Ransomware Incident Response Policy

Purpose

The purpose of this policy is to lay the guidelines for the appropriate response to a ransomware breach. This policy lays out the safeguards put in place by the company to protect user data and company resources.

Terms and Conditions

I. Payment of Ransomware will be determined on a case-by-case basis with consideration coming from the necessary department heads and company leaders. In most cases we will refuse ransomware payment, and revert to most up-to-date backups. See Section IV for more information on backups.

II. The Chief Information security officer will be held responsible for creating any emails needed in notifying users of the security breach, and ensuring their delivery in the allotted time period. The Chief Information security officer, together with the IT department heads, will determine appropriate emails. Notification will go out no less than seventy-two (72) hours from the moments of discovery. The email will be distributed to our customers through the Public Relations office, and overseen by the Chief Communications Officer.

   a. The moment of discovery will be logged and reported to the CIO at incidentReport@company.com. Any suspicious activity and indications of any intrusion should be reported to the incidentReport@company.com

III. The IT department in conjunction with the Information Security Officer will work to determine the severity of the incident and the fine details, this information will be shared with the CIO first who will then relay information to the other C-level executives.

IV. Full system backups will be created biweekly depending on the sensitivity and amount of critical system resources and PII that is added to the company's servers. Incremental backups will be performed daily to ensure data integrity with storage systems. Backups will be encrypted (AES encryption algorithm) and held in three locations: productions, local backup, and remote backup locations meeting NIST backup standards.

   a. Backups that are successful will be stored for one month, or two full rotations of full backups. The system will maintain two full, operational, system backups at all times.

   b. Full System backups will be tested biweekly, offset from the biweekly rotation of routine backups. The incremental backups created to keep productions servers functional will be tested during the inactive work periods. This schedule will begin at 7:00 PM on Fridays. Failed backups will be retested on Mondays. Successful backup testing will be documented and stored in the logs.

V. After ransomware security breaches have been resolved adequately and completely, as determined by the IT department leaders the breach will be further investigated to discover the cause of the incident. Upon discovering the cause for the incident, the appropriate departments will create training recommendations and programs targeted toward the breach cause's department.

   a. Departments receiving training will be required to show their understanding and comprehension of the training, with incentivized rewards determined by the party conducting the training.

Policy version: x.x
Last Updated [Date]