Published on *OASIS* (https://www.oasis-open.org)

Information Security Policy

Description:
Governing the operational procedures taken to securely store Personal Information and the requirements for reporting any security breach.

I. OBJECTIVE:

Our objective, in the development and implementation of this Information Security Policy ("ISP"), is to create effective administrative, technical and physical safeguards for the protection of Personal Information of OASIS members and employees and the prevention of unauthorized access, use or dissemination of Personal Information.

II. PERSONAL INFORMATION:

For purposes of this ISP, "Personal Information" means a person's first name/given name and last name/family name or first initial and last name/family name in combination with any one or more of the following data elements that relate to such person: (a) Social Security number or other government issued taxpayer ID; (b) driver's license number or government-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 financial account. "Personal Information" does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

III. PURPOSE:

The purpose of the ISP is to:

a. Ensure the security and confidentiality of Personal Information;
b. Protect against any anticipated threats or hazards to the security or integrity of such information.
c. Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

IV. SCOPE:

Our purpose in formulating and implementing the ISP is to:

1. identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Personal Information;
2. assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of

the Personal Information;

3. evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;
4. design and implement a ISP that puts safeguards in place to minimize those risks; and
5. regularly monitor the effectiveness of those safeguards.

V. RESPONSIBILITY:

We have designated Scott McGrath, COO, as the "Data Security Coordinator" to implement, supervise and maintain the ISP. The "Data Security Coordinator" is responsible for:

a. Implementation of the ISP;
b. Training employees;
c. Regular testing of the ISP's safeguards;
d. Evaluating the ability of each of our third party service providers to implement and maintain appropriate security measures for the Personal Information to which we have permitted them access; and requiring such third party service providers by contract to implement and maintain appropriate security measures;
e. Reviewing the scope of the security measures in the ISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing Personal Information;
f. Conducting an annual training session for all owners, managers, employees and independent contractors, including temporary and contract employees who have access to Personal Information on the elements of the ISP. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with the firm's requirements for ensuring the protection of Personal Information.

VI. Policy:

A. Storage of Information

The amount of Personal Information collected, and the time period for retention, should be limited to that amount reasonably necessary to accomplish OASIS' legitimate business purposes, or necessary for OASIS to comply with other legal requirements.

Physical Records — Records containing Personal Information (as defined above) must be stored in locked facilities, secure storage areas or locked containers.

Electronic Records — To the extent technically feasible, the following security protocols must be implemented:

1. Secure user authentication protocols including:
   a. control of user IDs and other identifiers;
   b. a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;

c. control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;

d. restricting access to active users and active user accounts only; and

e. blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

2. Secure access control measures that:
   a. restrict access to records and files containing Personal Information to those who need such information to perform their job duties; and
   b. assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;

3. Encryption of the following:
   a. all transmitted records and files containing Personal Information that will travel across public networks, and encryption of all data containing Personal Information to be transmitted wirelessly;
   b. all Personal Information stored on laptops or other portable devices;

4. Reasonable monitoring of systems, for unauthorized use of or access to Personal Information;
5. For files containing Personal Information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the Personal Information;
6. Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

B. Access to Information

Access to records containing Personal Information shall be restricted to current employees who are reasonably required to know such information in order to accomplish OASIS' legitimate business purpose or to enable the company to comply with legal requirements.

Records containing Personal Information shall only be removed from a OASIS site with specific authorization from the Data Security Coordinator. Employees who have access to Personal Information will logoff their computers when not in use for an extended period of time. During short periods of inactivity, these employees will lock their computers at the operating system level. Visitors' to OASIS sites where Personal Information is stored shall not be permitted to visit any area of the premises that contains Personal Information unless they are escorted by a OASIS employee. Employees are encouraged to report any suspicious or unauthorized use of Personal Information.

C. Transmission of Information

To the extent technically feasible, all records and files containing Personal Information which are

transmitted across public networks or wirelessly must be encrypted.

Employees are prohibited from keeping open files containing Personal Information on their desks or in their work areas when they are not at their desks. At the end of the work day, all files and other records containing Personal Information must be secured in a manner consistent with this policy.

D. Disposition/Destruction of Information

Paper and electronic records containing Personal Information must be disposed of by shredding or equivalent destruction of paper records and/or destruction or erasure of the physical medium on which data is stored in accordance with OASIS' Document Retention and Destruction Policy available at all OASIS sites.

Terminated employees must return all records containing Personal Information, in any form, which may at the time of such termination be in the former employee's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)

VII. Training

A copy of this ISP will be distributed to each employee, (as well as consultants and vendors as appropriate), who will have access to Personal Information. All such persons shall, upon receipt of the ISP, acknowledge in writing that he/she has received, read and understood the ISP. When the ISP is first issued, there will be training of employees and temporary employees who have access to Personal Information on the detailed provisions of the policy. All employees shall be retrained regularly. All attendees at such training sessions are required to certify their attendance at the training and their familiarity with the company's policy and procedures for the protection of Personal Information.

VIII. Violations

Violations of the policy will be met with disciplinary action up to and including termination of employment. The nature of the disciplinary measures will depend on a number of factors including the nature of the violation. Employees should report a suspected violation by notifying the Data Security Coordinator who will contact legal counsel, as appropriate.

IX. Breaches of the Policy

Whenever there is an incident that requires notification to government or other authorities, legal counsel shall be notified and there shall be an immediate post-incident review of events and actions taken, if any, with a view to determining whether any changes in the security practices are required to improve the security of Personal Information for which OASIS is responsible. Any breach of the policy will be logged, as will the actions taken in response to the breach. Such log will be provided to OASIS' legal counsel.

X. Third Parties

The contents of this ISP will apply to third parties who are intended to receive and process Personal Information and a similar policy or contractual restrictions must be in place before any such information is shared with them. OASIS' legal counsel will evaluate the third party's capacity to comply with the provisions of this policy. The operative contract will contain the requirement that the third party will

maintain safeguards consistent with this ISP.

XI. Exceptions

Any exceptions to this policy require prior written authorization and approval from the Data Security Coordinator or legal counsel.

EMPLOYEE ACKNOWLEDGEMENT FORM

I have received, read and understand the Information Security Policy. I understand that it is my responsibility to comply with it.

Printed name: _____
Signature:_____
Date:_____

Dates

Approved:
Wed, 2011-02-02
Effective:
Wed, 2011-02-02