Cyber Security and Incident Response Protocol

The Center for Applied Management Practices (CAMP) owns and operates the web-based application elogicgenesis.com. This document outlines our most current Cyber Security and Incident Response Protocols.

Incident Handling Protocol

In the event of an incident resulting in harm or loss due to a data breach or software malfunction, which exposes client information to ineligible parties, this protocol will be followed.

Incident Response Goals

1. Maintain informed and transparent communication with our users.
2. Ameliorate all issues arising from the incident.
3. Prevent future incidents similar in nature.

Incident Response Team

Incident Response Manager/Commander

Sheila Lucas, Administrative Officer

slucas@appliedmgt.com

Incident Control Team Lead

Adam Ferguson, Vice President of Information Technology

aferguson@appliedmgt.com

Incident Control Team

Marq Agboyani, Chief Solutions Specialist

magboyani@appliedmgt.com

Ben Richmond, Vice President

brichmond@appliedmgt.com

Incident Discovery

When an incident is recognized and reported, the following roles and steps will be used to start the response to the incident:

Discoverer: Any eLogic Genesis staff or user who discovers the bug/breach/incident and brings it to the attention of eLogic Genesis staff.

Time of discovery: The exact moment the discovery occurs. This must be documented immediately.

Notice of Incident

Upon discovery, immediate triage and risk assessment will be conducted. Risk evaluation will include as much of the following information as available:

- Which information was exposed?
- How and where was the information shared?
- Which user(s) were impacted?
    - We will make notice available to those users/clients directly affected by the incident.
- How many total client profiles or agencies were involved?
    - If the incident involves data from Colorado, pursuant to Colorado HB 1128 - Colorado Consumer Privacy Protection Act
        - In the event that a breach affects the information impacting more than 500 Coloradans, we will notify the Colorado Attorney General's office.
- Other information as necessary.

As much information about the incident that can be reasonably shared with all affected parties will be communicated by the Incident Response Manager in a timely manner. Information communicated will include a minimum of the following information:

- What happened;
- When it was discovered;
- Which steps will be taken to enact Incident Remediation steps;
- Any reasonable timelines for incident repair; and
- Next communication steps.

Incident Remediation

Any and all appropriate remediation steps will be taken to support our users during an incident. Data loss and damages will be determined by the Vice President of Technology and communicated to all affected parties as soon as is reasonable following an incident.

Recovering or repairing any data loss may be impossible under certain circumstances. In these situations, the President/CEO will endeavor to develop an agreeable and amicable resolution between all involved parties.

Given the circumstances of any incident, all necessary and appropriate steps will be taken to prevent similar incidents from occurring.

Decision Making Hierarchy

Primary - President/CEO

Secondary - Vice President, Vice President of Information Technology

Tertiary - Chief Solutions Specialist, Administrative Officer

Incident Response Risk Assessment and Review History

11/18/2020 - First annual 'fire drill'. Results are recorded here.

Incident Response Revision History

11/18/2020 - Initial draft. Revisions were made to accommodate new findings based on the fire drill.

Changes to our Cyber Security and Incident Response Protocols

We may update our Cyber Security and Incident Response Protocols from time to time. Any adjustments made to this document are effective immediately and administered at the discretion of our President/CEO.