Reach Student Life Management

DATA BREACH REPSONSE PLAN

Prepared by: Touchline Connect Pty Ltd

Last Modified: 30/10/2020

Contents

PURPOSE

REACH Boarding System (REACH) stores private and sensitive information related to students, staff, and internal business operations, as well as manages and maintains technical infrastructure required to house and maintain this information.

This Data Breach Response Plan (DBRP) outlines the procedures that REACH will undertake when unauthorized access or disclosure of private or sensitive information is identified. This DBRP forms part of REACH's Cybersecurity management plans and should be read in conjunction with the Cybersecurity Incident Response Plan (CIRP) and the Written Information Security Plan (WISP).

DEFINITIONS

Cybersecurity Incident Response Plan (CIRP)

The Cybersecurity Incident Response Plan outlines the procedures that REACH uses to detect and respond to unauthorized access or disclosure of private information from systems utilised maintained or serviced as part of the REACH Boarding System product.

Data Breach

A Cyber Security Incident in REACH which involves the unauthorized access or disclosure of personal or sensitive information.

Data Protection Officer (DPO)

Data protection officers are responsible for overseeing the company's data protection strategy and its implementation to ensure compliance with GDPR requirements and the company's Personal Data Privacy Policy.

Incident Response Manager (IRM)

The IRM oversees all aspects of the Cyber Security Incident. The key focuses of the IRM will be to ensure proper implementation of the procedures outlined in the Cyber Security Incident Response Plan, to keep appropriate Incident Logs throughout the incident. The IRM acts as the key liaison for the IRE for details, status and outcomes of the incident investigation. At the conclusion of a Cyber Security Incident, the IRM will conduct a review of the incident and produce both an Incident Summary Report and, where determined appropriate, a Process Improvement Plan.

Incident Response Executive (IRE)

The IRE oversees all aspects of the company's communications with stakeholders and affected parties. The key focuses of the IRE will be to monitor that the procedures outlined in the Cyber Security Incident Response Plan are being implemented and to act as the key liaison between the IRM, company management executives and other stakeholders such as clients or individuals.

Cyber Security Incident Log

The Cyber Security Incident Log will capture critical information about a Cybersecurity Incident and REACH’s response to that incident, and should be maintained while the incident is in progress.

Incident Summary Report (ISR)

The ISR is a document prepared by the IRM at the conclusion of a Cyber Security Incident and will provide a detailed summary of the incident, including how and why it may have occurred, estimated data loss, affected parties, and impacted services. Finally, it will examine the procedures of the Cyber Security Incident Response Plan, including the procedures when investigating the incident and whether updates are required. The template for the ISR may be seen in Appendix A.

Process Improvement Plan (PIP)

The PIP is a document prepared by the IRM at the conclusion of a Cyber Security Incident if the investigation and ISR provides recommendations for avoiding or minimizing the impact of future Cyber Security Incidents based upon the “lessons learned” from the recently-completed incident. This plan should be kept confidential for security purposes. The template for the PIP may be viewed in Appendix B.

DATA BREACH RESPONSE TEAM

INCIDENT RESPONSE MANAGER (IRM)	
Mr Bradley Gibby *Director of Technology, Research & Development* *Touchline Connect Pty Ltd*	All regions Globally

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

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

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).

DATA BREACH INCIDENT STEPS

When a data breach occurs in REACH the Incident Response Manager (IRM) will implement the following procedure for control, repair, notification and continuity.

Step 1: Contain the breach

Step 2: Assess the risks for any individuals associated with the breach

Step 3: Assess the technical risks associated with the breach

Step 4: Consider breach notifications

Step 5: Review the incident and take action to prevent future breaches

1. Contain the breach

i. Immediately identify and contain the breach. Restore or upgrade the security that was bypassed.
ii. Identify the cause of the breach and immediately contain any further breach
iii. Restore or Upgrade the security that was bypassed for the breach to occur

2. Assess the risks for individuals associated with the breach

i. Conduct initial investigation, and collect information about the breach promptly, including:
    - the type of personal information involved in the breach
    - how the breach was discovered and by whom
    - a list of the affected individuals, or possible affected individuals
    - the risk of serious harm to the affected individuals
    - the risk of other harms

ii. Determine whether the context of the information is important:
    - is the breach likely to result in serious harm to any of the individuals to whom the information relates?
    - is the data breach a reportable incident?

3. Assess the technical risks associated with the breach

i. Conduct initial investigation, and collect information about the cause and extent of the breach promptly, including:

- the date, time, duration, and location of the breach
- the type of information involved in the breach
- the cause and extent of the breach

ii. Assess priorities and risks based on what is known
iii. Ascertain the risks of altering the security structure to ensure that changes made are not opening other possible security risks.
iv. Keep appropriate records of the suspected breach and actions of the response team, including the steps taken to rectify the situation and the decisions made.

4. Consider breach notifications

Notify our Data Protection Officer (DPO) and determine who needs to be made aware of the breach (internally and externally).

- Does the breach trigger the requirements of data breach notifications (GDPR, regional privacy regulations)?
- Determine whether and how to notify affected individuals.
- Determine the timeliness of notifications to individuals and/or schools
- Consider whether others should be notified, including the police/law enforcement, or other agencies or organisations affected by the breach or can assist in containing the breach or assisting individuals affected by breach.

5. Review the incident and take action to prevent further breaches

i. Gather and review as much detail as possible about the event and determine all causes that lead to the event.
ii. Maintain a
iii. Undertake a detailed discussion between the IRM and IRE team from all regions in order to facilitate awareness and to determine any appropriate Process Improvement Plan.
iv. Conduct a post-breach review and on outcomes and recommendations as part of a Incident Summary Report.
   - Fully investigate the cause of the breach
   - Update security and response plan if necessary
   - Implement a strategy to identify and address any weaknesses in data handling that contributed to the breach
   - Make appropriate changes to policies and procedures if necessary
   - Revise staff training practices if necessary
   - Consider the option of further internal or external audits to ensure security continuity