POLICY ON INFORMATION SECURITY, CYBERSECURITY, AND PRIVACY FOR SUPPLIERS[1]

This Policy on Information Security, Cybersecurity, and Privacy for Suppliers ("Cyber Policy") provides the cybersecurity and privacy procedures Suppliers must implement on or before the effective date of any Purchase Order involving Special Conditions and maintain as long as Supplier has access to Edison's Computing Systems or access to, possession, custody, or control of Edison Data. These procedures are in addition to the security and confidentiality requirements of the applicable agreement and present a minimum standard only. They apply to Supplier's access to and use of Edison Data and Edison's Computing Systems, including BES Cyber Systems. They also apply to Supplier's work for Edison at any stage of the lifecycle of Edison Data and use of Edison's Computing Systems including creation, collection, storage, usage, processing, sharing, transferring, securing, retention and destruction. These procedures also apply to the Supplier's own internal information security and cybersecurity program insofar as those programs may affect or relate to Edison Data or Edison's Computing Systems.

It is Supplier's obligation to (i) implement and maintain appropriate measures to protect Edison's Computing Systems from unauthorized access or use and all Edison Data from accidental or unauthorized access, acquisition, disclosure, use, modification, loss, damage, or destruction, and to secure its own electronic network and systems, and Edison's Data from internal and external security threats; (ii) continually review and revise those measures to address new or ongoing risks and to implement industry best practices and legal requirements regarding cybersecurity and privacy; and (iii) to cooperate with Edison in its efforts to minimize risks to Edison's Computing Systems and Edison Data and reduce the impact of any unauthorized access to the Edison's Computing Systems, or disclosure or unauthorized use of Edison Data.

Supplier's security measures to safeguard Edison's Computing Systems and Edison Data in its possession, custody, or control shall be no less rigorous than industry cybersecurity and privacy best practices. Without in any way limiting the generality of the foregoing, Supplier's security and privacy practices and procedures must address the following areas and comply in all material respects with the following additional requirements for those areas:

A. Management of Information Security

1. Supplier shall maintain and update as necessary a comprehensive written information security program (the "Information Security Program" that: (i) contains appropriate administrative, technical, and physical safeguards to protect Edison's Computing Systems and Edison Data; (ii) complies with applicable laws and regulations and conforms to industry best practices; (iii) is reviewed and revised for adequacy and effectiveness at regular intervals (at least annually and whenever there is a material change in Supplier's practices that may materially affect the security of Edison Data or Edison's Computing Systems). During the course of providing the Services, Supplier shall not alter or modify its Information Security Program in such a way that will weaken or compromise the confidentiality, availability, or integrity of Edison Data or Edison's Computing Systems.

[1] As used herein, Supplier means any vendor that provides products or services to Southern California Edison Company or its affiliates. Supplier includes, but is not limited to, Contractor, Consultant and Licensor, as those terms may be used in agreements for products and services.

2. Supplier shall designate an individual responsible for information security within its organization (the "Information Security Officer") and have defined information security roles and responsibilities throughout the organization. Supplier shall provide the name and contact information of its designated Information Security Officer upon request**.**

B. Employee Policies

1. Security and Privacy Awareness and Training

Supplier shall provide its personnel with privacy and information security training before providing such personnel access to Edison's Computing Systems or Edison Data and at least annually thereafter. Supplier shall maintain employee completion reports and make such completion reports available to Edison upon Edison's written request. Supplier shall review the contents of the security and privacy awareness and training program at least annually to ensure it is updated and reflects current, relevant security information.

Depending upon the nature of the engagement Edison may specify in the purchase order, work order, or statement of work that Supplier shall supplement its information security training program with training or materials provided by Edison.

Supplier shall require that its internal and third-party software developers remain current on application security and secure coding best practices and that they regularly attend formal application security training programs.

Upon request, Supplier shall certify compliance with these training requirements.

2. Background Investigation

Supplier shall conduct, in accordance with industry best practices and applicable laws, a background investigation for every employee with access to Edison's Computing Systems or Edison Data. Background checks must include the following:

a. Thorough background verification including whether the prospective employee has been convicted of a felony, property crime or fraud in any state where the individual has resided, studied or worked during the past seven years; and

b. Check of United States' Specially Designated Nationals List and the Denied Persons List.

3. Agreements for Employees

Supplier shall use codes of conduct, ethics policies or confidentiality agreements to ensure employee awareness with Supplier's information security and privacy policies and procedures. Supplier shall obtain written acceptance of: (a) its codes of conduct, ethics policies, or confidentiality agreement; (b) Information Security Program; and (c) the requirements of this Cyber Policy from an employee before providing the employee access to Edison's Computing Systems or Edison Data, and at least annually thereafter for as long as the employee has such access. Supplier shall ensure all personnel sign the Edison's Computing Systems Use Acknowledgement ("Attachment 1") before accessing Edison's Computing Systems or Edison Data. If required by Edison in writing, Supplier shall return all such acknowledgements in a timely manner.

C. Supplier/Service Provider Management

Supplier shall assess and track cybersecurity and privacy risk associated with Subcontractors or its service providers with access to Edison's Computing Systems or Edison Data and shall take all commercially reasonable actions to promptly remediate these risks. Supplier shall contractually obligate Subcontractors or its service providers to protect Edison's Computing Systems and Edison Data, when accessed, processed, or stored by a Subcontractor or service provider, to the same level required of Supplier under this Cyber Policy.

D. Off-Shoring

Supplier shall not permit access to Edison's Computing Systems or transmit, access, use, or store Edison Data outside the United States without the prior written permission of Edison's Vice-President for Information Technology or the Director of Cybersecurity. Supplier is responsible for understanding and complying with the applicable cybersecurity and privacy laws and regulations of the foreign jurisdictions from which Edison agrees that Edison's Computing Systems or Edison Data may be accessed, used, or stored. As part of any offshoring request, Supplier shall inform Edison of any applicable foreign laws or regulations that may reduce the confidentiality, availability or integrity of Edison's Computing Systems or of Edison Data or impose additional burdens on Edison.

E. Asset Management

Supplier shall ensure that all of Supplier's or its Subcontractor's devices, including cell phones or other portable storage devices, used to store Edison Data shall be equipped with industry standard security and encryption features, which shall include at a minimum remote wipe and remote shutdown capabilities. Supplier's and Subcontractors' personnel may not access or store Edison Data on any personal or third party devices, including mobile devices, tablets or personally owned laptops, unless such devices have been configured with industry standard security and encryption features, which shall include at a minimum remote wipe and remote shutdown capabilities. .

F. Physical and Environmental Security

Supplier shall take appropriate steps to prevent unauthorized physical access, as well as accidental and intentional damage, to Supplier's physical premises and electronic systems that access, use, store or otherwise process Edison's Data. Supplier shall also take appropriate steps to protect against environmental risks and systems malfunctions or failures.

G. Communications and Operations Management

Supplier shall maintain written procedures and technological controls relating to the following areas.

1. Network Security - IDS/IPS Use and Signature Updates

Supplier shall subject all network traffic to electronic review and monitoring.

Supplier shall use Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS) systems that generate alerts containing sufficient information to detect and evaluate a

potential incident. Supplier shall ensure that IDS/IPS have the latest signatures applied in order to effectively monitor for the most recent threats and vulnerabilities.

2. Network Security - Firewall(s)

Supplier shall segregate its connected networks and electronic systems to ensure systems and applications are protected from outside threats. This shall include utilizing industry standard firewalls to segment and protect the organization's internal network from the Internet, and also to segregate systems that access, use, or store Edison Data from other less restricted internal networks and systems.

3. Firewall Configuration

Supplier shall disable, on public-facing firewalls, all ports and services that are not required for documented business purposes.

4. Network Logging

Supplier shall apply appropriate monitoring and logging technologies to record relevant actions involving access to Edison’s Computing Systems or Edison Data.

5. Malware Protection

Supplier shall use anti-malware software on networks, servers, workstations and portable devices that may be used to access Edison’s Computing Systems, or to access, use, or store, Edison Data; the malware signatures shall be regularly updated in a timely manner.

6. Patches and Updates

Suppler shall follow industry best practices for patching and updating software and firmware on networks, servers, workstations and portable devices that may be used to access Edison’s Computing Systems, or to transmit, access, use, or store, Edison Data.

7. Administrative Activity

Supplier shall minimize administrative privileges and allow personnel to only use administrative accounts when required.

Supplier shall appropriately log and monitor network, server and workstation activities, including log-in attempts, to record administrative activity for accountability and audit purposes.

8. Log Monitoring and Retention

Supplier will maintain and review audit logs for anomalies.

Supplier shall retain system and network logs for at least one year after the engagement is completed to allow for the successful auditing of historical events, to meet legal requirements, and for law enforcement and forensic purposes of either Supplier or Edison.

9. Email Relaying

Supplier shall secure access and prevent misuse of its own email resources.

10. Physical Media Tracking

Supplier shall establish effective processes and procedures for handling, storing and transporting media to protect Edison Data from unauthorized access and/or disclosure.

11. Unapproved Wireless Networks

Supplier shall have all network connections and devices adequately tracked, managed, authorized, and controlled to protect against threats and to maintain security for the systems and applications using the network.

12. Wireless Networks Encryption

Supplier shall implement processes and tools to control the use of wireless local area networks, access points and wireless systems, including encryption for authorized wireless access points.

13. Network Security- Authorized Network Traffic

Supplier shall formally review, approve and authorize all permitted network services.

14. System and Data Recovery

Supplier shall ensure that Edison Data and systems that access, store or use Edison Data are regularly backed up. Backups of these systems and data shall be available, including in the event of a disaster and the ability to restore from such backups shall be tested periodically.

15. Change Control

Supplier shall ensure that changes affecting Edison's Computing Systems or Edison Data are made within a formal change control program.

16. Data Encryption

a. Edison Confidential Information, including any backups, must be secured through whole disk or media encryption and file or database encryption (if applicable) and strong access controls at all times; and

b. Transmission of Edison Confidential Information must be encrypted at all times.

17. BES Cyber System Information

Supplier shall not use email to transport or store BES Cyber System Information.

H. Access Control

Supplier shall control access to its technology assets and Edison Data, including implementation of the following requirements:

1. Password Controls

Password controls meeting industry best practices, including:

(i) Encrypting passwords using "hashing" and "salting" techniques, in transit and at rest;
(ii) Enforcing password complexity requirements on users
(iii) Limiting failed attempts before lockout;
(iv) Prohibiting obvious or common passwords; and
(v) Not sending credentials through email for password resets.

2. Logical and Physical Access Authorizations and Suspensions

Supplier shall limit access to Edison's Computing Systems and Edison Data only to active users who require access to perform the Services. Supplier shall immediately notify Edison management to promptly revoke or disable user access rights to Edison's Computing Systems and to Edison Data of any employee who is terminated, resigns, or retires, or who is reassigned from work requiring access to Edison's Computing Systems or to Edison Data. Supplier also shall immediately revoke the employee's or former employee's access to Edison Data in Supplier's possession, custody, or control.

3. Multifactor Authentication for Remote Access

Supplier shall use two-factor authentication for remote access to systems that access or store Edison Data.

4. Logging and Monitoring of Persons with Access to BES Cyber System Information

Supplier shall assign an employee to track and monitor Supplier employees, agents, and subcontractors who have access to BES Cyber System Information in Supplier's possession, custody, or control. Supplier shall maintain logs identifying (i) such persons to whom Supplier provides access to BES Cyber System Information in Supplier's possession, custody, or control; (ii) whether such persons have been trained or re-trained, if training is required by Edison; and (iii) the dates that Supplier provided or revoked that person's access rights to BES Cyber System Information.

5. Return or Destruction of Edison Data

All Edison Data shall be and remain the property of Edison. At the end of each engagement, Supplier may keep one copy of the Edison Data solely for archival purposes, except that all BES Cyber Information must be rendered irretrievable as soon as possible, but in no event more than fifteen (15) days after the conclusion of the engagement, regardless of how it is stored or accessed. The destruction of Edison Data shall require use of industry best practices for rendering information irretrievable. Within fifteen (15) days after the conclusion of the engagement, Supplier shall provide Edison with a written confirmation executed by a manager or officer of Supplier confirming that all CEII and BES Cyber System Information in its possession, custody or control has been rendered

irretrievable.

I. Security Incident and Communications Management

Supplier shall implement a formalized information security incident management program (the "Security Incident Management Program"). The program shall describe how the organization will report incidents internally and to affected external parties. It shall also identify Supplier's incident response team (the "Supplier Incident Response Team") and define their roles and responsibilities.

1. Technical Compliance Checking – Vulnerability Testing and Remediation

Supplier shall regularly scan systems for vulnerabilities. Supplier shall rank all vulnerabilities and promptly remediate detected vulnerabilities ranked as critical, high or moderate. Supplier will use commercially reasonable efforts to identify and notify Edison in writing within one business day of identification of any critical, high or moderate vulnerabilities, risks or threats that could potentially impact Edison Data and that Supplier cannot remediate within 30 days. If Supplier later determines that it cannot remediate within 30 days, it shall promptly notify Edison in writing. Supplier's notification shall provide detailed information describing the controls used to mitigate these un-remediated vulnerabilities, risks, or threats.

2. Information Security Incident Management Policy & Procedures Content

Supplier shall establish, document and distribute a formal Security Incident Management Program, which includes the reporting procedure for a Cyber Incident, the requirement of a Supplier Incident Response Team, escalation procedures, and remediation process, and which provides for periodic testing. Any reasonably suspected or confirmed Cyber Incident must be reported to Edison via email to cybersecurity@sce.com immediately for any Cyber Incident relating to a NERC CIP Project or BES Cyber System Information, or CEII, and as soon as possible but in no event more than one business day after Supplier's awareness of any other Cyber Incidents. Notification shall include the nature of the event, date and time of the event, suspected amount of information exposed and steps being taken to investigate the circumstances of the exposure. Supplier will take all necessary steps to eliminate or contain the Cyber Incident and Supplier must cooperate with and assist Edison's Cybersecurity Incident Response Team in the investigation, analysis and resolution of Cyber Incidents, including if requested by Edison, providing breach notifications to individuals and regulatory and law enforcement agencies or providing support to Edison if Edison decides to send out such notices. Supplier shall provide Edison with details of the investigation and final disposition of the Cyber Incident relevant to the services provided to Edison or which may impact the confidentiality, integrity, or availability of those services.

J. Subpoenas for Edison Data

Unless prohibited by law or court order, Supplier shall, within two (2) business days of receipt of a subpoena for disclosure of any Edison Data, provide written notice to Edison pursuant to the notices section of the applicable agreement so that Edison and Supplier may engage in good faith discussions about the appropriate response to the subpoena. If Edison informs Supplier that it will seek to quash or modify the subpoena, then Supplier shall delay responding to the subpoena to permit Edison time to quash or modify the subpoena. If requested by Edison, Supplier shall within fifteen business days of receiving the request confirm whether it received

any subpoena for Edison Data within the prior twelve months and the date and scope of all such subpoenas. Nothing in this Cyber Policy is intended to preclude Supplier from complying with the subpoena when and as required to do so by law or court order.

K. Changes to this Policy

If either Supplier or Edison becomes aware of any changes to the law related to the subject matter of this Cyber Policy, then that Party shall notify the other Party of the change, and the Parties shall meet in good faith as soon as practicable to discuss achieving compliance with the changed legal requirements. Supplier acknowledges that Edison may revise, modify, or replace this policy from time to time in its sole discretion. Following written notice from Edison of any change to this policy, Supplier may be asked to execute and return an amendment to the applicable agreement in which Supplier warrants that it will comply with the new policy. Supplier acknowledges that if it elects not to execute the amendment (1) it will continue to be obligated to comply with the version of the policy in effect at the time the relevant Purchase Order was executed; and (2) it may not be considered for additional work.

ATTACHMENT 1 – Computing Systems Use Acknowledgement For Non-SCE Personnel

Computing Systems Use Acknowledgement
For Non-SCE Personnel

As a condition of granting use of its **telecommunications, computing and information systems**, including, but not limited to, computers, servers, applications, files, electronic mail, instant messaging services, electronic equipment, wireless devices, data resources, and SCE-sponsored connections to the Internet communications network (collectively, "SCE Computing Systems"), Southern California Edison (SCE) requires that each individual read, understand and acknowledge by signing, this Computing Systems Use Acknowledgement (CSUA).

1. SCE grants you access to SCE Computing Systems and related resources solely so you can perform SCE-related business, and access and transmit/receive business-related information.
2. You will not use SCE Computing Systems in a manner that disrupts SCE business, is offensive to others, or violates SCE's Equal Opportunity or Sexual Harassment policies.
3. You will not: • Store or use unapproved software on SCE Computing Systems. • Disclose, share with, or allow another to use your IDs, passwords and dial-up numbers, except as required by authorized IT personnel to resolve technical issues. • Knowingly introduce illegal or destructive code into SCE Computing Systems. • Copy, transfer or sell SCE-developed or licensed software, data, information or documentation to unauthorized systems or destinations. • Employ unapproved data encryption schemes on SCE Computing Systems. • Install SCE-licensed software on any device not owned or approved for such installation by SCE. • Store confidential SCE data or information on any unauthorized device or media. • Have any unauthorized software, including mobile software, on any portable storage media that is attached to SCE Computing Systems. • Install unauthorized hardware or software on SCE-owned equipment (including wireless devices).
4. You should be aware that SCE continuously monitors activities on SCE Computing Systems. Security monitoring extends to personal or other non-SCE devices or media while they are attached to SCE Computing Systems. Monitoring can include all information and communications stored, transiting or that has transited thereon, including erased or deleted files that may still be recovered by SCE and communications stored by a third party for which you are the sender or intended recipient, whether protected by SCE-assigned or personally-selected passwords. SCE may remove any material stored on SCE Computing Systems that it deems offensive or inappropriate. By using SCE Computing Systems, you consent to such monitoring. You should have no expectation of privacy when using SCE Computing Systems or personal or non-SCE devices or media attached to SCE Computing Systems.
5. Remote connections to SCE Computing Systems require authorization and an SCE assigned VPN token or SCE authorized remote access software on a computer/tablet/laptop/cell phone that has up to date antivirus capability and that is allowed under your employer's contract with SCE or is otherwise authorized by SCE.
6. Violations of SCE policies or this CSUA may lead to loss of access privileges and could result in SCE terminating its business relationship with your employer. SCE will report unlawful activities to the appropriate enforcement/regulatory agencies.

I have received and read this acknowledgement.

Signed: _____ Date: _____

Printed Name (Last, First, Middle Initial): _____