Cottonwood, Inc.
Policies and Procedures

SECTION: Information Technology **POLICY NO:** 07-006

SUBJECT: Cybersecurity Incident Response Plan

EFFECTIVE DATE: May 2023

Policy:

The Cybersecurity Incident Response Plan is designed to protect the organization, maintaining the confidentiality, integrity, and availability of data and other assets, to avoid disruptions to business and reputational damage. Data assets include intellectual property, health protected information, strategy, company financials and customer information. These elements, if affected by an incident, could have varying degrees of impact on Cottonwood, Inc.

Incident response efforts involve a significant level of communication among different groups within Cottonwood, Inc., as well as with external stakeholders. An incident response communication plan should address how these groups work together during an active incident and the types of information that should be shared with internal and external responders. **(05-048 Privacy of Protected Health Information, Page 68 X. Breach Notification)**

Procedure:

1. Preparation – Perform a risk assessment and prioritize security issues, identify which are the most sensitive assets, and which critical security incidents the team should focus on. Create a communication plan, document roles, responsibilities, and processes, and recruit members to the Cyber Incident Response Team (CIRT).

Key Contacts:

- Information Technology (CIRT)
  - Information Technology Manager
  - Database Developer
  - Computer Support Specialist
- Senior Management
  - Chief Executive Officer
  - Administrator of Services
- Human Resources
  - Human Resources Director
- Public Relations
  - Community Relations Development Director
- Legal
- Insurance

2. Identification – The team should be able to effectively detect deviations from normal operations in organizational systems, and when an incident is discovered, collect additional evidence, decide on the severity of the incident, and document the “Who, What, Where, Why, and How”.

Begin with ‘patient zero’, the initial compromised device. The goal is to understand the root cause of the compromise.

True identification of an incident comes from gathering useful indicators of compromise (IOC’s). Rather than just rebuild the original infected device, look to identify any unique IOC’s that can be used to search across your estate for further evidence of compromise. If the incident relates to a malware infection, then ask the following questions:

- What network connections does the malware generate?
- Does the malware connect to any domains?
- What files are created on disk?
- What running processes are created?
- Are there any unique registry keys that have been created?

This data can then be used to search for further evidence of compromise and identify any other infected machines in your estate.

3. Containment – Once the team identifies a security incident, the immediate goal is to contain the incident and prevent further damage:

- **Short-term containment** — for example, isolating network segments or taking down infected production servers and handing failover.
- **Long-term containment** — applying temporary fixes to affected systems to allow them to be used in production, while rebuilding clean systems.

4. Eradication – The team must identify the root cause of the attack, remove malware or threats, and prevent similar attacks in the future. Patching devices, disarming malware, disabling compromised accounts are all examples of what may be required in the eradication phase of an incident.

5. Recovery – The team brings affected production systems back online carefully, to ensure another incident doesn’t take place. Important decisions at this stage are from which time and date to restore operations, how to verify that affected systems are back to normal, and monitoring to ensure activity is back to normal.

Alternatively, any compromised device will need rebuilding to ensure a clean recovery.

The following will aid the recovery process:

- Offline / segregated backups of data will be kept as online backups could be affected.
- Daily, weekly, and monthly backups will be created to protect against infection/damage if it isn't noticed immediately.
- Backups of system configurations (e.g., specialist systems) will be performed.
- Review the availability of spare devices if needed to replace or fully rebuild devices if the infection is unknown and/or hard to remove.

6. Lessons Learned – This phase should be performed no later than two weeks from the end of the incident, to ensure the information is fresh in the team’s mind. The purpose of this phase is to complete documentation of the incident, investigate further to identify its full scope, understand where the response team was effective, and areas that require improvement.

Appendix A: Structure and Members

Cyber Incident Response Team – The mission of Cottonwood, Inc. CIRT is to provide timely analysis and actions for security incidents that impact the confidentiality, integrity, and availability of Cottonwood, Inc. information systems and personnel.

CIRT will maintain an Incident Response Playbook to respond to different cyber-attacks.

Executive Management – Available to support critical decisions such as taking an important system offline.

Incident/Recovery Manager - Responsible for ensuring all actions are tracked and that the incident is documented and communicated clearly. Lead technical response and recovery.

IT & Infrastructure – Support by taking containment and remediation actions. Sometimes investigating and providing data.

HR / PR / Legal – Leads for other aspects of the investigation such as regulatory or media.