Security Policy

Last Updated: March 16, 2022

LAYERED SECURITY

APPLICATION SECURITY FOR BACKGROUND CHECKS

Data transmitted to or from the Iqsoc applications is encrypted using TLS 1.2. We store sensitive information in encrypted form using a unique key. We engage independent security experts to audit our code and test our applications for vulnerabilities.

ACCOUNT SECURITY FOR EMPLOYERS AND CANDIDATES

We follow best practices for protecting your Iqsoc employer or candidate account, with passwords hashed and salted using bcrypt, role-based access controls, and suspicious activity alerts.

ORGANIZATIONAL SECURITY

All Iqsoc employees undergo in-depth background checks before joining the team, and our in-house privacy and security experts regularly audit compliance with policies and procedures.

All employee laptops have mandatory full-disk encryption, and we strictly limit and audit access to customer data.

INFRASTRUCTURE SECURITY

Our infrastructure service providers, such as Amazon Web Services, have achieved SSAE 16 and/or ISO 27001 compliance and meet rigorous standards for protecting the networks and servers powering Iqsoc.

HIGH AVAILABILITY

UPTIME MONITORING

The Iqsoc platform is independently monitored 24/7 from 60+ locations around the globe for any signs of downtime or service degradation.

Our US-based support team is on hand, Monday thru Friday from 8AM to 8PM ET to answer any questions should you suspect an uptime issue.

BACKUP AND FAILOVER

We architect Iqsoc's platform, applications and databases across multiple availability zones for fast failover and send frequent backups in encrypted form to an offsite location.

NON-DISRUPTIVE DEPLOYMENT OF CODE

Our engineering team uses blue/green deployments for releasing changes into production, which lets us deliver frequent updates while minimizing the need for maintenance windows with downtime.

SCALABLE ARCHITECTURE

Iqsoc is a scalable, highly available, fault-tolerant US-based web service, leveraging best-of-breed infrastructure providers to optimize availability and performance.

REPORT A SECURITY CONCERN

If you believe you have discovered a security and/or privacy vulnerability that affects Iqsoc services, please report it to us. We appreciate reports from everyone, including customers, developers, and researchers. The company participates in a bug bounty program.

When reporting a security or privacy vulnerability, please include the following:

- The specific product and software version which you believe to be affected
- A thorough description of the behavior observed of the vulnerability
- A clear list of steps required to reproduce the issue; if the steps to reproduce the problem are difficult to document, we encourage you to include a video capture of the steps along with the written description

Once we receive your report, we will review the details and contact you if we need more information. Please report your findings to info@iqsoc.com .