PropEx

Written Information Security Program

I. Introduction

The objective of PropEx in the development and implementation of this **Written Information Security Program ("WISP")** is to create effective administrative, technical, and physical safeguards for the protection of **Personally Identifiable Information ("PII")** of our customers. The WISP sets forth our procedure for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, protecting, and disposing of our customers' PII.

II. Purpose

The purpose of this WISP is to ensure:

1. Confidentiality and security of PII PropEx collects, uses and maintains.
2. Protect against any reasonable threats or hazards to the security, confidentiality, integrity and availability of such information.
3. Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of harm or inconvenience to any of our customers.

III. Scope

In formulating and implementing PropEx's WISP, the intended scope is to do the following:

1. Identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing PII.
2. Assess the potential damage of these threats, taking into consideration the sensitivity of the PII.
3. Evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control identified risks.
4. Design and implement this WISP to place safeguards to minimize those risks, consistent with the requirements of the New York State SHIELD Act, NIST Cybersecurity Framework, Massachusetts 201 CMR 17.00, Canada PIPEDA and PCI-DSS.
5. Regularly monitor the effectiveness of those safeguards.

IV. Definitions

Personally Identifiable Information

Personally Identifiable Information ("PII") means any information that identifies, relates to, describes or is capable of being associated with, a particular individual, including, but not limited to, a name, alias, social security number, address, phone number, e-mail address, driver's license or state identification data.+

Financial Information

Financial Information means any information that would permit access to a person's financial account such as, but not limited to, financial account number, credit or debit card number, with or without any required security code, access code, or personal identification number or password.

V. Roles and Responsibilities

PropEx has designated the Chief Information Officer ("CIO") to provide overall guidance, leadership, and support for the organization's entire incident response platform, while also assisting other applicable personnel in their day-to-day operations. The CIO is mainly to report to other members of senior management on a regular basis regarding all aspects of the organization's information systems posture.

1. Seek approval from Senior Leadership for the administration of the Information Security Program and other policies tied to it.
2. Advise on improvements in the WISP based on the threat environment.

PropEx has designated the Chief Information Security Officer ("CISO") to implement, supervise and maintain the WISP. This designated employee will be responsible for the following:

1. Initial implementation of the WISP.
2. Training of all employees regarding the WISP.
3. Regular testing of the WISP's safeguards.
4. Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in PropEx's business practices that may implicate the security or integrity of records containing PII.
5. Conducting an annual training session for all employees, including all temporary and contract employees who have access to PII on the elements of the WISP. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with our requirements for ensuring the protection of PII.

VI. Policies in the Information Security Program

1. Access Control

The purpose of this policy is to ensure that access controls are implemented and in compliance with IT security policies, standards, and procedures. This policy is applicable to all departments and users of PropEx's resources and assets. The IT Department shall:

a. Identify and select the following types of information system accounts to support organizational missions and business functions: individual, shared, group, system, guest, emergency, developer/manufacturer/vendor, temporary, and service.

b. Authorize access to the information system based on a valid access authorization or intended system usage.

c. Ensure that the information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

d. Separate duties of individuals as necessary, to prevent malevolent activity without collusion.

e. Restrict privileged accounts on the information system to the IT Administrators.

f. Ensure that the information system audits the execution of privileged functions.

g. Enforces a limit of consecutive invalid logon attempts by a user and locks the account automatically until released by an administrator when the enforced limit is exceeded.

h. Ensure that an employee's account is disabled within 7 days of the employee leaving the company.

i. Every individual must have Single Sign-On (SSO) enabled for all possible services and systems in the organization.

j. Every individual must have Multi-Factor Authentication (MFA) enabled for all possible services and systems in the organization.

2. Risk Assessment

To ensure that the IT Department performs risk assessments in compliance with IT security policies, standards, and procedures. The IT Department shall:

a. Conduct (or have conducted by a qualified third-party) an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

b. Document and review the risk assessment results in an annual IT Risk Assessment.

c. Update the risk assessment quarterly or whenever there are significant changes to the information system, identification of new threats and vulnerabilities, or other conditions that may impact the security state of the system.

d. Scan for vulnerabilities in the information system and hosted applications by employing vulnerability scanning tools and techniques quarterly and/or randomly and when new vulnerabilities potentially affecting the system/applications are identified and reported.

e. Analyze vulnerability scan reports and results and remediate legitimate vulnerabilities within one month in accordance with an organizational assessment of risk.

f. Share information obtained from the vulnerability scanning process with the Chief Information Officer.

3. Password Policy

To ensure that all accounts on the information system shall use strong passwords. The IT Department shall ensure that every password:

a. Consists of 12 characters at least.

b. Does not contain any personal information like birth dates, addresses, phone numbers, pets, family members etc.

c. Contains at least 4 special characters.

Employees must ensure that:

a. Passwords are not written down and stored in a way that can potentially be accessed by unauthorized persons.

b. Has not been reused by employees anywhere else for any purpose.

4. Data Storage

To ensure that Information Technology (IT) controls access to and disposes of media resources in compliance with IT security policies, standards, and procedures.

Policies for data in paper form:

a. Information/data which happens to be considered confidential/critical must not be printed out without any prior authorization from the IT department.

b. Any sort of information in physical format should be kept confidential and in a secure location where only authorized personnel can access.

c. No physical data should be left in a way that allows unauthorized access.

d. Any sensitive/critical data on paper must be shredded once no longer required.

Policies for data in electronic form:

a. All the data stored in electronic format must be stored encrypted at rest.

b. Without proper authentication measures no device or endpoint shall have access to the data stored on company's resources.

c. All the credentials of the employees as well as the customers that PropEx's systems have gathered must be stored in encrypted format.

5. Acceptable Encryption

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively.

Policies for Key generation:

a. Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

b. Key generation must be seeded from an industry standard random number generator (RNG).

Policies for Key Agreement and Authentication:

a. Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, or Elliptic curve Diffie-Hellman (ECDH).

b. All servers and applications used for authentication, or using TLS must have installed a valid certificate signed by a known, trusted provider.

Algorithm Requirements:

a. Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents

according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

b. Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

6. Secure Use of Social Media

The primary purpose of this guideline is to provide best practices for the secure use of social media for collaboration and transparency.

a. Use of social media on behalf of an entity or access to social media from entity resources should be at the discretion of executive management.

b. Authorize use of social media after a proper evaluation of risk and demonstration of a justified business need.

c. Do not use the same passwords for social media sites as are used to access entity resources.

d. Do not post any personally identifying information (PII) information on social media sites.

e. Where possible, minimize the posting of information about one's role in an organization, including organizational email addresses, on social media sites.

7. Logging and Monitoring

This policy is applicable to all systems and devices in PropEx's network, resources, and assets. The IT Department shall:

a. Continuous and automated monitoring along with alerting of access and network activity must be implemented.

b. All the systems and networks logs must be audited semi-annually.

c. Information Security Audits must be performed at least annually.

d. IDS/IPS and Firewall must be implemented to avoid unauthorized access along with monitoring the systems.

8. Incident Response Plan

The purpose of this policy is to ensure that Information Technology (IT) properly identifies, contains, investigates, remedies, reports, and responds to cybersecurity events.

a. TableTop exercises must be conducted annually to find the gaps in the Incident Response Plan and updates must be implemented both in the infrastructure as well as in the Plan.
b. All the suspicious activity in any of the company's systems must be reported to a specific ticket generating portal or email address, further a required personnel to report suspected security incidents to the incident response capability within 72 hours.
c. For any other relevant information please refer to PropEx Incident Response Plan- https://docs.google.com/document/d/1tPOi6qMmXBT5xEal9wVuJDnYF-iaFgwGWrvvp8UkWJ4/edit

9. Breach Notification

The purpose of this policy.

a. As soon as a theft, data breach or exposure containing PropEx's Protected data or PropEx's Sensitive data is identified, the process of removing all access to that resource will begin.

b. Breach notifications to all parties must be implemented within 72 hours of the identification of the breach.

c. In the event of the breach, the following information must be conveyed to the consumers and the regulatory authorities:

    i. The date of the breach and the date of discovery.
    ii. Recommendations to consumers to mitigate the effects of the breach.
    iii. Contact information of the customer support team to the consumers and of the liaison to the regulators.

d. For more information refer to PropEx's Data Breach Notification Policy - https://docs.google.com/document/d/1FLMVhPT_-_KVLO_NR0WaDO3ObvXeWfoZa3ihZ1TnGhs/edit

VII. Revision History