REACH BOARDING SYSTEM

Written Information Security Plan (WISP)

Prepared by: Touchline Connect Pty Ltd

Last Modified 31/10/2020

1. OBJECTIVE

The objective of REACH Boarding System (REACH) in the development and implementation of this comprehensive written information security program ("WISP"), is to create effective administrative, technical and physical safeguards for the protection of personal information. The WISP sets forth our procedure for evaluating and addressing our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information.

For purposes of this WISP, "personal information" is as defined in the regulations: a 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; provided, however, that "personal information" shall 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.

2. PURPOSE

The purpose of the WISP is to:

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

3. SCOPE

In formulating and implementing the WISP, REACH Boarding System has addressed and incorporated the following protocols:

i. identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information;
ii. assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;

iii. evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;
iv. designed and implemented a WISP that puts safeguards in place to minimize those risks, consistent with the requirements of US and International Law.
v. implemented regular monitoring of the effectiveness of those safeguards.

4. DATA SECURITY TEAM

The Data Security Coordinator is responsible for implementing, supervising and maintaining the WISP. These responsibilities include the following:

i. Implementation of the WISP including all provisions outlined in Section 7 - Daily Operational Protocol;
ii. Training of all employees;
iii. Regular testing of the WISP's safeguards;
iv. Reviewing the scope of the security measures in the WISP 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;
v. 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 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 personal information.

DATA SECURITY COORDINATOR	
Mr Bradley Gibby *Director of Technology, Research & Development* *Touchline Connect Pty Ltd*	All regions Globally

DATA PROTECTION OFFICERS (DPO)	
Mr Garry Jowett *Managing Director – Touchline Connect Pty Ltd*	Australia, New Zealand, Asia-Pacific, Africa, Rest of world
Mr Brian Murray *Managing Director – REACH North America*	USA, Canada
Mr James England *Director – REACH Europe*	UK, Ireland, European Union, GDPR designated DPO

INCIDENT RESPONSE EXECUTIVES (IRE)	
Mr Garry Jowett *Managing Director – Touchline Connect Pty Ltd*	Australia, New Zealand, Asia-Pacific, Africa, Rest of world
Mr Brian Murray *Managing Director – REACH North America*	USA, Canada
Mr Adam Bates *Managing Director – REACH Europe*	UK, Ireland, European Union

ADDITIONAL MEMBERS
In addition to those individuals listed above, additional experts may be included on the Incident Response Team, depending upon the nature and scope of the incident. In particular, technical experts may be included from various providers of hardware or service services use by REACH Boarding System (such as cloud hosting service provider).

5. Internal Risk Mitigation Policies

To guard against internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory security measures:

i. We will only collect personal information of clients, customers or employees that is necessary to accomplish our legitimate business transactions or to comply with any and all federal, state or local regulation for jurisdictions that we operate in.
ii. Access to records containing personal information shall be limited to those employees whose duties, relevant to their job description, have a legitimate need to access said records, and only for this legitimate job-related purpose.
iii. Written and electronic records containing personal information shall be securely destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements.
iv. A copy of the WISP is to be distributed to each current employee and to each new employee on the beginning date of their employment. It shall be the employee's responsibility for acknowledging in writing, by signing the attached sheet, that he/she has received a copy of the WISP and will abide by its provisions. Employees are encouraged and invited to advise the WISP Data Security Coordinator of any activities or operations which appear to pose risks to the security of personal information. If the Data Security Coordinator is him or herself involved with these risks, employees are encouraged and invited to advise any other manager or supervisor or business owner.

v. A training session for all current employees will be held on May 1 each year to detail the provisions of the WISP.
vi. All employment contracts, where applicable, will be amended to require all employees to comply with the provisions of the WISP and to prohibit any nonconforming use of personal data as defined by the WISP.
vii. Terminated employees must return all records containing personal data, in any form, in their possession at the time of termination. This includes all data stored on any portable device and any device owned directly by the terminated employee.
viii. A terminated employee's physical and electronic access to records containing personal information shall be restricted at the time of termination. This shall include remote electronic access to personal records, voicemail, internet, and email access.
ix. Disciplinary action will be applicable to violations of the WISP, irrespective of whether personal data was actually accessed or used without authorization.
x. All security measures including the WISP shall be reviewed at least annually beginning March 1, to ensure that the policies contained in the WISP are adequate meet all applicable federal and state regulations.
xi. Should our business practices change in a way that impacts the collection, storage, and/or transportation of records containing personal information the WISP will be reviewed to ensure that the policies contained in the WISP are adequate meet all applicable federal and state regulations.
xii. The Data Security Coordinator or his/her designee shall be responsible for all review and modifications of the WISP and shall fully consult and apprise management of all reviews including any recommendations for improves security arising from the review.
xiii. The Data Security Coordinator shall maintain a secured and confidential master list of all lock combinations, passwords, and keys. The list will identify which employee possess keys, keycards, or other access devices and that only approved employees have been provided access credentials.
xiv. The Data Security Coordinator or his/her designee shall ensure that access to personal information in restricted to approved and active user accounts.
xv. Current employees' user ID's and passwords shall conform to accepted security standards. All passwords shall be changed at least annually, more often as needed (e.g. seasonally).
xvi. Employees are required to report suspicious or unauthorized use of personal information to a supervisor or the Data Security Coordinator.

Whenever there is an incident the Data Security Officer will follow the procedures set out in REACH's Cybersecurity Incident Response Plan.

6. External Risk Mitigation Policies

- Firewall protection, operating system security patches, and all software products shall be kept up to date and installed on all company computers and devices.
- Personal information, wherever possible, will be stored only on the secure cloud servers of REACH and not on company devices unless there is a legitimate business need and use of reasonable security measures, as described in this policy.
- All system security software including, anti-virus, anti-malware, and internet security shall be kept up-to-date and installed on any computer that stores or processes personal information.
- A secure upload portal on REACH's secure clout network at https://securedrop.reach.cloud will be provided for all client files that are to be supplied to REACH.
- There shall be secure user authentication protocols in place that:
    - Control user ID and other identifiers;
    - Assigns passwords in a manner that conforms to accepted security standards, or applies use of unique identifier technologies;
    - Control passwords to ensure that password information is secure.

7. DAILY OPERATIONAL PROTOCOL

This section of the WISP outlines the daily efforts to minimize security risks to any computer system that processes or stores personal information, ensures that physical files containing personal information are reasonably secured and develops daily employee practices designed to minimize access and security risks to personal information of our clients and/or customers and employees.

The Daily Operational Protocol is effective from *March 1, 2017* and shall be reviewed and modified as deemed necessary at a meeting of the Data Security Coordinator and the Data Protection Officers and other staff authorized for the security of personal information.

Any modifications to the Daily Operational Protocol shall be published in an updated version of the WISP. At the time of publication, a copy of the WISP shall be distributed to all current employees and to new hires on their date of employment.

7.1. Record keeping Protocol:

We will only collect personal information of clients and customers and employees that is necessary to accomplish our legitimate business transactions or to comply with any and all federal and state and local laws.

Within 30 days of the publication of the WISP or any update the Data Security Coordinator or his/her designee shall perform an audit of all relevant company records to determine which records contain personal information, assign those files to the

appropriate secured storage location, and to redact, expunge or otherwise eliminate all unnecessary personal information in a manner consistent with the WISP.

Any personal information stored shall be disposed of when no longer needed for business purposes or required by law for storage. Disposal methods must be consistent with those prescribed by the WISP.

Paper or electronically stored records containing personal information shall be disposed of in a manner that complies with state and federal law and as follows:

(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.

The Data Security Coordinator and Data Protection Officers are authorized to access and assign to other employees files containing personal information:

7.2. Access Control Protocol:

All our computers shall restrict user access to those employees having an authorized and unique log-in ID assigned by the Data Security Coordinator.

All computers containing access to personal information that have been inactive for 10 or more minutes shall require re-login.

8. Breach of Data Security Protocol

Should any employee know of a security breach at any of our facilities, or that any unencrypted personal information has been lost or stolen or accessed without authorization, or that encrypted personal information along with the access code or security key has been acquired by an unauthorized person or for an unauthorized purpose, they are required to notify the Data Security Coordinator.

The Data Security Coordinator will follow the procedures set out in REACH's Cybersecurity Incident Response Plan and, where it involves a data security breach, REACH's Data Breach Action Plan.

9. Disposal of records containing personal information

When disposing of records, REACH or any agency or person shall meet the following minimum standards for proper disposal of records containing personal information:

i. paper documents containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed;
ii. 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.

Any third party hired to dispose of material containing personal information shall implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation and disposal of personal information.