Security Incident Management Policy

April 2021

This document outlines the times at which an Incident is determined to be occurring and the policy for how to manage an incident. This policy is communicated to all members of the Thinking Cap Support and Development team and clients.

Thinking Cap at all times operates with the highest expectations of Security and Availability. Conditions that occur that impact these commitments include:

1. When external 3rd party Monitoring detects a Server Down condition.
2. When a Server Down ticket is received in our ticketing system from a Client or Staff member.
3. When any call is added to the Support Voicemail after Support Hours or where Support is unavailable.
4. When a call is received by a staff member directly from a client.

In all cases, an email goes to an automated paging system operated by a 3rd party. That system will auto-dial all members of the tech team from the most senior to the most junior in that order. Once a call is received and accepted the calls will stop and that team member will begin the process of investigation and contacting both additional resources if needed and the client Primary contact. Primary contact information is kept in an internal client management application and on paper in the Thinking Cap office.

If the condition is a Security issue, a determination is made if this is a Critical or High issue where a vulnerability is found that is allowing data to be altered or stolen and it can not be immediately resolved the following actions will be taken:

1. Turn Off Web Servers
2. Turn off Database Access to the Web Servers and all external clients i.e Aurora.
3. Notify primary contact by email (if available) or by phone within 1 hour with details of the detection, notes from the first investigation, a notice of the preventative shutdown and next steps.
4. A ticket will be opened if not already created in our Support System.

Once the system is fully isolated from the outside world we will begin an investigation of the incident and will begin a formal incident report. The report will document the chronological steps taken for investigation and will outline recommended remediation based on:

1. Our determination what data has been compromised.
2. Our determination the mechanism by which the breach occurred.
3. The incident report will be updated to define next steps to return to confidence.

The Service will not be restarted until the client approves remediation plan and that plan has been executed. A Pentest by a Third Part will always be performed, and evidence will be provided that the Pentest is capable of detecting the cause of the breach in the future and explanations will be provided why such testing did not detect the issue prior to that code going into production.