Don Johnston Incorporated

Security and Privacy Plan - Breach Incident Response Overview

Identification Phase

Anyone can report a suspected breach at legal@donjohnston.com. Services are constantly monitored for breaches. Suspected breaches related to Don Johnston Products & Services are reported directly to the Chief Privacy Officer for Software as a Service. Suspected breaches related to Don Johnston marketing or website are reported directly to the Chief Privacy Officer for Marketing/Sales. This starts the Identification Phase of incident response. The Identification Phase has as its goal the discovery of potential security incidents and the assembly of an incident technical response team that can effectively contain and mitigate the incident.

Containment/Eradication Phase

Goal of this phase is to:

- Preserve Evidence
- Contain the Incident
- Remove the Threat

This phase is led by Chief Privacy Officer

Communication Phase

If the issue is identified as a breach affecting privacy and information is available, the Chief Privacy Officer will work with the company President and VP of Marketing to communicate both internally and externally within 48 hours (2 business days). The President will contact and work with our Business Insurance Provider. Individual Organizational Customers and Consumers who have set up accounts directly will be communicated through the web service. Districts/Schools who have purchased organizational accounts will have all information directed to the key license contact or a specified contact if a specialized agreement is in place. In some cases, specialized contracts specify a different contact or additional contacts to also receive communication. Communication will include What Happened, What Information Was Involved, What are We Doing, What You Can Do and For More Information. To help with communication, we will provide information and language to inform parents.

Chief Privacy Officer and President will also determine whether to notify the authorities/law enforcement (situation dependent). Chief Privacy Officer and President will consult our legal counsel to examine any applicable federal, state, and local breach reporting requirements to determine which additional authorities or entities must be notified in order to satisfy compliance requirements. Chief Privacy Officer and President will seek involvement of law enforcement when there is a reason to believe a crime has been committed or to maintain compliance with federal, State, or local legal requirements for breach notification. Chief Privacy Officer and President will determine responsibility and roles in communication. Any situation will be added to the Risk Analysis and Mitigation for future policies/procedures for risk mitigation.