Priority Engine Data Security Documentation

TechTarget, Inc. (“TechTarget”) follows NIST guidelines including FIPS 199 to assess its information systems into categories. TechTarget’s systems, processes, and policies are aligned with many of the standards in ISO/IEC27001. We follow the Cobit framework and our security controls are tested twice a year by internal and external audit firms.

Access Control

Access to our network requires a unique individual user name and password. We have a password policy that requires at least 8 characters and a mix of upper case, lower case, numbers and symbols. We also maintain an account lockout policy that meets industry standards.

Physical Security

Physical access to the data center is contained in audit logs that are retained for review. Physical access is limited only to individuals who require access to our systems. Procedures are in place that any unauthorized access to facilities and/or hardware are immediately reported.

Network Security

Strong cryptographic solutions are applied to all Priority Engine systems to protect the confidentiality of customer information when being transmitted mailed or stored in electronic form. Inbound and outbound traffic is restricted to only allow necessary services through the firewall.

Salesforce.com Data in Priority Engine

Salesforce.com (“SFDC”) data is encrypted and stored using 128-bit AES on TechTarget servers. The private encryption key is not stored in TechTarget’s databases. Priority Engine transmits a small number of identifying SFDC Lead, Contact, and Account data points used to match objects with Priority Engine companies. TechTarget also transmits a small number of identifying SFDC Organization and User data points to authenticate, provide usage logs and support email notification features. All data is transferred to Priority Engine using HTTPS.

Frequency of Data Transfer

Priority Engine is primarily a web browser application. The majority of data transfers will occur on demand when a SFDC User clicks a link or button or otherwise interacts with a Priority Engine page. If email notifications are enabled by an administrative user on the client’s account, then the system will send a weekly notification email initiated by SFDC. If an administrative user on the client’s account enables daily synchronization between their SFDC database and Priority Engine, then there will be a daily transfer of new and updated account matching data points initiated by SFDC.

Authentication

Priority Engine uses SFDC's authentication to be installed, configured, and used. All requests to Priority Engine servers include an access key used to authenticate an SFDC Organization and provide access to services and data. Priority Engine access keys will be discontinued and re-issued if either TechTarget or the client has any concern about misuse or theft.

Salesforce.com Data in Priority Engine

Third Parties

Priority Engine does not share client SFDC data points with third parties.

PE Configuration Page

The server off which Priority Engine runs requests permission to load the Priority Engine configuration page and does not transmit any identifying data points.

PE and Salesforce Email Notifications

Emails are sent using SFDC and are subject to the SFDC's policies and limits. The Org URL is used to provide links back to the SFDC Account pages referenced in the emails. Emails will be sent from the SFDC User who enabled notifications on the PE's configuration page (typically an individual administrator level access).

Opportunity Data

SFDC opportunity data is synchronized to the PE servers only if a customer chooses to opt in. When a client opts out, all opportunity data is purged from our servers. Data is transferred securely using HTTPS.

Priority Engine Inbound Convertor

Priority Engine Inbound Convertor allows Priority Engine to identify accounts that have both visited a client's website and are actively researching relevant solutions on the TechTarget network.

Clients can enable this feature by inserting TechTarget's Inbound Convertor JavaScript script on the pages of their sites where they wish to have their website traffic tracked. Accessing these tagged pages will send a request to a TechTarget activity tracking end-point. Data retrieved during this process is stored on TechTarget's servers for the duration of the campaign.

For clarity, individual visitors to client's websites are not identified via PE Inbound Converter; rather clients will have the ability to identify the accounts which have accessed their website. Additionally, information about specific accounts that have visited the tracked website will only be available to Priority Engine users with access to the Account Lists that are generated by the system.