Written Information Security Program (W.I.S.P.)

Policy Statement:

The Written Information Security Program ("WISP") in regards to Clambake, Inc., DBA Lobster Pot at 321 Commercial Street, Provincetown, MA 02657 is intended as a set of comprehensive guidelines and policies designed to safeguard all confidential and restricted data and comply with applicable laws and regulations on the protection of Personal Information and Nonpublic Financial Information.

The objective is to create effective administrative, technical and physical safeguards that are appropriate to the size, scope and type of our business, the amount of resources available to our business, the amount of Personal Information (PI) stored (electronically and physically), and the need for security and confidentiality of both consumer and employee information, as well as to comply with obligations under 201 CMR 17.00.

Person(s) In Charge (PIC):

Mike Potenza
321 Commercial Street
Provincetown, MA 02657
508-487-0842
mpotenza@ptownlobsterpot.com

Walt Winnowski
321 Commercial Street
Provincetown, MA 02657
508-487-0842
walt@ptownlobsterpot.com

Overview & Purpose:

The WISP was implemented to comply with regulations issued by the Commonwealth of Massachusetts entitled "Standards For The Protection Of Personal Information Of Residents Of The Commonwealth" [201 Code Mass. Regs. 17.00], and by the Federal Trade Commission [16 CFR Part 314], and with our obligations under the financial customer information security provisions of the federal Gramm-Leach-Bliley Act ("GLB") [15 USC 6801(b) and 6805(b)(2)].

In accordance with these federal and state laws and regulations, Clambake, Inc. DBA Lobster Pot is required to take measures to safeguard personally identifiable information, including financial information, and to provide notice about security breaches of protected information to affected individuals and appropriate state agencies.

For purposes of this WISP, "personal information (PI)" means a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account.

Scope:

The scope of information security encompasses the protection of the confidentiality, integrity and availability of company information including the PI of management and staff. This program applies to all Clambake, Inc. employees, whether full or part-time. It also applies to certain contracted third-party vendors as required. The data covered includes any information stored, accessed or collected by Clambake, Inc.

The WISP is not intended to supercede any existing policy that contains more specific requirements for safeguarding certain types of data, except in the case of PI and Nonpublic Financial Information. If such policy exists and is in conflict with the requirements of the WISP, the other policy takes precedence.

A thorough analysis of all Clambake, Inc. information networks and systems will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information. The analysis will determine the types of threats - external or external, natural or manmade, electronic and non-electronic - that affect the ability to manage the information resource. The analysis will also document the existing vulnerabilities which potentially expose the information resource to threats. Finally, the analysis will also include an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.

Based on the periodic assessment, measures will be implemented that reduce the impact of threats by reducing the amount and the scope of the vulnerabilities.

Policies for Safeguarding Confidential Data:

It is the policy of Clambake, Inc. that information in all its forms—written, spoken, recorded electronically or printed—will be protected from accidental or intentional unauthorized modification, destruction or disclosure through its life cycle. This protecting includes the appropriate level of security over the equipment and software used to process, store and transmit that information.

All policies and procedures are documented and made available to individuals responsible for their implementation and compliance. All documentation, which may be in electronic form, must be retained for at least six years after initial creation, or, pertaining to policies and procedures, after changes are made. All documentation must be periodically reviewed for appropriateness and currency.

All systems implemented after the effective date of these policies are expected to comply with the provisions of this policy where possible Existing systems are expected to be brought into compliance where possible as soon as is practical.

To protect data classified as Confidential, the following policies and procedures have been developed that relate to access, storage, transportation and destruction of records:

Some Personal Information (PI) is found on paper records and files that are maintained at employees' desks for the period of time that the corresponding accounts are being worked.

Some additional (paper) files and documents are kept in locked filing cabinets. Keys are kept in concealed office location(s). Managers deemed to have a true, business-related need have physical access to the filing cabinets that contain PI.

PI is also found in an electronic format in the company server system and other computers. All employees that require access have a unique user ID and password for systems that contain PI, and security permissions are set to restrict access to employee data to management only.

PI can also transmitted via email during the course of normal operations. Internally, systems are password protected. On laptops, transmission of PI is protected by password to the device and any documents are only stored temporarily and protected by passwords for each document.

Access & Storage:

Only those employees or authorized third parties requiring access to Confidential data in the regular course of their duties are granted access to this data, including both physical and electronic records.

To the extent possible, all electronic records containing Confidential data should not be stored on local machines or unsecured servers. PI must not be stored on cloud-based storage solutions that are unsupported.

Members of the Community are strongly discouraged from storing Confidential data on laptops or on other mobile devices (e.g., flash drives, smart phones, external hard drives). However, if it is necessary to transport Confidential data electronically, the mobile device containing the data must be encrypted.

Upon termination of employment or relationship with Clambake, Inc., electronic and physical access to documents, systems or other network resources containing Confidential data is immediately terminated.

Standards for Disposal of Records:

Massachusetts General Law 93I states that when disposing of records, each agency or person shall meet the following minimum standards for proper disposal of records containing personal information:

(a) paper documents containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed;

(b) electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.

Computer System Safeguards:

Records containing Confidential data must be destroyed once they are no longer needed for business purposes, unless state or federal regulations require maintaining these records for a prescribed period of time.

Clambake, Inc. PIC staff monitor and assess safeguards on an ongoing basis to determine when enhancements are required. Clambake, Inc. has implemented the following to combat external risk and secure systems containing Confidential Data:

Secure user authentication protocols:
(a) Unique passwords are required for all user accounts; each employee receives an individual user account.

(b) Server accounts are locked after multiple unsuccessful password attempts.

(c) Computer access passwords are disabled upon an employee's termination.

(d) User passwords are stored in an encrypted format; root passwords are only accessible by system administrators.

(e) Financial Data is transmitted with TrustWave protection to defend in real time against advanced threats . TrustWave also monitors, uncovers and responds to malicious activity and indicators of compromise, particularly around endpoints. The system is also to test and patch vulnerabilities, especially in remote access software and point-of-sale systems.

Enforcement:

Any employee who willfully accesses, discloses, misuses, alters, destroys, or otherwise compromises Confidential or Restricted data without authorization, or who fails to comply with this Program in any other respect, will be subject to disciplinary action, which may include termination in the case of employees

Effective Date:

This Written Information Security Program was implemented January 1, 2019. Revisions: May 2019, June 2019. Clambake, Inc. will review this Program at least annually and reserves the right to change, modify, or otherwise alter this Program at its sole discretion and at any time as it deems circumstances warrant.

Transporting Confidential Data:

Members of the Clambake, Inc. community are strongly discouraged from removing records containing Confidential data. In rare cases where it is necessary to do so, the user must take all reasonable precautions to safeguard the data. Under no circumstances are documents, electronic devices, or digital media containing Confidential data to be left unattended in any unsecured location.

When there is a legitimate need to provide records containing Confidential data to a third party, electronic records shall be password-protected and/or encrypted, and paper records shall be marked confidential and securely sealed.

Notice To Employees:

An electronic copy of the WISP will be distributed to each employee, and new employees, who shall, upon receipt of the WISP, acknowledge that he/she has received a copy of the WISP. There will be immediate training and annual retraining of employees on the detailed provisions of the WISP as the Program evolves.

All employees are required to comply with the provisions of this WISP, and are prohibited from using personal information in any nonconforming manner during or after employment. Mandatory counseling and/or disciplinary action will be taken for violations of the security provisions of the WISP taking into account the nature of the violation and the nature of the personal information affected by the violation. A portion of employees' performance evaluations will be based on the adherence to the provisions of this WISP.

Employees are prohibited from removing files, records or documents that contain PI from the building. The only allowable use of said files, records or documents will be in an electronic format on an encrypted and approved portable device as noted below in the External Risks & Threats section.

Such terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the premises or information. Moreover, such terminated employee's remote electronic access to PI must be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated.

Employees are required to report any suspicious or unauthorized use of PI. Whenever there is an incident that requires notification under M.G.L. c. 93H, §3, there shall be an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in our security practices are required to improve the security of PI for which the business is responsible.

External Risks & Threats:

System security agent software which includes malware protection, patches and virus definitions, is installed on all systems processing PI. This software is updated daily automatically (and manually when needed) on all systems.

All records and files transmitted across public networks (e.g., via email) or wirelessly, must also be, to the extent technically feasible, encrypted. Encryption here means the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by regulation by the Office of Consumer Affairs and Business Regulation.

All computer systems will be monitored on a monthly basis for unauthorized use of or access to personal information. Any unauthorized use or access found will be immediately reported. Further, actions will be taken to assess the impact of the unauthorized use/access, appropriate measures will be taken against employees not complying with this WISP, and updates will be made to the safeguards specified in this WISP if needed to prevent future unauthorized access/ use of PI.

Secure user authentication protocols are in place on systems, including (1) protocols for control of user IDs and other identifiers; (2) a reasonably secure method of assigning and selecting passwords; (3) control of data security passwords to ensure that such passwords are kept in a secure location (paper copies in a locked file cabinet or drawer and electronic copies on a password-protected electronic document).

Requirements For Security Breach Notifications:

Pursuant to M.G.L. c. 93H, s. 3(b), if you own or license data that includes personal information of a Massachusetts resident, you are required to provide written notice as soon as practicable and without unreasonable delay to:

The Attorney General (AGO)

The Director of the Office of Consumer Affairs and Business Regulation (OCABR); and
the affected Massachusetts resident when you know or have reason to know (a) of a breach of security; or (b) that personal information of a Massachusetts resident was acquired by or used by an unauthorized person or used for an unauthorized purpose.

The notice to the Attorney General and the Director of Consumer Affairs and Business Regulation shall include, but not be limited to: (1) the nature of the breach of security or the unauthorized acquisition or use; (2) the number of Massachusetts residents affected by such incident at the time of notification; and (3) any steps the person or agency has taken or plans to take relating to the incident.

Notice To Affected Massachusetts Residents:

A person or business that has experienced a breach of security or the unauthorized acquisition or use of personal information of Massachusetts residents must also provide notice to those affected Massachusetts residents. This notice shall include, but not be limited to:

1) The consumer's right to obtain a police report.

2) How a consumer requests a security freeze.

3) The necessary information to be provided when requesting the security freeze.

4) Any fees to be paid to any of the consumer reporting agencies, provided however, that the notification shall not include:
    (a) The nature of the breach or unauthorized acquisition or use; or
    (b) The number of Massachusetts residents affected by the security breach or the unauthorized access or use.