Brunel Energy, Inc.

Cyber Security Policy

Contents

1. Purpose

1.1. Brunel Energy, Inc., hereinafter referred to as, "the Company," has established a program intended to create effective administrative, technical, electronic, and physical protections to safeguard the personal information of the Company's clients and employees.

1.2. The Company's proprietary and confidential information, the physical security of our premises, and the integrity of our electronic systems so that they are best positioned to function smoothly without interruption.

2. Applicability

2.1. This policy applies to employees, subcontractors and/or visitor(s) of the Company. For the purposes of this policy, an employee shall be considered on the job whenever he/she is:

2.1.1. On or in, any Company or client property, including parking areas; or

2.1.2. On Company time even if off Company premises (including paid lunch, rest periods and periods of being on call).

2.2. As a condition of employment, Company employees are required to abide by additional governmental or customer policies and requirements that may be imposed at a worksite in addition to the requirements of these policies and procedures. Nothing set forth in this policy constitutes, construes, or interprets in any way as a contract of employment.

3. Definitions

3.1. ***Policy*** refers to the Information Security Policy.

3.2. ***Clients*** refers to the companies' clients, former and prospective clients

3.3. ***Information System*** means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

3.4. ***Nonpublic Information*** is all electronic information that is not Publicly Available Information and is:

3.4.1. Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access, or use of which, would cause a material adverse impact to the business, operations, or security of the Covered Entity.

3.4.2. Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements:

3.4.2.1. social security number

3.4.2.2. drivers' license number or non-driver identification card number

3.4.2.3. account number, credit, or debit card number,

3.4.2.4. any security code, access code or password that would permit access to an individual's financial account, or

3.4.2.5. biometric records.

3.4.3. Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.

3.5. ***Passwords*** are a string of characters that, when possible, is at least 8 characters long and contains at least three of the following: upper case letter, lower case letter, a number, a special character (%, & #, etc.).

3.6. ***Person*** means any individual or non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency, or association.

3.7. ***Third Party Service Providers*** is a person that is not an affiliate of the Company that provides services to the Company and maintains, processes or is otherwise permitted access to Nonpublic Information through its provision of services to the Company.

4. Responsibilities

4.1. Management:

4.1.1. Is responsible for implementing, training, supporting, and enforcing the requirements of this Procedure in their locations.

4.1.2. Reviewing the security measures in this Policy annually or when there is a change in applicable laws or regulations or in business activities of Agency; and conducting training as necessary for all Company employees with access to Nonpublic Information.

4.1.3. Implementing policies and procedures to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers.

4.2. Employee(s):

4.2.1. Are responsible for attending all assigned cyber security training and complying with the procedures that are required for their location.

5. Data Governance and Classification

5.1. Special protection for nonpublic information

5.1.1. Nonpublic Information is to be accorded the highest level of confidentiality

by the Company and employees.

5.1.2. Examples of Nonpublic Information include, but are not limited to - first name and last name, or first initial and last name, and any one or more of the following:

5.1.2.1. Social Security number.

5.1.2.2. Driver's license number, passport number, or state-issued identification card number.

5.1.2.3. Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password.

5.1.2.4. Personal or protected health information.

5.1.2.5. Biometric records.

5.1.3. The information listed above, even if it is not connected with a name, should each be treated as Nonpublic Information.

5.2. Where Nonpublic Information is Stored

5.2.1. The Company and its employees recognize that the Company possesses Nonpublic Information in the following places, whether in the Company's premises or off site, and whether created or maintained by Company or third parties on behalf of Company:

5.2.1.1. Hard copy and electronic files on Clients and employees, located at desks, in file drawers, storage areas and on the Company's Systems

5.2.1.2. Personnel files, Form I-9s, benefits information, payroll information, and direct deposit information for employees wherever located, including but not limited to hard copies at desks, in file drawers and other storage areas, and in electronic form on the Company's Systems

5.2.1.3. Off-site back-ups, in any form.

5.2.1.4. Third Party Service Providers entrusted with Nonpublic Information from the Company.

5.2.2. This Policy is intended to protect Nonpublic Information possessed by the Company from unauthorized access, dissemination and/or use.

5.2.3. Nonpublic Information may not be disseminated, communicated, or stored on or through any social media websites or services, at any time or for any reason.

5.2.4. Employees will adhere to the Company document retention schedule and requirements. When it is appropriate to destroy Company records, paper and electronic records containing Nonpublic Information must be destroyed in a manner in which they cannot be read or reconstructed.

5.2.5. Unless otherwise directed by the Information Security Coordinator, a commercial shredding Company will be used to destroy paper documents.

When computers, digital copiers, scanners and/or printers with electronic storage capacity, or portable electronic devices and media are discarded, such disposal should be coordinated with the Information Security Coordinator, and care needs to be taken to ensure that the hard drives or other storage media are destroyed in a manner that all data becomes unreadable.

6. Asset Inventory and Device Management

6.1. Employees should keep mobile electronic communications devices (such as PDAs, smart phones, etc.) with access to Nonpublic Information in their possession or in a secured location at all times, and Employees will not share passwords or other access information with others.

6.2. Employees will not put any Company data on thumb drives, laptops or other portable media, drives and devices unless authorized by the Company. If so authorized, the thumb drives, laptops or other portable media, drives and devices should be password-protected and encrypted, and the portable mobile electronic communications devices and laptops should be password-protected and encrypted.

6.3. Employees that no longer work for the Company must: (1) return to Company all Company information (including, but not limited to, any Nonpublic Information) in any form, whether stored on computers, laptops, portable devices, electronic media, or in files, records, work papers, cloud- or web-based storage, etc.; (2) return all keys, IDs, access codes and/or badges; and (3) not access Nonpublic Agency information (including, but not limited to, any Private Information).

6.4. In accordance with the Company's human resources manual, access by the former employee to Company email and voice mail accounts can be immediately disabled and access transferred to other Company staff to assure a continuity of work, and inactivated when determined appropriate by Company.

6.5. Employees are required to report all actual or potential unauthorized access to, use of or disclosure of Nonpublic Information to the Information Security Coordinator.

7. Asset Controls and Identity Management

7.1. Internal Controls

7.1.1. Company computers will require a user ID and password and Company mobile devices should require a password (and be encrypted, if reasonably feasible). Employee log-ins and passwords should be appropriately strong (with the minimum number of characters and other elements required by the Company's Systems). Each employee will be required to have their own user name and password.

7.1.2. Electronic files containing Nonpublic Information will not be left accessible to others, such as on computers or portable storage devices accessible

(e.g., computer screens must be locked when an employee using such files leaves his or her computer, even briefly). Paper and electronic files must not be removed from Company premises or accessed remotely unless specific authorization has been provided in advance, and then, the security of that Nonpublic Information must be maintained.

7.1.3. Employees are expected to log off or lock their computers when they leave them unattended (such as when on breaks, at lunch, in a meeting or out of the office). The Company will implement controls to terminate computer sessions and/or lock computers after a predetermined time of inactivity (e.g., 10 minutes).

7.1.4. Employees should not open any email attachment, link, or application where the employee does not reasonably believe the information expected to be accessed is from a trustworthy source. Employees will not use Company equipment to access any application or software not approved by the Company.

7.1.5. To combat internal risks to the security, confidentiality and/or integrity of records containing Nonpublic Information, the following measures will be taken:

7.1.6. The Company will retain only the last four digits of credit card numbers and will not retain bank routing numbers, personal bank account numbers and checks, and all credit- and banking-related information not retained will be destroyed in accordance with applicable law and Company business practices.

7.2. External Controls

7.2.1. In addition to the measures taken to combat internal risks, the following measures will be taken to minimize external risks to the security, confidentiality and/or integrity of records containing Nonpublic Information:

7.2.1.1. Visitors will be escorted within the office and will not have access to Company computers or property that may contain Nonpublic Information. Guests' wireless access should be fire-walled (off) from the Company's Systems.

7.2.1.2. The Company will maintain security measures so that its wireless networks cannot be accessed remotely by the public.

7.2.1.3. Servers and other equipment at the Company's premises containing Nonpublic Information will be maintained in a secure location.

8. Systems and Network Security, Operations and Availability

8.1. The Company will employ an email filter (hardware, software, or third-party provided) that works to restrict and eliminate viruses, spyware, and other malware before getting to the Company desktop and portable computers.

8.2. The Company will maintain up-to-date network and firewall protection and operating system security patches on its Systems, servers and desktop and laptop computers, as well as other security measures deemed appropriate.

8.3. The Company will maintain security software, which includes malware protection with up-to-date patches and virus definitions, on its Systems and its servers, desktop and laptop computers, and all mobile devices, which is updated as frequently as possible, but at least daily.

8.4. All back-ups will be password-protected and encrypted and kept in a secured location off site.

8.5. Company employees should use care in communications (e.g., outgoing email and attachments) to ensure: first, that the Nonpublic Information needs to be sent by email and, if so, that it is transmitted using secure email in accordance with Company policy.

8.6. The Company will create a secure SSL tunnel between its website and the consumer before allowing the consumer to enter any Nonpublic Information or to enter a password.

8.7. When an employee accesses Company Systems and/or Nonpublic Information from a remote location, the Company's secure SSL connection must be used (such as Virtual Private Network (VPN), GoToMyPC, LogMeIn).

8.8. Employees should not access Company Systems or Nonpublic Information using non-Company equipment (e.g., a home computer) unless authorized by the Agency and provided with appropriate firewalls and virus protection and done through the Company's secure SSL connection. Employees will not store any Nonpublic Information on any non-company equipment.

9. Systems and Network Monitoring

9.1. The Company will monitor its Systems and equipment for any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System, including but not limited to implementing hardware, software and/or procedural mechanisms to record and report activity for the Systems and equipment.

9.2. The Company will exercise due diligence in making sure third-party service providers that are provided Nonpublic Information have the requisite security controls and written policy in place, provide the Company a written commitment to safeguard and store Nonpublic Information with at least the same level of security controls as the Company maintains (as outlined in this Policy), and advise the Company as to any actual, suspected or potential breaches of Private

Information.

10. Business Continuity and Disaster Recovery

10.1. A security breach occurs when there is an unauthorized acquisition, dissemination, use or loss of Nonpublic Information. Each employee shall be responsible for notifying the Information Security Coordinator whenever he or she learns that there has been or may have been a security breach that may have compromised Nonpublic Information or other company information about Clients, employees or company business.

10.2. The Company will take the following actions in the event of a security breach:

10.2.1. assess the security breach.

10.2.2. consult counsel.

10.2.3. review the requirements of the applicable state laws and regulations

10.2.4. notify the carriers whose policyholders insured through the Company may have been affected by the event

10.2.5. notify the carrier for the Company's cybersecurity coverage

10.2.6. notify individuals, regulatory and law enforcement authorities (if and as required and further as deemed appropriate by Company management)

10.2.7. take and document corrective actions to contain and control the problem.

10.2.8. identify who will address any media inquiries.

10.2.9. draft the content of all communications regarding the event for potentially affected individuals.

11. Training

11.1. Employees will receive Cyber security training upon initial hire and annually thereafter.

11.2. The training will include security awareness and the need for operations security. Supplies will be provided inscribed with security reminders, i.e., Email advisories, notices from senior organizational officials, displaying logon screen messages and conducting security awareness events. Practical exercises may include for example, no-notice social engineering attempts to collection information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking via spear phishing attacks, malicious web link.