Cultivate Incident Escalation Policy

Purpose

This policy outlines Cultivate's incident escalation procedures and quality assurance systems.

Policy owner

The Chief Technology Officer is the policy owner of the Incident Escalation Policy for Cultivate.

Policy review

This Incident Escalation Policy will be reviewed on an annual basis with all revision history as noted in the Revision History Table.

What is a Security Incident?

A security incident is an event that compromises or has the potential to compromise:

- the operation of covered core systems
- confidentiality or integrity of covered data assets
- A security incident may involve any or all of the following:
- a violation of work computer security policies and standards
- unauthorized computer or data access
- presence of a malicious application, such as a virus
- a denial of service condition against data, network or computer
- misuse of service, systems or information
- physical or logical damage to systems
- computer theft
- Security failures, concerns or complaints
-

It is anticipated that as new technologies and new requirements are introduced, this document should be reviewed at least annually. This function will be performed by the Chief Technology Officer.

Incident Response Plan Overview

There are many different security incidents that can occur with assorted severity levels and not all incidents will require focus on each step. However, it is important to be prepared and understand that typically different phases exist in responding to an incident, and the goals and objectives of each phase. The different phases of a security incident response plan at Cultivate are as follows:

- Prepare
- Report
- Identify
- Contain

- Eradicate
- Recover
- Review

Prepare

In preparing for security incidents several items need to be addressed.

- Incident handling team should include Chief Technology Officer, Chief Executive
- Officer and Head of Machine Learning
- End users should be trained at an appropriate level
- Contact information is included to this document and should be available on a
- shared drive for:
    - personnel that might assist in handling an incident
    - key partners who may need to be notified
    - key decision makers
- Backups should be taken and tested

Report

Please report security incident to the Chief Technology Officer immediately. If the Chief Technology Officer cannot be reached, please contact the Chief Executive Officer or the Head of Machine Learning.

You must also complete an incident intake report online for documentation Purposes.

Identify

Awareness that a security incident has occurred can originate from different sources such as technical people, end users or even clients.

Best practices suggest declaring that an incident has occurred when Chief Technology Officer sense that an adverse risk to the company exists and then assemble the team and implement the plan. It is also suggested to early on have multiple people involved, to save all key system files or records such as log files and start detailed documentation as soon as possible.

In many security incidents, the Chief Technology Officer needs to decide what are the goals in handling a particular incident, such as immediate business recovery or forensic examination.

Contain

Following basic procedures can contain many incidents. Specific procedures will

frequently depend on the nature of the incident, as well as the direction of the Chief Technology Officer. Remember that a compromised machine might not present valid data! Basic steps to consider include:

- Obtain and analyze as much system information as possible including key files and a backup of the compromised machine for later forensic analysis
- Powering off a machine might lose data and evidence. Preferably disconnecting wifi facilitates containment and forensic activity. (Putting the computer on a separate network with a network analyzer might help analyzing network activity)
- If one machine has been exploited others might be vulnerable. Actions that might need to be taken on a large scale might include:
    - Download security patches from vendors
    - Update antivirus signatures
    - Close firewall ports
    - Disable compromised accounts
    - Run vulnerability analyzers to see where other vulnerable hosts are
    - Change passwords as appropriate

Eradicate

To eradicate the problem specific procedures will frequently depend on the nature of the incident as well as the direction of the Chief Executive Officer.
Key considerations include:

- If machines OS has been compromised, it needs to be rebuilt using hardened machines on appropriate platforms
- Test any backups prior to restore and monitor for a new incident.
- Document everything

Recover

The recovery phase's goal is to return safely to production. Once again specific actions might depend on the nature of the incident as well as the direction of the Chief Executive Officer. Key considerations include:

- Retest the system preferably with a variety of end users
- Consider timing of the return to production
- Discuss customer notification and their concerns
- Discuss media handling issues
- Continue to monitor for security incidents

Review

This phase is to allow Cultivate to better handle future security incidents. A final report should be generated describing the incident and how it was handled. Suggestions for handling future incidents and reworking this document should be included in this report.

Incident tracking

Every incident is tracked as a ticket in Cultivate's ticket system of record, Assembla.

Incident tickets are typically created by a support engineer in response to a customer ticket or by a developer recognizing a monitoring alert as being an incident. At Cultivate we urge people to create a ticket if they're worried about something, rather than wait to escalate it.

Incident tickets in assembla will be tagged with the label "Incident".

Incident manager

Each incident and therefore ticket, is driven by the incident owner, who has overall responsibility for and authority for the incident. This person is indicated by the assignee on the incident ticket. The incident owner is empowered to take any action necessary to resolve the incident, which includes calling anyone in the organization and keeping those involved in an incident focused on restoring service as quickly as possible.

The incident owner is a role, not an individual on the incident. The advantage of defining roles during an incident is that it allows people to become interchangeable. As long as a given person knows how to perform a certain role, they can respond for any incident.

Revision History Table

Date of Review	Performed by	Description of Any Changes
09/12/2018	CTO	No changes needed.