Questis

Security Overview

Overview

Questis is passionate about and dedicated to protecting, safeguarding, and securing our customer data. To do so, Questis has established a strong security program supported by a comprehensive suite of security, confidentiality, and privacy policies, processes, procedures, and controls.

Questis is composed of a distributed microservice architecture that supports many independently developed, versioned, and scaled components. This allows for rapid development, testing and deployment of new features and fixes. Questis's microservice architecture allows for changes to be deployed quickly. New code is deployed to production on a bi-weekly basis at a minimum.

This security overview highlights Questis' approach to each of the following areas:

Security Governance

Security Strategy, Program, and Policies
Risk and Vulnerability Management
System Resiliency, Business Continuity and Disaster Recovery

Physical Security

Data Centers
Office Buildings

System Security

Logical Access Control
System Hardening, Baselines, and Configuration Management
Logging, Monitoring, and Alerting
Segregation of Duties
Code Security and Change Management
Data Classification, Handling, and Encryption
Data Leakage Protection

Personnel Security

Human Resources Security
Security Awareness

Security Governance

Security Strategy, Program, and Policies

Questis' approach to security uses a defense-in-depth strategy. This strategy is supported by an established, operational Information Security Program, with a supporting suite of policies, processes, controls, and procedures. Questis leverages defense-in-depth to harden each layer of Questis' infrastructure, systems, and processes.

Risk and Vulnerability Management

Questis employs a defense-in-depth security model allowing defense against malicious attacks and intruders at each layer. To proactively identify potential risks, Questis utilizes several vulnerability and risk detection mechanisms including, but not limited to, routine security vulnerability scans, conducting regular compliance and security audits, reviewing security alerts, and engaging third-party assessment organizations to conduct external penetration tests.

Results of these activities are consolidated and put into Questis' Task Management platform. The Questis Task Management platform is reviewed by the Head of Information Security on a regular basis. Questis performs routine reviews of scan results, audit findings, Security Information and Event Management system (SIEM) events, system security alerts, and other relevant information. Risk ratings are applied to each risk and are calculated based on both the impact and likelihood of each risk. Questis' Information Security team creates risk mitigation plans for each risk and executes these risk mitigation plans. Status of risk mitigation activities contained within Questis' Task Management platform are communicated to Questis' management team on a regular basis. Any blockers identified in risk mitigation activities are provided to Questis' management team in order to diffuse any risk mitigation issues in a timely manner.

Security Governance

System Resiliency, Business Continuity and Disaster Recovery

Questis production systems are architected with the level of resiliency required to meet or exceed operational up-time requirements. Questis operates using 2N (redundant) production environments. Each production environment is located in geographically separate, fault-tolerant zones, significantly reducing the likelihood of full system failure and impactful system outages.

Questis stores all production application and audit logs for a minimum of 7 years and they are replicated to multiple backup locations each with 99.999999999% durability. All application data is version controlled and replicated in real-time to multiple locations. This ensures data integrity and availability.

OS baselines and associated system configurations, code repositories, and development system data are regularly backed up to help ensure timely restoration of systems and system configurations in the event of catastrophic system failure. Mission critical systems are backed up hourly or replicated in real-time.

Questis maintains a Business Continuity Plan that identifies business impacting systems and processes, critical dependencies, and strategy plans to restore business operations in the event of an impacting event. In order to support the Business Continuity Plan, Questis also has a Disaster Recovery Plan that lists and describes critical system components, identifies recovery time and point objectives, and contains procedures to recover from a catastrophic system failure. The Disaster Recovery and Business Continuity Plans are reviewed, updated, and tested on an annual basis.

Physical Security

Data Centers

Questis relies on secure data center facilities to house Questis infrastructure including, but not limited to, buildings, power (including redundant power supplies, UPS, and generator backup power), HVAC (including temperature and humidity controls), racks, and system components (including network devices and servers).

Data center facilities are certified against a variety of security standards, including:
SOC 1, 2, and 3
DIACAP, FISMA and FedRAMP
DOD CSM Levels 1-5
PCI DSS Level 1
ISO 9001/ ISO 27001
ITAR
FIPS 140-2

Office Buildings

Physical access to Questis corporate office buildings is secured to allow only Questis personnel with an active electronic access. Physical access is removed when personnel leave Questis. Physical access control lists are reviewed periodically for appropriateness. Visitors are required to sign in using the visitor access log prior to being provided a visitor badge. The visitor badge is a card that does not have the ability to enter through Questis corporate office doors. Visitors are escorted at all times by authorized Questis personnel.

System Security

Logical Access Control

Logical access to Questis production system components is limited to only authorized personnel with a legitimate business justification and documented security management approval. Questis performs in-depth background checks on all personnel that have logical administrative access. Questis follows the principle of least privilege by provisioning only the needed permissions to users in order to perform his/her job function.

Users are authenticated to the Questis production environment using strong multifactor authentication mechanisms that include complex passwords and one-time passcode authentication tokens. User access to systems and user permissions are reviewed on a periodic basis. User access is removed from Questis systems when personnel leave Questis.

System Hardening, Baselines, and Configuration Management

Questis systems are hardened using industry-recognized hardening standards such as Defense Information Systems Agency (DISA), Security Technical Implementation Guide (STIG), and Center for Internet Security (CIS) benchmarks. A baseline Operating System (OS) image is used for every system build. All applications are built using immutable images that are promoted through environments, ensuring application integrity throughout the promotion and deployment process.

Patches are applied to systems in a timely manner. Patching includes updating the baseline OS image for all new builds and also includes updating systems currently running in production. As part of the patch application process, Questis strategically applies updated patches (including major version changes) to systems in a pre-production environment for testing and system analysis on a bi-weekly basis. When testing is complete in a pre-production environment, patches are methodically applied to systems in the production environment. All applications include the latest patches at deployment time. OS configurations are orchestrated by centrally managed deployment mechanisms. System configuration deviations are identified, logged, and reported by this centrally managed deployment mechanism.

Network devices are configured to use secure configurations. Network device firmware is kept up-to-date by applying the latest patches provided by network device manufacturers. Firewalls are configured to deny all traffic except that permitted by justified exception. Firewall rules are reviewed bi-weekly to help ensure rule sets are configured to limit ingress and egress communications to only those required for the operations of Questis services.

System Security

Logging, Monitoring, and Alerting

System, database, and application activities are logged and monitored for irregular and suspicious behaviors. Logs are sufficiently detailed to support incident response and root cause analysis processes. Logs are in read-only format, protecting against direct and inadvertent modification. All systems sync with authoritative NTP time sync sources to help ensure events and logs are using accurate time stamps. Questis uses metrics and monitoring systems to produce alarms and notifications, which are sent to the Questis team to investigate, determine root cause, and remediate issues.

Segregation of Duties

Questis segregates its development and production environments, both via network segmentation and logical access restrictions. Development and testing of code takes place in the development environments. Production code, after testing and authorization, is promoted into the production environment. In addition to segregating application environments, Questis also segregates request, approval, and provisioning duties as part of both the logical access request process and the deployment process. Deployment of code to production systems is performed only after Information Security approval. Segregating environments and duties in these critical processes is key to reducing the risk of fraud, error, and other potential malicious activities.

System Security

Code Security and Change Management

Application code is managed and deployed using a centrally managed version control repository. Changes to software repositories require a documented description of the change, a peer review, systematic code style checks, and code security reviews.

Code is deployed to servers in a controlled manner. Deploying code to a test environment, testing the deployed code in the test environment, and, when confirmed successful, code is then eligible to be promoted to the production environment. Image promotion ensures integrity of application code being deployed.

Code deployment and promotion is limited to only authorized operations team members. By limiting access to only a select set of individuals with the ability to promote images reduces the likelihood of untested or potentially malicious code being deployed to production systems.

Version Control repositories are regularly backed up to ensure a timely restore of applications in the event of catastrophic system failure. Production images are replicated to multiple datacenters across geographically separated regions.

Data Classification, Handling, and Encryption

Questis handles data commensurate with the level of data sensitivity. Questis classifies and protects data according to the sensitivity. Data classified as either Confidential or Sensitive are encrypted in transit and at rest using cryptographically strong encryption mechanisms.

For data in transit, Questis encrypts transmissions using TLS 1.1 or above. For data at rest, Questis uses AES-256 keys to encrypt sensitive data. At the end of the life cycle, data is destroyed securely. Sensitive and Confidential data is only stored in the production environment on authorized systems.

Data Leakage Protection

Access to database zones containing sensitive information is limited to only authorized personnel and only behind a secure Virtual Private Network (VPN) requiring multi-factor authentication. All authorized access is logged and reviewed by the security team regularly.

Personnel Security

Human Resources Security

Questis personnel are required to pass a robust background check prior to starting employment at Questis. Job roles and responsibilities are communicated to Questis personnel. For Questis personnel with security-related roles and responsibilities, the Information Security team provides additional security-related training and instruction to these personnel. Questis personnel found not adhering to the Questis Policy are subject to investigation with appropriate consequences, including disciplinary action up to termination of employment.

Security Awareness

All Questis personnel are trained and educated to be assertively security-minded. Security and compliance processes are embedded into Questis' culture, and are demonstrated by the members of the organization. Questis performs regular phishing and social engineering tests against all employees to ensure increased employee awareness.

As part of Questis' new hire orientation, new hires are provided thorough information security awareness training. This training is provided as a refresher to Questis personnel on an annual basis and is a requirement of employment at Questis. As part of this awareness training, Questis personnel are instructed to report any suspicious behavior to the Information Security team.

Summary

Questis invests heavily in reducing security risks at each layer of the organization and each level of Questis' infrastructure. Part of Questis' security program includes a continuous improvement program, where policies, controls, mechanisms, detection and prevention systems, threats, and risks are reviewed, evaluated, and enhanced to achieve progressive hardening against external and internal threats.

Please direct any questions to security@myquestis.com.