JOOR

Security Protocol

JOOR Security Protocol

Privacy

We provide username and password authentication to access the JOOR platform. Credentialed clients can access JOOR based on the permissions they are granted contractually. An individual client (Retailer, Brand) can only access the data they have entered in their JOOR account or data from their connections on JOOR.

Visibility

We use key-based authentication to connect to each server. Keys are very closely monitored and revoked as necessary. Access to servers is also restricted to internal JOOR employees, depending on job role.

Data Protection

Our security protocol is based on defense-in-depth. Essentially, we provide several controls to ensure the confidentiality, integrity, and availability of the data on the JOOR platform. Some of the ways we do this include firewalling logically dissimilar data tiers, authentication protocols on all layers of our stack, snapshotting and full backups of all server instances. We use Amazon Web Services (AWS) and leverage the compliance and data availability techniques that have made the platform so popular. See AWS Cloud Compliance for more details.

Encryption

JOOR uses SSL encryption for all data processes within our site. More specifically, we're using a RSA Encryption (1.2.840.113549.1.1.1) encryption algorithm with a 2048-bit key. Data is encrypted at rest in Amazon's S3 service.

Data Backup

Our database is constantly backed up with five-minute resolution. We have a tiered backup scheme, where we take a series of daily, weekly, bi-weekly and monthly incremental snapshots, in addition to full image (AMI) backups. This allows for full server rebuilds, incremental restores, and custom builds depending on the restoration requirement.

Data Loss

We currently use AWS RDS to house our PostgreSQL databases. In the rare likelihood that there might be an instance of data loss or corruption, our RDS instances can be restored to very precise points in time. In most instances, 5 minutes immediately prior to the point of loss / corruption.

Data Location

The AWS US East region (where we house our servers) is located in Northern Virginia. Within the datacenter, our data is then spread across multiple Availability Zones, connected by low-latency links for redundancy / high-availability.

Data Security

From the http://aws.amazon.com/security/ page: "The AWS cloud infrastructure is housed in AWS's highly secure data centers, which utilize state-of-the art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis. All personnel must be screened when leaving areas that contain customer data. Environmental systems in the data centers are designed to minimize the impact of disruptions to operations. And multiple geographic regions and Availability Zones allow you to remain resilient in the face of most failure modes, including natural disasters or system failures." For more details on AWS security protocols, see this whitepaper: Amazon Web Services: Overview of Security Processes