WILEY

Wiley EPIC and PAC Infrastructure, Security, and Data Privacy

Wiley is committed to protecting all confidential and personally identifiable information collected in the delivery of our assessment products and services. We have developed a robust security policy framework and related controls which are regularly scrutinized. Our policies and controls define and enforce security practices that safeguard the data our customers and participants entrust to our keeping, as well as ensure the highest levels of availability of our assessment platforms for doing business at any time, in any time zone in the world.

DATA CENTER SECURITY

Our application platform is maintained in three Tier 3 data centers, and each facility benefits from recommended hardened hosting environment features including:

- 24x7 security guard protection
- Security camera monitoring
- Restricted physical access to systems
- ISO/IEC 27001-based policies and procedures, which are reviewed by independent auditors
- Fully documented change-management procedures
- Secure media handling and destruction procedures for all customer data

Data centers are audited to the ISAE 3402 and SSAE 16 standards and maintain current SSAE 16 SOC 2 reports, which are available to our customers and prospects. Our platforms were among the first to be EU-US and US-Swiss Privacy Shield certified, and we are on-track to be compliant with GDPR regulations when they come into force in May of 2018.

NETWORK AND SERVER SECURITY

Servers and networks are actively monitored by a suite of proven monitoring solutions. This system monitors over 1800 sensors on over 200 servers and infrastructure devices. Resources are checked at least once every five minutes, and critical indicators are sampled every 60 seconds.

Data for each monitoring point is automatically recorded and tracked for historical trend analysis. Other network and server security safeguards include:

- Automated system installation using hardened and patched OS
- Dedicated redundant stateful network firewalls and application layer firewalls
- DDoS (Distributed Denial of Service) and threat mitigation systems
- Quarterly third party vulnerability scanning and penetration testing

EVERYTHING DiSC A Wiley Brand   THE FIVE BEHAVIORS OF A COHESIVE TEAM™   PXT SELECT™ A Wiley Brand   Profiles International®

11/07/2017

WEB TRAFFIC SECURITY

All sensitive assessment web traffic is redirected to a secure Hypertext Transfer Protocol (HTTPS) and encrypted using SSL certificates, providing security compatibility with every major browser. All non-essential protocols are blocked at the firewall. Remote administration is conducted via encrypted remote desktop sessions over IPsec VPN connections, and passwords are stored using a one-way hash.

BUSINESS CONTINUITY AND DISASTER RECOVERY MEASURES

In the event of a major failure situation, a warm standby data center with adequate infrastructure, connectivity and security is employed to conduct all disaster recovery procedures. For a worst-case scenario, the maximum RPO is two hours and the maximum RTO is four hours. Business continuity measures include:

- Databases are log shipped to a warm standby data center every hour.
- Operational copies of all application server tiers are maintained at the warm standby data center and are synchronized with their primary instances during each application deployment cycle.
- Warm standby system failover testing is performed at least once annually.
- Staging and production environments are backed up nightly. Backups are retained for two weeks at a secure onsite facility and are retrievable within 4 hours in the event of an emergency.

ADDITIONAL SECURITY

Wiley engages additional security measures such as security awareness training, periodic risk assessments and system health checks by third parties. Software Developers and Systems Administrators undergo annual role-specific security training based on OWASP vulnerabilities and operational best practices. All colleagues are required to complete security training during the onboarding process, and in addition to annual refresher training, periodic internal communications highlight relevant security topics. Wiley employs personnel who are subject matter experts and/or certified in:

- Information Security Management
- Network Security
- Windows Administration
- Database Administration
- Change Management
- Project Management
- ITIL Service Management

Privacy Shield Certified

TrustArc the new TRUSTe

OWASP Open Web Application Security Project

AICPA Service Organization Control Reports℠ AICPA SOC 2 Formerly SAS 70 Reports

GDPR The General Data Protection Regulation

WILEY