center at (512) 322-6077 and the Austin Energy contact person identified in the Agreement (by phone or e-mail). Consultant shall communicate the nature of its access and the nature of the security breach. In addition, Consultant shall, within 24 hours of the security breach, notify the Austin Energy contact person by written notice as described in Section 8, *Notices and Contacts*.

As used in this Section 4.4, the term "security breach" means any actual or threatened unauthorized access to the Network or the Systems, or to the details or specifications that would enable another individual to gain access, or to any information or data obtained during access. By way of examples, (1) knowledge that a specific Login ID has been published or otherwise made available to an unintended recipient constitutes a security breach, or (2) knowledge that an individual might have copied Austin Energy files, without the express permission of Austin Energy, or that an individual might have used access to the Network or Systems for any purpose other than that described in Section 1, *Scope of Access*, constitutes a security breach.

Consultant shall cooperate fully with Austin Energy to investigate any security breach and to take such steps as to minimize the impact thereof.

4.5 Third-Party Software

Access to the Network and Systems may involve access to software or other technology licensed by Austin Energy or other City departments from third parties. Consultant will use such software or technology for the sole purpose described in Section 1, *Scope of Access*, and shall comply with all restrictions applicable to that software and technology.

4.6 Transmission of Harmful Material

Consultant will not transmit nor permit the transmission of any unlawful, threatening, libelous, defamatory, obscene, scandalous, inflammatory, pornographic or profane material through the Network and Systems. Consultant acknowledges that Austin Energy intends to cooperate fully with law enforcement, regulatory, or judicial investigations of any access to the Network and Systems. This cooperation can include disclosure of the identity of, and the information transmitted or received by, persons accessing the Network and Systems.

4.7 Security Audits

In addition to, and without limiting, any rights contained in the Agreement, Austin Energy, at its sole expense, may conduct security audits of Consultant's access and of any Consultant systems that have access to the Network and Systems. These audits can include (1) an inspection of Consultant's systems and environment, (2) a review of Consultant's security procedures, and (3) an execution of security tests to verify system integrity. Consultant will immediately resolve any material issues identified through these audits.

4.8 Removal of Data

Consultant shall not retain copies of any data or information (including Third-Party Software) obtained from access to the Network and Systems, except as expressly permitted by Austin Energy in writing. Upon Austin Energy's request, Consultant shall promptly return such data and information to Austin Energy or destroy it as directed by Austin Energy, and so certify the same to Austin Energy in writing.

4.9 Confidentiality

All details, specifications, and other information regarding Consultant's access to the Network and Systems, including, but not limited to, all Login IDs and any information obtained as a result of access to, the Network and Systems, shall be deemed "Confidential Information" of Austin Energy.

Consultant agrees that it will not use, disclose, publish, or otherwise divulge to any third party either during or after the termination of this Agreement or permit its officers or employees to so divulge any Confidential Information of Austin Energy without prior written consent of Austin Energy. Consultant shall employ no less stringent procedures than the procedures used to protect its own confidential data. If disclosure to a third party, such as an auditor, is required, the third party is required to first sign a confidentiality agreement with the owner of the confidential information.

5. DISCLAIMER

ACCESS TO THE NETWORK, THE SYSTEMS AND ANY SOFTWARE OR EQUIPMENT PROVIDED THEREWITH IS PROVIDED "AS IS" WITHOUT ANY WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. Nothing in these terms and conditions shall be construed as granting Consultant a right of access to the Network or Systems, a right to access the premises of Austin Energy, or a right to use any software or equipment provided therewith without express permission from Austin Energy.

6. SPECIFIC CONNECTIONS

6.1 Conditions for Client Connections

Consultant agrees that it or any of its associated affiliates, subsidiaries, or subcontractors is prohibited from directly accessing or connecting to the Network from any non-U.S.-based remote access or connection point, and agrees any such connection constitutes an immediate violation of this Agreement such that Austin Energy shall immediately sever any such access without liability or legal exposure of any sort.

Unless otherwise authorized by Austin Energy, all remote access for support or monitoring purposes shall go through Austin Energy's secure corporate remote access solution.

All access to the Network and Systems shall be strictly limited, both physically and technologically, to that which is necessary to perform the permitted tasks.

6.2 Conditions for Cyber Security Adherence

Consultant agrees to comply with Austin Energy Consultant/Vendor Acceptable Use Policy (attached as Appendix) and any other mutually agreed upon cyber security requirements defined in this Agreement or other contract.

Consultant is responsible for implementing antivirus software and updating virus signatures on a regular basis (at least monthly) and for implementing applicable system security software updates. Such updates shall be applied within a reasonable period after software release, availability or written notification, not to exceed 30 days. In the event of serious network security incident or breach deemed by Austin Energy Information Security, Consultant may be required to immediately apply updates or to disconnect from the Network at Austin Energy's request.

Consultant shall immediately notify Austin Energy, as described in Section 4.4, upon discovery of any security incident. Security incidents include but are not limited to, virus, network intrusion, or other event on Consultant's computer network that could affect the Network or system or data contained therein. During such incidents, Consultant shall immediately disconnect the computer network connection, either at the request of Austin Energy or as Consultant deems appropriate to protect the Network, the Systems, or data.

7. DELEGATION OF AUTHORITY

Consultant Executive shall delegate a Consultant Delegated Agent who shall be responsible for reviewing and approving individual Consultant Personnel requests for remote access as defined in this Agreement. All Consultant Personnel connections are subject to Austin Energy consent, and subject to continued compliance with this Agreement.

The Consultant Executive or Delegated Agent may designate a replacement by providing written notice to the Austin Energy contact named in this Section 8, *Notices and Contacts*.

8. NOTICES AND CONTACTS

Unless otherwise provided above, all notices and contacts regarding remote access to the Network or Systems shall be made to the following:

If to Austin Energy:

Austin Energy
721 Barton Springs Rd
Austin, Texas 78704
Attn: Michael Goin
E-mail: Michael.Goin@austinenergy.com
(512) 322-6076

If to Consultant:

[Consultant Company name]
[Company Address]
[City, State Zip]
Attn: [Consultant Delegated Agent]
E-mail: [xxxxxxx@xxx.com]
[(area) xxx-xxxx]

All written notices must be delivered by hand-delivery, nationally recognized overnight courier, or U.S. mail and sent in a manner that provides confirmation of receipt. Where immediate notice is specifically required, notices shall be communicated first by telephone and followed up by e-mails, and then by written notice.

Either party may change its contact by providing written notice to the other using the above contact information.



9. SURVIVAL; MISCELLANEOUS

This Agreement and its provisions shall survive the expiration or termination of the project implementation or contracted service for so long as necessary as to carry out the intent of this Agreement. No act or omission on the part of Austin Energy shall be construed as a waiver of the terms and conditions contained in this Agreement unless in writing signed by Austin Energy, and no waiver in any particular instance shall act as a waiver in any future instance unless so stated in the writing.



Appendix to Network Connection Agreement Austin Energy Consultant/Vendor Acceptable Use Policy

1 PURPOSE

The purpose of this policy is to establish guidelines and minimum requirements governing the acceptable use of Austin Energy (AE) information technology resources and remote access connections provided to vendors and consultants as part of a contract agreement.

This policy is in addition to any mutually agreed upon cyber security requirements as defined by contract or connection agreement.

2 USER RESPONSIBILITIES

- 2.1 Be accountable for all activity conducted under the user's login or e-mail account.
- 2.2 Take all reasonable precautions to prevent the unauthorized use of workstations and laptops by unauthorized individuals.
- 2.3 Lock the keyboard or use a password-enabled screen saver whenever you leave your workstation or laptop to protect your account from unauthorized access.
- 2.4 Ensure up-to-date virus protection is installed and activated on any information technology system that is connected to the AE information technology systems.
- 2.5 Communicate data security needs of information under your purview to your AE Customer Relationship Manager or Project Manager.
- 2.6 Save all AE business data to authorized AE drives or AE-approved disk storage.
- 2.7 Follow all security requirements as specified in the contract and/or connection agreement approved by AE and the authorized consultant/vendor company representatives.
- 2.8 Use information technology resources efficiently and productively.
- 2.9 Do not download and/or install non-authorized software on AE information technology resources.
- 2.10 Be courteous and follow accepted standards of etiquette for e-mail communication.

3 GENERAL STATEMENT OF THE POLICY

- 3.1 The use of AE Internet, e-mail and information technology systems must be related to, and for the benefit of City of Austin government and/or AE business.
- 3.2 All on-line communications, such as e-mail messages (and attachments) and postings to various on-line discussion groups and forums, are subject to the same laws, regulations, policies, and other requirements as information communicated in other written forms and formats. This includes proper business correspondence practices and other appropriate use policies for AE equipment and systems.
- 3.3 Network resources must be used responsibly to avoid creating a negative impact on others who share those same resources (see section *4.7 Resource Considerations*).



4 IMPLEMENTATION

4.1 Security

- 4.1.1 Because the Internet and its tools adhere to open and documented standards and specifications, it is inherently an unsecured network that has no built-in security controls.
 - 4.1.1.1 Avoid including confidential and sensitive information in e-mail and on-line communications unless proper, formalized security precautions have been established and are used (such as, encryption).
 - 4.1.1.2 Protect privileged or confidential information whenever intentional, inappropriate, or accidental disclosure of the information might expose AE or an individual to loss or harm.
- 4.1.2 Protect your password. Passwords must not be shared with anyone, including managers.
- 4.1.3 Authorized AE information technology staff reserve the right to access your password information and change it through legitimate means for business or security reasons.
- 4.1.4 Remote access connections shall be through Secure Shell (SSH) that provides encryption to protect the transferred information and authentication that the target remote system is correct. Telnet use for remote access is prohibited.

4.2 Privacy

Users acknowledge that they have no legitimate expectation of privacy when using AE resources as follows:

- 4.2.1 All electronic files and data developed under contract are the property of AE, regardless of their physical location or the form in which they are maintained. These files and data may be used, stored and disclosed at AE's discretion.
- 4.2.2 Internet usage, e-mail, or other forms of electronic messaging are not considered personal or private when using AE resources.
- 4.2.3 AE has the right to access and disclose all messages, attachments, and other electronic data sent or received over the AE electronic mail system or stored in its files.
- 4.2.4 Any e-mail and attachments sent from or received under an AE e-mail account can be public records and are subject to the mandatory public disclosure requirements of the Texas Open Information Act, unless excepted by the Act.
- 4.2.5 AE ITT staff routinely monitors every connection to the Internet (including e-mail, Websites, and instant messaging) to ensure compliance with this policy.

4.3 Acceptable Use

Acceptable uses of computer resources are those that conform to the purpose, goals, and mission of AE, to each user's job duties and responsibilities according to contracted services between AE and the consultant or vendor. The following list, although not all-inclusive, provides some examples of acceptable uses:



- 4.3.1 Accessing computer systems and resources to perform work required to fulfill contractual obligations
- 4.3.2 Communications and information exchanges directly relating to the mission, charter, and work tasks of AE including e-mail in direct support of work-related functions or collaborative projects.
- 4.3.3 Communications with vendors of products used or being considered for use by AE, either to investigate use of their product or to receive help in using their product.
- 4.3.4 Research and information gathering in support of AE.

4.4 Unacceptable Use

Unacceptable use can be defined as activities that do not conform to the purpose, goals, and mission of AE and to each user's job duties and responsibilities as contracted between AE and the consultant or vendor. Any questionable computer usage should be avoided. When in doubt, seek clarification with AE management prior to pursuing the activity.

AE computers, e-mail, and/or Internet or remote access connections cannot be used to perform any of the following activities:

- 4.4.1 Seek or gain unauthorized access to AE or City of Austin network resources or Internet or intranet resources. Provide a means of unauthorized access to any AE or City of Austin resources.
- 4.4.2 Destroy the integrity of computer-based information.
- 4.4.3 Compromise the privacy and/or security of users.
- 4.4.4 Disrupt the functions of AE and/or City of Austin networks or other computer resources, including, but not limited to, propagation of worms or viruses or other debilitating programs.
- 4.4.5 Circumvent legal copyrights or trademarks or participate in their infringement.
- 4.4.6 Conduct or promote commercial or private/personal business enterprises or products.
- 4.4.7 Support or solicit on behalf of groups, organizations, or such that are not related to AE or City of Austin or engage in political lobbying.
- 4.4.8 Transmit unsolicited commercial information (such as junk mail or advertising). Issue or propagate unsolicited e-mail or bulk e-mail.
- 4.4.9 Listen to, view, or download audio or video files for entertainment or leisure activities unless authorized by the appropriate AE project manager or supervisor.
- 4.4.10 Transmit material that may be deemed offensive to its recipient. View, transmit, or receive sexually explicit material. Advocate racial, ethnic, religious, or gender-based slurs.
- 4.4.11 Threaten or harass others. Contribute to the harming of minors.
- 4.4.12 Conduct or participate in illegal or fraudulent activity. Commit forgery or impersonation.



4.5 Remote Access

- 4.5.1 Remote access is a privilege, not a right. Any violation in its use can result in access being terminated.
- 4.5.2 Do not share connection information, such as passwords, phone numbers, encryption keys or software, with anyone.
- 4.5.3 Follow all Terms and Conditions of the Network Connection Agreement approved by AE and the authorized consultant/vendor company representatives.

4.6 Wireless Network/Access

- 4.6.1 Wireless connections to the AE network are expressly prohibited unless sanctioned by AE Information Technology Infrastructure Management.
- 4.6.2 Wireless home networks are not allowed to be connected to AE's network.

4.7 Resource Considerations

The following policies relate to activities that can negatively affect network performance and resources:

- 4.7.1 Only approved staff within AE are permitted to broadcast messages to all AE employees at once. Contact the AE Technology Control Center if such notifications are needed.
- 4.7.2 Delete unnecessary messages and attachments on AE e-mail accounts, according to AE record retention requirements. Contact the AE Records Coordinator for the appropriate workgroup for more information.
- 4.7.3 Whenever possible, avoid sending e-mails with 100kb or larger document attachments. For internal correspondence, when possible, place the document in a shared location and link it in the e-mail. For external correspondence, it is preferable to use FTP to transfer large files.
- 4.7.4 Limit downloading large files to a time after normal business hours at both local time and the time at the remote site. Users must be knowledgeable about the network and desktop resource requirements for the transfer.
- 4.7.5 Only subscribe to very active mailing lists, discussion groups or news groups if absolutely necessary to support a job duty or assignment. A high volume of messages can impact your time, network resources, and file storage requirements.
- 4.7.6 Avoid downloading music or videos to AE's resources for entertainment purposes. These programs can have virus, copyright and bandwidth issues.



**CITY OF AUSTIN
PURCHASING OFFICE
ATTACHMENT D: EXCEPTION FORM
RFP 1100 ELF3000, MANAGED CONTACT CENTER COMMUNICATIONS & INFRASTRUCTURE SOLUTION**

The City will presume that the Offeror is in agreement with all sections of the solicitation unless the Offeror takes specific exception as indicated below. Complete the exception information indicating each exception taken, provide alternative language, and justify the alternative language. Copies of this form may be utilized if additional pages are needed.

Proposers who comply with or who are most responsive to accepting the City's Standard Purchasing Terms and Conditions and Commercial and Legal Contract Requirements will receive consideration for evaluations from the City's evaluation team in determining points awarded for meeting criteria outlined in Section 0600 Proposal Preparation Instructions Evaluation Factors. Failure to agree to the standard contract terms may result in the City choosing to move forward with an award of a contract to the next best Offeror.

The City, at its sole discretion, may negotiate exceptions that do not result in material deviations from the sections contained in the solicitation documents. Material deviations as determined by the City may result in the City deeming the Offer non-responsive. The Offeror that is awarded the contract shall be required to sign the contract with the provisions accepted or negotiated.

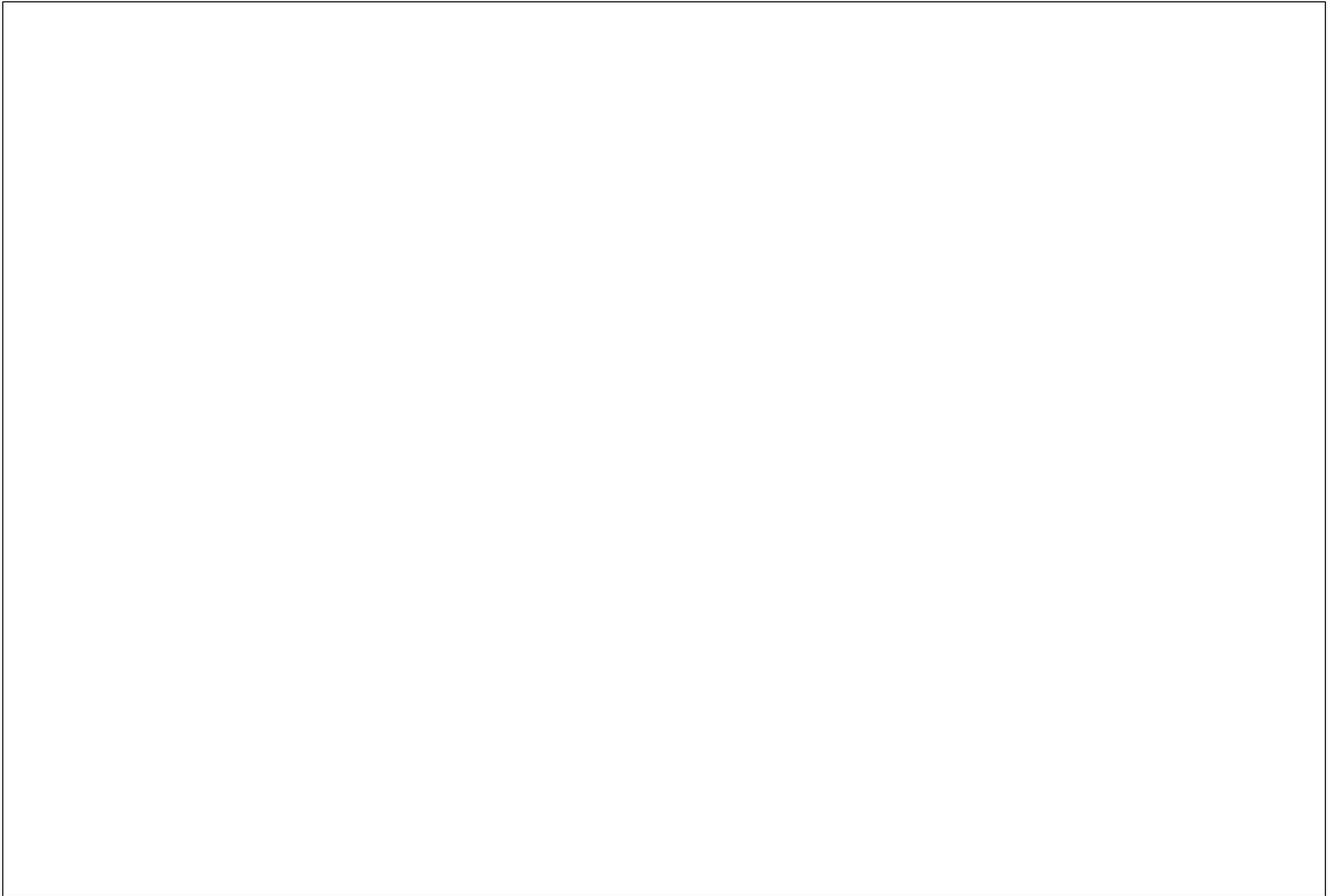
Indicate:

- 0300 Standard Purchase Terms & Conditions**
- 0400 Supplemental Purchase Provisions**
- 0401 Supplemental IT Cloud Purchase Provisions**
- 0500 Scope of Work**

| Page Number | Section Number | Section Description |
|--------------------|-----------------------|----------------------------|
|--------------------|-----------------------|----------------------------|

Alternate Language:

Justification:





Consultant Remote Access Request

For Consultants/Vendors Doing Business with Austin Energy

- Complete this form to request remote access connection to the AE network and computer and information systems.
- Sign and obtain your Delegated Agent signature. Send form to your AE IT sponsor or AE Business Unit contact.
- AE IT sponsor or AE Business Unit contact will submit form to the AE Technology Control Center (TCC) for processing.
- For online completion, use TAB or SHIFT+TAB to advance or return to entry fields.
- If completed manually, print using BLACK or BLUE ink.

| | | |
|--|--|---------------|
| Consultant Employee Name (First Last): | Job Role: | |
| Consultant Company Name: | Employee Phone: | |
| <input type="checkbox"/> US Citizen/Permanent Resident <input type="checkbox"/> Temporary Worker; Classification: <input type="checkbox"/> Temporary Visitor for Business; Classification: | <u>Work location</u> City: State: Country: | |
| AE Business Unit Contact: | AE Contact Work Phone: | |
| IT Sponsor Name: | IT Sponsor Work Phone: | |
| Start Date: | End Date: | |
| Project or contract name: | Anticipated frequency of access: | |
| Business Justification: | | |
| <ul style="list-style-type: none"> • Consultants are prohibited from access to the Austin Energy network while they are outside the U.S. • Allow maximum of 10 business days for your account to be processed. • Technical support is available 6AM-6PM business days. After-hours support is available 24/7 for critical or emergency situations. Call the TCC at (512) 322-6077. • Remote access is limited to 6-month increments. Call the TCC on or near expiration date to extend if contract is still active. • The system may be unavailable during some hours due to maintenance. • The AE IT Security Manager is responsible for review and final approval. | | |
| Remote access privileges are subject to all responsibilities and limitations as agreed to by Consultant Company in the AE Network Connection Agreement and AE Consultant/Vendor Acceptable Use Policy. Consultant Delegated Agent has made a copy of the Agreement and Policy available to the undersigned Consultant Employee. | | |
| _____ Consultant Employee Name (Print) | _____ Signature | _____ Date |
| _____ Consultant Delegated Agent Name (Print) | _____ Signature | _____ Date |
| _____ Business Unit Process Manager Name (Print) | _____ Signature | _____ Date |
| _____ IT Sponsor Name (Print) | _____ Signature | _____ Date |
| List all server names, folders, and files. | | |
| _____ Server Name | _____ Folder path/name | |