Scope of TOMs:

1. UserTesting Human Insight Platform app.usertesting.com
2. UserZoom Manager - manager.userzoom.com
3. EnjoyHQ - app.enjoyhq.com

Link to UserTesting TOMs as listed below -
https://www.usertesting.com/privacy-center/data-processing-agreement

UserTesting's Information Security is centrally managed by its Information Security team. The UserTesting Information Security team's responsibilities include the management of information security across all global locations, all UserTesting products and services and engagement of UserTesting Subprocessors.

UserTesting will comply with the following:

1. Security Governance

a. UserTesting's security policy is approved by its executive team and formally reviewed annually. It requires that all employees be trained on their responsibilities in protecting personal and confidential information. New employees are trained during orientation. All employees are required to refresh their training at least yearly.

b. UserTesting has obtained SOC 2 Type 2 certification for the Human Insight Platform, UserZoom Manager, and EnjoyHQ. The certification report is shared upon request from customers and prospects (under NDA). UserTesting is also self-certified under Privacy Shield although we do not rely on Privacy Shield as a legal basis for transfers of Customer Personal Data.

2. Service Authentication

a. Complex passwords are required for Customer and Contributor access. Passwords must be at least 8 characters long and must contain at least one uppercase letter, one lowercase letter, and one digit. They may also contain special characters.

b. Users are logged out of the system after periods of inactivity.

c. When users create new accounts, they create their own secure passwords. When existing users create accounts for others, the new users are invited by email and are then asked to create their own secure passwords.

d. Lost passwords are not retrievable but can be reset by the user by responding to an email sent to the account's email address that is already on record.

e. Accounts are locked if a user fails to supply a valid password.

3. Single Sign-on

UserTesting also supports login via single sign-on using SAML 2.0 protocols. This enables customers to implement additional security requirements for passwords and the login process.

4. Multi-factor authentication (MFA) for internal accounts

UserTesting requires that internal email and development accounts use MFA.

5. Data Hosting and Encryption

a. All confidential and proprietary data (including video files, Customer and Contributor data) are hosted through Amazon Web Services (AWS). AWS is a SOC 2 and ISO 27017 certified hosting provider.

b. All data is encrypted at rest and in transit. Data is stored in encrypted form using 256-bit AES encryption. Encryption keys are managed by AWS Key Management Services.

c. All communication to and from the data center is encrypted (TLS 1.2 or greater required).

6. Vulnerability Scanning

UserTesting performs quarterly vulnerability scans on infrastructure devices, servers, and user computers. Cloud infrastructure, virtual instances, web applications, and production code changes are scanned for vulnerabilities to ensure weaknesses are identified fast, and vulnerabilities remediated quickly.

7. Prototype, Image and Asset Hosting

UserTesting is able to host some web assets used during tests. The assets are encrypted at rest and only accessed through SSL. These are kept securely in our AWS infrastructure and only accessible through secure links that are inactive unless the test is in progress and used by the assigned, active contributor.

8. Data Lifecycle Management

Unless UserTesting is required by law to retain a copy of Customer Content, UserTesting will delete Customer Personal Data upon request from Customer.

9. Personnel Security

a. To the extent permitted by law, UserTesting ensures that background checks are conducted on all employees and contractors. The nature of such checks varies from jurisdiction to jurisdiction.

b. Employees who leave the company or change business roles will have their access privileges revoked or modified within 24 hours.

10. Clean Desk Policy

UserTesting's clean desk policy mandates that employees keep all confidential information stored in a secure location and never left unattended in workspaces.

11, Facility Security

All UserTesting's office locations are secured by keycard locks that are assigned to individual employees and are monitored by video at all times. Visitors must sign in and be escorted at all times. Physical security audits are performed annually.

12. System Development

a. UserTesting builds its platform using an agile development methodology that releases small changes frequently after peer review and testing.

b. Every change that is built runs first on a local system. Changes are peer reviewed and then tested on non-production systems. After all tests are passed, and peer reviews completed, changes are deployed to the production system. Each change is processed by static analysis tools that look for known vulnerabilities in any component used. Tests are performed on separate systems (built the same way) but using seed data or obfuscated production data so that tests may be performed without risking the production system.

c. Deployment is managed by automated tools. The scripts that drive the tools are also kept under change control.

d. Virtual instances are checked nightly and critical software patches are applied as necessary.

e. Data owned by Customers is not used outside of production. Exceptions are made when troubleshooting issues where real data is relevant and even then the data is first anonymised to prevent exposure of the personal information of Customers and Contributors.

13. Network and Device Security

a. UserTesting employs firewalls to protect our internal systems. Access to admin and hosting systems requires secure login to a centrally managed VPN.

b. Wireless access within the site requires corporate credentials. Other computers and mobile devices use an alternative access point that is outside the firewall.

c. Company-owned computers are managed and kept up-to-date with the latest operating system, antivirus, and productivity software updates.

d. BYOD (Bring your own device) are allowed in limited circumstances and computers must meet the above company standards to be used for business purposes.

e. All production systems are backed up to geographically diverse AWS data centers and securely stored in encrypted form.

14. Security Audits

UserTesting requires an annual, independent security audit of both internal systems and the platform. Copies of the most recent audit reports are available upon request.

15. Logging

System activity is centrally logged. Logs are kept for a minimum of 12 months in ways that make them virtually impossible to tamper with.

16. Intrusion Detection, Prevention and Incident Response

System accesses are monitored and logged. Alerts are investigated by engineers according to an incident response plan. The plan is designed to effectively escalate incidents to the appropriate level of authority, ensuring quick fixes followed up with a root cause analysis and work plan, to prevent future incidents. The incident response plan is reviewed annually.

17. Web Application Firewall (WAF)

UserTesting employs a WAF implemented using AWS WAF platform to prevent certain kinds of common attacks. AWS automatically updates the managed rules as new exploits and bad actors emerge.

18. Data Loss Prevention (DLP)

UserTesting deploys DLP tools on company workstations to track and alert when unusual activity is detected. Additional DLP tools are deployed in critical cloud infrastructure.

19. Service Providers

UserTesting uses a number of third parties to deliver its full platform of services. Most do not have access to a Customer's confidential information (including personal data). Any that do are

subject to annual security reviews and are obligated by contract to provide a security posture that is at least as stringent as what we provide directly.

20. Business Continuity

Business continuity is included as part of UserTesting's security policy. The platform has been designed to be robust and recoverable.

- The platform is hosted on multiple servers running in AWS with load balancing and failover provisions
- Instances can be spun up as needed if one fails
- Videos are stored in journaled S3 buckets
- Videos are stored in at least two geographically-diverse data centers
- Databases are backed-up to alternate data centers.
- Data centers are located in geographically-diverse locations for the purposes of data redundancy, in the case of a catastrophic event

21. Responses to Government requests for information

In the event that UserTesting receives a government request for confidential information belonging to a Customer (including personal data), unless prohibited by applicable law, it shall take reasonable steps to notify the relevant Customer before responding to such request.