mesearchr
SECURITY STATEMENT

This Security Statement is aimed at being transparent about our security infrastructure and practices, to help reassure you that your data is appropriately protected. Visit our privacy policy for more information on data handling.

USER SECURITY

Authentication: User data on our database is logically segregated by account-based access rules. User accounts have unique email addresses and passwords that must be entered each time a user logs on. Mesearchr issues a session cookie to record encrypted authentication information for the duration of a specific session. The session cookie does not include the password of the user.

Passwords: User application passwords have minimum complexity requirements. Passwords are individually salted and hashed.

Data Encryption: Certain sensitive user data, such as credit card details are stored in encrypted format.

Data Portability: Mesearchr enables you to export your survey data from our system in a variety of formats so that you can back it up, or use it with other applications.

Privacy: We have a comprehensive privacy policy that provides a very transparent view of how we handle your data, including how we use your data, who we share it with, and how long we retain it.

Data Residency: All Mesearchr user data is stored on servers located in the United States.

PHYSICAL SECURITY

All Mesearchr information systems and infrastructure are hosted in world-class data centers. These data centers include all the necessary physical security controls you would expect in a data center these days (e.g., 24×7 monitoring, cameras, visitor logs, entry requirements). For further information on the security practices please refer to the AWS Security Whitepaper.

AVAILABILITY

Connectivity: Fully redundant IP network connections with multiple independent connections to a range of Tier 1 Internet access providers.

Fire Detection and Suppression: Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Power: The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

Climate and Temperature: Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Management: The data centre monitors electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

Uptime: Continuous uptime monitoring, with immediate escalation to Mesearchr staff for any downtime.

Backup Frequency: Our database is backed-up multiple times per hour and uses full transaction logging for recovery between backups. Backups are stored in different availability zones to the databases.

NETWORK SECURITY

Testing: System functionality and design changes are verified in an isolated test "sandbox" environment and subject to functional and security testing prior to deployment to active production systems.

Firewalls: Firewalls restrict access to all ports except 80 (http) and 443 (https) for external IP addresses. Specific ports that facilitate admin and maintenance are locked down to specific IP addresses within our trusted network.

Access Control: Restricted firewall access via trusted IP addresses, and role- based access is enforced for systems management by authorized engineering staff.

Logging and Auditing: AWS central logging systems capture and archive all internal systems access including any failed authentication attempts.

rating on SSL Labs' tests. We also employ Forward Secrecy and only support strong ciphers for added privacy and security.

VULNERABILITY MANAGEMENT

Patching: Latest security patches are applied to all operating systems, applications, and network infrastructure to mitigate exposure to vulnerabilities.

Third Party Scans: Latest security patches are applied to all operating systems, applications, and network infrastructure to mitigate exposure to vulnerabilities.

ORGANIZATIONAL & ADMINISTRATIVE SECURITY

Information Security Policies: We maintain internal information security policies, including incident response plans, and regularly review and update them.

Employee Screening: We perform background screening on all employees, to the extent possible within local laws.

Training: We provide security and technology use training for employees.

Service Providers: We screen our service providers and bind them under contract to appropriate confidentiality and security obligations if they deal with any user data.

Access: Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis.

Audit Logging: We maintain and monitor audit logs on our services and systems.systems.

SOFTWARE DEVELOPMENT PRACTICES

Stack: We code in C#, Java and NodeJS and run on SQL Server, Windows and Node.

Coding Practices: Our engineers use best practices and industry-standard secure coding guidelines which align with the OWASP Top 10.

Deployment: We deploy code multiple times during the week, giving us the ability to react quickly in the event a bug or vulnerability is discovered within our code.quickly in the event a bug or vulnerability is discovered within our code.

HANDLING OF SECURITY BREACHES

Despite best efforts, no method of transmission over the Internet and no method of electronic storage is perfectly secure. We cannot guarantee absolute security. However, if Mesearchr learns of a security breach, we will notify affected users so that they can take appropriate protective steps. Our breach notification procedures are consistent with our obligations under various state and federal laws and regulation, as well as any industry rules or standards that we adhere to. Notification procedures include providing email notices or posting a notice on our website if a breach occurs.

CUSTOMER REQUESTS

Due to the number of customers who use our service, specific security questions or custom security forms can only be addressed for customers purchasing a certain volume of user accounts within a Mesearchr subscription. If your company has a large number of potential or existing users and is interested in exploring such arrangements, please contact us.

Last updated: September 15, 2017.