1. **Purpose**
   This document describes a policy in the event of an incident which compromises system integrity, service provision, and either the confidentiality or the integrity of client data.
2. **Policies**
   a. Priorities (in order of importance):
      i. Retain confidentiality and integrity of client data.
      ii. Investigate/fix the underlying cause of the incident.
      iii. Restore services.
   b. Initial Discovery:
      i. CCI Systems Team will notify CCI Management of an incident. A quick assessment of the severity should be determined.
      ii. CCI Management will make the decision if/when to notify client. However, in the case of a potential leakage of sensitive data, including Personally Identifiable Information, credit card information, or financial information, the client must be notified immediately.
   c. Incident Repair
      i. CCI Systems Team will make a determination as to whether or not service can be continued. The default position is to terminate service, but a decision should be made based on whether the incident is read-only (Ex: personal information viewable on the web), or write (database injection, XSS attack, system hacking) and the severity of the data involved.
      ii. CCI Systems Team will apprise CCI Management of their status. It is important that CCI Management deal with clients and other CCI Staff, to allow the Systems Team to work unimpeded.
      iii. Upon finding the cause, CCI Systems Team will attempt to give Management an estimated time for repair. This estimated downtime should be passed on to the client.
      iv. The decision to repair or rebuild a new system will be determined by the Systems Team. The default position will be to start with a clean system, restore client data from the last verified backups and save the old system for forensic purposes.
   d. Incident Response
      i. The appropriate authorities may be contacted, only after discussion between the client, CCI Systems Team, and CCI Management.
      ii. Customers of the client may be contacted, only after discussion between the client, CCI Systems Team, and CCI Management.
      iii. If the incident is caused by an application, CCI Application Developers may be required to assist the Systems Team in fixing the problem.
   e. Incident Postmortem
      i. An Incident Report must be filled out by CCI Systems Team and CCI Management.
      ii. Incident Reports must be shared with affected clients upon client request.
3. Enforcement
   a. Incident Management is the responsibility of the CCI Systems Team and CCI Management.
   b. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

08/26/2021
- Originated

08/31/2021
- Reviewed
- Formatting updated
- personal information changed to Personally Identifiable Information

08/31/2022
- Reviewed

08/31/2023
- Reviewed