Data Breach Response Policy

Overview

Jivasoft treats the security of its customer and user data as mission critical. Jivasoft will employ technological measures to protect the privacy of customer data, and all Jivasoft employees and/or contractors will protect the privacy and security of customer data. Software developed by Jivasoft that is used to collect and access customer and user data will be engineered to minimize the potential for data breaches.

Jivasoft does not store sensitive information, such as Social Security Numbers, HIPAA-protected information, bank account numbers or credit/debit card numbers in its systems. Customers are primarily responsible for choosing what information is kept in Jivasoft's systems. In the event that Jivasoft becomes aware that customers have elected to store sensitive information in Jivasoft's systems, Jivasoft will notify the customer that such information is to be removed and not to be stored in Jivasoft's systems. If the customer will not comply with this request in a reasonable timeframe, Jivasoft will remove the sensitive information from its systems.

Identification

Jivasoft will undertake commercially reasonable measures to monitor for data breaches. In the event that any Jivasoft staff member determines that a data breach has occurred or may have occurred, they will immediately notify executive management of the company. It is possible that a data breach will be identified by a customer or user of Jivasoft's services or by some other third party. Any notification received from a customer, user or third party by an employee or contractor of Jivasoft will immediately be presented to executive management.

Response

Jivasoft's response to a data breach will involve mitigation, recovery and notification of affected parties, as well as notification of and cooperation with appropriate state, local and federal law enforcement authorities. Jivasoft maintains a commercial liability policy that includes coverage for data breach response. In the event of a data breach or suspected data breach, Jivasoft will notify its insurance carrier and initiate the claim process to provide additional financial resources to support its response.

Mitigation

Jivasoft will take immediate action to mitigate a data breach. This action could include taking down servers, databases, websites, and web services to prevent further compromise of customer and user data. These mitigation steps could result in a service interruption for some or all of Jivasoft's customers. While Jivasoft will always strive to provide continuous availability of its software and services, data security takes precedence. Therefore, Jivasoft will not compromise the security of its customer data to avoid service interruptions.

Jivasoft will redirect all appropriate staff from normal duties to assist in identifying the cause of a data breach and preventing further exploitation of the breach. If Jivasoft staff is not able to identify the cause of the breach and to mitigate further exploitation of the breach, the company will immediately employ appropriate third-party resources to assist. These resources will consist of Rackspace technical support and/or cyber-security consulting firms.

Notification

As soon as mitigation steps are underway, Jivasoft will notify all affected or potentially affected customers of the breach. Jivasoft will offer to notify all affected employees of each customer of the breach. Each customer will be asked whether they prefer to notify their employees themselves or to have Jivasoft perform the notification to each individual employee who may have been affected.

Jivasoft will notify its insurance carrier of any breach and initiate a claim process to provide additional resources to fund its response.

Jivasoft will notify appropriate law enforcement authorities of the breach. Notification will be made to the San Antonio office of the Federal Bureau of Investigation and to the San Antonio Police Department.

Jivasoft will notify Rackspace of the breach in order for Rackspace to provide assistance with mitigation and to assist Rackspace in preventing further exploitation of its servers and other infrastructure.

This policy is effective as of 1/1/2016