VEIC

VENDOR INFORMATION SECURITY REQUIREMENTS

Vermont Energy Investment Corporation and its individual operating companies, divisions, subsidiaries and affiliates (collectively, "VEIC") must ensure that access to its information systems, networks, facilities and other resources (collectively, "VEIC Systems") and its data is appropriately controlled and that these resources are adequately protected. This includes access by vendors, other third parties and their respective employees, agents, subcontractors and representatives (collectively, "Vendors" and each individually, a "Vendor").

This Vendor Information Security Requirements document (this "VISR") sets forth the obligations that apply to Vendors that receive access to (i) VEIC Systems, (ii) VEIC Data (as defined below) and/or (iii) VEIC premises in connection with receipt of access to VEIC Systems and/or VEIC Data, when engaged in business with any VEIC entity (such entity, "Company"). This VISR supplements the terms and conditions set out in any agreement between Company and Vendor to which this VISR is attached or that otherwise incorporates this VISR by reference (the "Agreement"). VEIC Systems and VEIC Data are confidential information of VEIC. For purposes of this VISR, "VEIC Data" means personally identifiable information / personal information of VEIC's customers or associates, protected health information, payment card information, and any other confidential or restricted information or data of VEIC that if disclosed to the public or unauthorized parties (including competitors) is likely to cause significant harm or competitive disadvantage to VEIC (e.g., trade secrets, marketing plans, financial information, budgets, IP (internet protocol) addresses and IP ranges, strategic plans, employee compensation and performance information).

1. General Obligations

If Vendor is provided with access to VEIC Data or VEIC Systems as part of its engagement with Company, Vendor shall for the entire duration of the engagement:

a) maintain at all times a comprehensive and formally documented information security program that:

1. is based on a reputable information security standard;
2. complies with applicable laws and regulations and;
3. includes appropriate administrative, technical, physical, organizational and operational safeguards and other security measures designed to:
4. establish minimum required standards related to the safeguarding of Vendor data and VEIC Data contained in both paper and electronic records;
5. protect the security and confidentiality of Vendor data and VEIC Data in a manner consistent with applicable industry standards;
6. protect against any anticipated threats or hazards to the security or integrity of Vendor data and VEIC Data; and
7. protect against unauthorized processing, loss, use, disclosure or acquisition of or access to any Vendor data or VEIC Data; and upon Company's request, provide a summary or overview of this security program and/or a written confirmation that an assessment of Vendor's information security program has been conducted by an independent assessor and that any discovered program deficiencies have been remediated;

b) cooperate with security audits/assessments/testing as may be periodically requested by Company (and no more than annually unless a problem is identified) upon prior written notice to Vendor, to be performed by or on behalf of Company to confirm Vendor's compliance with this VISR; provided that such audits/assessments shall be conducted at a time(s) mutually agreed by the parties, during Vendor's normal business operations, in a manner minimally disruptive to Vendor's business, and subject to reasonable confidentiality requirements consistent with the confidentiality provisions in the Agreement);

c) ensure that Vendor personnel or representatives that receive access to VEIC Data are competent, properly trained in information security matters and understand Vendor's obligations under this VISR;

d) ensure that Vendor personnel are assigned unique authentication credentials, such as user names, passwords, digital certificates, tokens and smartcards, for access to VEIC Data, and that these credentials are handled with the utmost care and confidentiality to prevent unauthorized disclosure or misuse;

e) ensure that, unless expressly authorized in writing by Company, no VEIC Data shall be permanently stored on laptops that are not equipped with full hard drive encryption, and that no VEIC Data is stored on or accessed by USB drives, mobile devices, or any other portable storage media belonging to Vendor or Vendor personnel;

f) grant access to VEIC Data only on a need to know basis, and not distribute such VEIC Data outside the purpose of the engagement;

g) have effective and up-to-date endpoint protection in place, which includes capabilities for dynamic exploit protection, dynamic malware protection, mitigation, remediation and forensics, on all Vendor systems that are used to access VEIC Data;

h) upon termination of the engagement, upon request of Company, or at any such other time as may be required by applicable law, securely return, securely destroy or render unreadable or undecipherable all VEIC Data provided to Vendor that remains in Vendor's possession or control, and provide Company with a written certification that such return or alternate action has occurred;

i) notify Company of any unauthorized use of, disclosure of, or access to VEIC Systems or VEIC Data, or any failure to comply with this VISR, promptly and in no event more than twenty-four (24) hours after Vendor confirms such prohibited activity and shall cooperate with Company in taking necessary or advisable corrective actions.

j) handle all Confidential Information in accordance with all applicable laws and contractual obligations. In the event that the Vendor, pursuant to applicable law or regulation or legal process, is requested or required to disclose VEIC Data, the Vendor shall provide the Company with prompt notice of such requirement in order to enable the Vendor to confer with the Company concerning the steps that may be taken to reduce the extent of VEIC Data that must be disclosed and/or to enable the Company to seek an appropriate protective order or other remedy reducing the extent of VEIC Data that must be disclosed. In any event, the Vendor shall disclose only such VEIC Data that the Vendor is advised by legal counsel is legally required to be disclosed in order to comply with such applicable law or regulation or legal process (as such may be affected by any protective order or other remedy obtained by the Company) and shall use reasonable efforts to ensure that all VEIC Data is so disclosed will be accorded confidential treatment.

2. Access to VEIC Systems

Compliance with this section of the VISR is required for the entire duration of the engagement if Vendor is provided access to VEIC Systems. In these situations, Vendor shall:

a) ensure that requests to grant Vendor access to VEIC Systems follow approved, formal processes and adhere to the "least privileged access principle" (i.e., access to information resources must be limited to only those individuals whose job requires such access, and access to information resources must be prevented unless explicitly allowed);
b) ensure that all remote access to VEIC Data by Vendor personnel or representatives is secured using multi factor authentication via a secure method or another authentication mechanism as agreed upon with VEIC;
c) ensure that Vendor personnel shall not attempt to gain access to any VEIC Systems that are not specifically related to fulfilling the purpose of the engagement;
d) ensure that system access provided to Vendor personnel is promptly terminated (i) upon termination of the engagement with Vendor, (ii) when Vendor personnel change functions and no longer require access, (iii) when Vendor personnel are no longer assigned to Company's account or, (iv) when for any reason, access is no longer required; and
e) accept and agree that, if and while Vendor personnel are using any VEIC Systems, system activity (e.g. system events, unauthorized log-in attempts or unauthorized transmissions of confidential information) may be subject to monitoring, to protect Company information assets, to the extent allowed by law and pursuant to all reasonable security instructions and VEIC policies or guidelines.

3. Access to VEIC Premises

Compliance with this section of the VISR is required for the entire duration of the engagement if Vendor is provided physical access to any non-public areas in Company's location or premises and receive access to VEIC Systems or VEIC Data. In these situations, Vendor shall and shall ensure that Vendor personnel will:

a) comply with guidance and policies provided by the Company, verbally or in writing, with regard to building safety and security, while working on site at Company's premises;
b) not attempt to gain access to any Company facilities or areas within those facilities that are not specifically related to fulfilling the purpose of the engagement;
c) treat security and identification devices (such as access badges) provided to them by Company with the utmost care and confidentiality to prevent unauthorized access;
d) ensure that Vendor personnel shall have available a valid photo ID at all times while on Company premises and shall present such identification upon request of Company personnel; and
e) refrain from interfering with VEIC's network and infrastructure or causing any damage or threat to such network and infrastructure.

4. Housing Services, Hosting Services and Cloud Services

Compliance with this section of the VISR is required for the entire duration of the engagement if Vendor provides facilities that host Company infrastructure (e.g., data centers), provides facilities and infrastructure for Company to manage and store its data, provides facilities and infrastructure to host supplier-provided IT solutions, or provides professional services that support the deployment and ongoing management of externally-hosted (not within Company facilities) information resources. If Vendor is providing any of these services to Company, Vendor shall:

a) comply with the SOC2 control framework and regulations, or a similar control framework with at least an equal security standard;
b) periodically provide Company (at least annually) with an unqualified SOC 2 (Type II) examination in accordance with the AICPA AT Section 101, or any successor or equivalent standards, by qualified, independent auditors engaged and compensated by Vendor, covering Vendor's controls and systems relating specifically to all aspects of the services provided ("SOC 2 Report"); and
c) provide security operational integration such as logs, monitoring and remediation, for integration with VEIC's SOC requirements.
d) ensure that all confidential data is encrypted in transit and at rest.

5. Developing or Maintaining Software

Compliance with this section of the VISR is required for the entire duration of the engagement if Vendor develops and/or maintains software for Company as part of the engagement. In these situations, Vendor shall:

a) maintain a secure Systems Development Life Cycle (or "SDLC") process, including at a minimum:
    1. evidence of a secure code review process;
    2. periodic application penetration test executed by a specialized third party;
    3. a procedure that results in timely resolution of all discovered high and medium risk vulnerabilities (using the Common Vulnerability Scoring System (or "CVSS"); and
    4. a security checkpoint in change management.
    5. if a web/internet-based application – ensure staff is trained on, and adhere to secure coding principles described in OWASP Secure Coding Guidelines that covers, but not limited to:
        i. input validation
        ii. output encoding
        iii. authentication and password management
        iv. session management
        v. access control
        vi. cryptographic practices
        vii. error handling and logging
        viii. data protection
        ix. communication security
        x. file management
        xi. memory management
        xii. general coding practices
b) apply the following measures in accordance with industry best practices:

1. patch management;
2. vulnerability assessment;
3. strong access control;
4. logging; and
5. system hardening.

c) provide to Company, upon request (in the event of an incident or no more than annually), evidence that periodic application penetration tests are performed and discovered vulnerabilities are remediated; and

d) periodically (no more than annually) provide Company with an ISO, SOC2 Type II or Type III, or similar certification reflecting the compliance of Vendor with the above obligations.

6. Maintaining Hardware

Compliance with this section of the VISR is required for the entire duration of the engagement if Vendor maintains hardware for Company as part of the engagement. In these situations, Vendor shall apply the following measures with respect to the hardware and peripherals it provides and/or maintains:

a) hardware hardening according to industry best-practices or VEIC instructions; and

industry standard-based security or prevention measures (anti-tampering, air gapping etc.).

7. Privileged Access

Compliance with this section of the VISR is required for the entire duration of the engagement if Vendor (i) manages IT systems (hardware or software) for VEIC or (ii) is responsible for any aspect of Identity and Access Management (IAM) related to VEIC systems, including Privileged Access controls. For purposes of clarity, this Section 7 will apply only if Vendor is providing services pursuant to Sections 4, 5 or 6 above. "Privileged Access" is defined as access that provides a capability to alter the properties, behavior, or control of an information resource, change system control parameters, alter other users' access to data, or bypass or change system and security controls. In these situations, Vendor shall:

a) Maintain and disseminate to Vendor employees a written access control policy based on reputable industry standards and the least privileged access principle.

b) Include formal instructions for the following in Vendor's IAM procedures:
   1. Approval for, creation of and providing entitlements for privileged accounts;
   2. Removal of Privileged Access upon termination of the engagement with Vendor, when Vendor personnel change functions and no longer require access, when Vendor personnel are no longer assigned to the VEIC account or, for any reason, Privileged Access is no longer required.

c) Maintain a recertification cycle (validation of permissions granted) for privileged accounts that includes:
   1. Maintaining a list of Vendor personnel with Privileged Access to VEIC Systems or other IT resources that support VEIC Systems or operations;
   2. Reviewing Vendor personnel's access rights at regular intervals (at least quarterly) and after any changes, such as promotion, demotion, or termination of employment;
   3. Taking immediate action to correct any discrepancies discovered during this review; and

4. Upon request by Company, providing reporting related to this review.

d) Monitor and adequately log creation of and changes to privileged accounts for systems used by, accessed by, or in-place to support Company and, upon discovery of anomalies, notify Company.

e) Monitor and adequately log all actions performed by Vendor personnel with Privileged Access to systems used by, accessed by or in-place to support Company, report any anomalies to Company and, upon request, provide a history of all system management actions performed by Vendor personnel that could impact the confidentiality, integrity or availability of services or systems.

f) Implement procedures for emergency access (e.g., a “break glass” account) and ensure that passwords are properly secured and changed after each use.

g) Ensure that all Vendor personnel (including technical and functional support personnel, operators, network administrators, system programmers, and database administrators) have an individually-assigned unique identifier (user ID) that can be traced to the accountable individual.

h) Implement controls to ensure secure log-on procedures, quality passwords, a secure authentication method, and session time-outs for inactive sessions at the network, operating system and database level.

i) Ensure that non-personal accounts (e.g., Admin or Root, service accounts, batch accounts, and back-up accounts) cannot be used by an individual for system access.

j) Where technically feasible, integrate solutions provided by Vendor with the VEIC privileged access management (PAM) solution.