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 committed to comply with GDPR.

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®

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

WILEY

Frequently Asked Security Questions

Where do your servers physically reside? Are there any legal ramifications regarding our data privacy we should know about for having our data stored in that location?
Our primary data storage location is MN, USA, and our backup location is IA, USA. There has been new guidance from the EDPB to have additional measures in place if data is stored outside of Europe. This isn't a legal requirement, but many European companies are taking this seriously. Therefore, we have provided a mechanism for your clients to sign a DPA directly with Wiley (a DPA is one of the approved additional measures). If you'd like to take this route, there is more information available on MLC.

Who has access to our data in the cloud? What is your Wiley's policy for ensuring only authorized employees can access client data?
While we do not currently use any type of cloud storage, we do still limit access to customer data on an extremely limited, need-to-know basis. Every single Wiley employee with access to customer data has a defined business need for that access.

Can you share your standard service level agreement (SLA)?
This is not something that we currently have or can provide.

What uptime guarantees do you make in your standard service level agreement (SLA)?
We don't currently have an SLA, but our uptime is consistently 99.999% (5 nines).

What are your procedures for suspected security violations?
We have a full incident response program that involves escalation, investigation, remediation, and notification if deemed necessary. We follow all procedures in the case of *any* suspected incident.

Do you perform penetration testing and vulnerability testing on your systems? If so, when was the last test, and what were the results?
We perform monthly vulnerability scanning with a third party and occasional penetration testing on products as driven by business need. While we do not share results externally, we do commit to remediating any critical or high vulnerabilities within 30 days.

How do you protect access to GUI's and API's?
We have an extremely limited number of authorized administrators with access to our systems. Access is also fully logged and documented in our enterprise-level SIEM program.

What are your terms when it comes to ownership of data? How about any metadata we generate while using your service/platform/application?
This is available to view in detail in our privacy policy. Wiley acts as a subprocessor for personal data and so we will comply with requests for deletion from partners and their clients. We do retain unidentified, anonymized data on file for research aggregation purposes, but if it is daintified, it can no longer be traced to the individual. No personal information metadata is used or stored.

What are your security measures for protecting your data centers and other facilities?
Our datacenter is a Tier 3 co-location with a maintained SOC 2 Type II report. More information is available here: https://www.oneneck.com/it-security-services/secure-data-center

Which data transmissions do you encrypt?
All data is encrypted in transit using TLS 1.2 or higher.

What level of technical support is included in your standard SLA?
N/A

Do you have a disaster recovery plan? How often do you test it? In the case of a data center disaster, where do you backup our data?
Yes, we have a full DRP that is reviewed, tested, and updated (if needed) annually. We also maintain a DR warm site in Iowa, USA, that can support a cutover in less than 8 hours.

Do you have a statement about data accessibility per Section 508 of the US Rehabilitation Act?
Yes, see following page.

Statement on Section 508 of the U.S. Rehabilitation Act[1]

Everything DiSC®, The Five Behaviors of a Cohesive Team®, PXT Select™

Each year, nearly 2.5 million people complete Wiley assessments on the EPIC and PAC platforms and use our reports to improve their workplace relationships. This includes a number of individuals with disabilities. Because our assessments and reports are delivered online, we occasionally receive questions about Section 508 compliance from individuals with visual impairments.

The United States government states that this law requires federal agencies to "*make their electronic and information technology accessible to people with disabilities. Inaccessible technology interferes with an ability to obtain and use information quickly and easily. Section 508 was enacted to eliminate barriers in information technology, open new opportunities for people with disabilities, and encourage development of technologies that will help achieve these goals*." (This text is available at https://section508.gov/manage/laws-and-policies#508-policy.)

Although we are not required to maintain compliance with Section 508 regulations for disabilities, we value the goal of making our tools accessible and beneficial to every individual. Therefore, we have taken steps and offer the following recommendations to help those with visual impairments experience the benefits that our assessments can offer.

When taking an assessment on a PC, the response site can be magnified by holding Ctrl and using the mouse wheel or the plus key. The same can be accomplished on a MAC using the command key and the plus key together (⌘+). Another option is for a member of Human Resources to read questions aloud and mark answers. This is a common practice for taking our assessments if someone has difficulty viewing the items.

Our reports are delivered in PDF format and can interact through many programs, including those that help individuals with visual disabilities. Our PDFs are set to "Allow Content for Accessibility". With this setting, screen-reader software should be able to access content for those with visual impairments. One of the most common screen-reading programs is JAWS (Job Access with Speech), which provides speech and Braille output. However, some of the Everything DiSC® and The Five Behaviors of a Cohesive Team® reports utilize graphics that cannot be read by screen-reading software and have unusual paragraph breaks and bullet points that might cause the individual to lose their place. It might be helpful to prepare participants who are using screen readers with this information to ensure they are aware of these issues.

[1] http://www.section508.gov/

WILEY