Security Incident and Breach Notification Policy	
Effective Date: 9/07/2020	
Version 2.0	Responsible Party: Albert Strong

Introduction

UPLEVEL is responsible for the security and integrity of all data it holds. UPLEVEL must protect this data using all means necessary by ensuring at all times that any incident which could cause damage to UPLEVEL' assets and reputation is prevented and/or minimized. There are many types of incidents which could affect security.

It is the responsibility for all system users to formally report all security incidents, perceived incidents, or violations of the security policy immediately to their immediate supervisor, Chief Information Security Officer, or any member of the Security Review Board (SRB).

Reports of security incidents shall be escalated as quickly as possible. Each member of the UPLEVEL SRB must inform the other members as rapidly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. All reported incidents are logged, and the remedial action indicated. It is the responsibility of the SRB to provide training on any procedural changes that may be required because of the investigation of an incident.

A security breach is any incident that results in unauthorized access of UPLEVEL data, applications, services, and/or networks by bypassing our underlying security mechanisms. A security breach occurs when an individual or an application illegitimately enters our private, confidential or unauthorized logical IT perimeter.

A computer security incident is an event affecting adversely the processing of computer usage. This includes:

- Loss of confidentiality of information
- Compromise of integrity of information
- Denial of service
- Unauthorized access to systems
- Misuse of systems or information
- Theft and damage to systems
- Virus attacks
- Intrusion by humans

Ensuring efficient reporting and management of security incidents will help reduce and, in many cases, prevent incidents occurring.

UPLEVEL has an Incident Management Policy in place which details the procedures for the identifying, reporting and mitigation of all incidents including security incidents. Security incidents should be managed by this process and reference to that policy is made herein.

By continually updating and informing UPLEVEL employees, partner agencies, contractors and vendors of the importance of the identification, reporting and action required to address incidents, UPLEVEL can continue to be pro-active in addressing these incidents as and when they occur.

All UPLEVEL employees, partner agencies, contractors and vendors are required to report all incidents – including potential or suspected incidents, as soon as possible via UPLEVEL' Incident Reporting procedures.

Any loss of data and/or disclosure whether intentional or accidental must be reported immediately.

All UPLEVEL employees, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible to the Security Officer or Compliance Manager. This obligation also extends to any external organization contracted to support or access the Information Systems of UPLEVEL.

1 Customer Notification

The purpose of this policy is to define the circumstances under which UPLEVEL shall provide notice to customers regarding a breach in security.

UPLEVEL shall provide timely and appropriate notice to affected individuals when there is reasonable belief that a breach in the security of private information has occurred. Personal and/or proprietary

2 Scope

Attacks on UPLEVEL resources are infractions of the Terms of Service constituting misuse, or they may be vandalism or other criminal behavior. Reporting information security breaches occurring on UPLEVEL resources to appropriate authorities is a responsibility of all persons affiliated with UPLEVEL in any capacity.

3 Policy Statement

Suspected or confirmed information security breaches must be reported to the UPLEVEL Chief Information Security Officer (CISO). Contact the CISO immediately by Text or Phone at 571-214-7446 or by email at albert.strong@strongcybersolutions.com.

The CISO and Security Review Board (SRB) will investigate the report, and if a security breach of private and/or highly sensitive information may have occurred, will inform the CEO, CTO and/or law enforcement, as appropriate.

In the event that a public notification of the security breach may be warranted, the CEO or CTO will consult with the appropriate Counsel to develop the response and make the final determination if a public notification of the event is warranted.

4 Procedures

If a security incident is suspected:

1. Immediately report the attack to management and the CISO.
2. The CISO in turn will advise the CTO who will manage the technical response including, f possible, blocking or preventing escalation of the attack or other responses as appropriate;
3. Follow instructions communicated from the CISO in subsequent investigation of the incident and preservation of evidence;
4. Implement recommendations from the CISO;
5. Repair the resultant damage to the system.

5 Triggering Related Policies and Procedures

The CISO and Security Review Board (SRB), after a preliminary determination of the nature, scope, and impact of the Breach shall make a decision as to whether to invoke the following related policies and procedurs:

- Incident Response Policy
- Business Continuity Plan
- Disaster Recovery Plan

6 Internal Notifications

The Chief Information Security Officer will report serious computer security breaches to the CEO in a timely manner. The CEO or designee will consult with one or more of the Leadership Team as appropriate, and decide if the Critical Incident Management Team must be convened to determine a response strategy, or if an alternate group is appropriate for the response. This determination may be made prior to completion of the investigation of the security breach.

The CEO or designee will report the incident to Counsel when, based on preliminary investigation, criminal activity has taken place and/or when the incident originated from a UPLEVEL system.

7 Determination of External Notification

To determine if unencrypted private or highly sensitive information has been acquired, or is reasonably believed to have been acquired by an unauthorized person, the (likelihood of the) following will be considered:

1. Possession (lost or stolen device?)
2. Credible evidence the information was copied/removed
3. Length of time between intrusion and detection
4. Purpose of the intrusion was acquisition of information
5. Credible evidence the information was in a useable format
6. Ability to reach the affected individuals
7. Applicable UPLEVEL policy, and/or local, state, or federal laws

8 External Notification

If it is determined that an external notification to the affected Companies are warranted, the following procedures will apply:

1. E-mail notices developed by the Marketing department in coordination with the Information Security Officer, and approved by the CEO, and other executive team members as appropriate.
2. A blog post to be written by the Marketing department in coordination with the Information Security Officer, and approved by the CEO, and other executive team members as appropriate.

If the information acquired includes identifiable customer data that is not in an encrypted format, a public notification may be warranted.

Notification policy will comply with all applicable laws including US state law and applicable international laws in relevant jurisdictions.

Notification may not be warranted for information that is publicly and lawfully available to the general public, such as address, phone number, and email address.

Version History

Date	Version	Author	Details of Amendment
9/08/2020	1.0	Albert Strong	Final Draft
9/15/2020	2.0	Albert Strong	Edits and corrections

Review/Approve for Content/Compliance:

Job Title	Name
Chief Information Security Officer	Albert Strong
Chief Executive Officer	Joe Levy
Chief Technology Officer	Nimrod Vered