WhatsApp

WhatsApp Business Data Security Terms ("Data Security Terms")

These terms do not take effect until October 29, 2020 at 5PM UTC/10AM PT.

These WhatsApp Business Data Security Terms ("Data Security Terms") apply in respect of WhatsApp's provision of Business Services to you in accordance with the Business Terms. Capitalized terms used but not defined in these Data Security Terms have the meanings given in the Business Terms. These Data Security Terms describe the minimum security standards that WhatsApp maintains applicable to the Business Services made available under the Business Terms, including the data you send to WhatsApp using the Business Services ("Covered Data").

1. Organization of Information Security. WhatsApp has personnel responsible for oversight of security of the Business Services.

2. Physical and Environmental Security. WhatsApp's security measures will include controls designed to provide reasonable assurance that physical access to physical processing facilities under WhatsApp's control that are used to provide the Business Services ("Data Processing Facility") is limited to authorized persons and that environmental controls are established to detect, prevent, and control destruction due to environmental hazards. The controls will include:

a. Logging and auditing of physical access to the Data Processing Facility by employees and contractors;

b. Camera surveillance systems at the Data Processing Facility;

c. Systems that monitor and control the temperature and humidity for the computer equipment at the Data Processing Facility;

d. Power supply and backup generators at the Data Processing Facility;

e. Procedures for secure deletion and disposal of data, subject to the Business Terms; and

f. Protocols requiring ID cards for entry to all WhatsApp facilities for all personnel working on the Business Services.

3. Personnel

Training. WhatsApp will ensure that all personnel with access to Covered Data undergo security training.

g. Confidentiality. WhatsApp will contractually bind personnel with access to Covered Data to appropriate confidentiality requirements.

h. Screening and Background Checks. WhatsApp will have a process for:

   i. verifying the identity of the personnel with access to Covered Data; and

   ii. performing background checks, where legally permissible, on personnel working on or supporting aspects pertaining to the Business Services in accordance with WhatsApp standards.

i. Personnel Security Breach. WhatsApp will take disciplinary action in the event of unauthorized access to Covered Data by WhatsApp personnel, including, where legally permissible, punishments up to and including termination.

4. Security Testing. WhatsApp will perform regular security and vulnerability testing to assess whether key controls are implemented properly and are effective.

5. Access Control.

a. Password Management. WhatsApp has established and will maintain procedures for password management for its personnel, designed to ensure passwords are personal to each individual, and inaccessible to unauthorized persons, including at minimum:

i. password provisioning, including procedures designed to verify the identity of the user prior to a new, replacement, or temporary password;

ii. cryptographically protecting passwords when stored in computer systems or in transit over the network;

iii. altering default passwords from vendors;

iv. strong passwords relative to their intended use; and

v. education on good password practices.

b. Access Management. WhatsApp will also control and monitor its personnel's access to its systems using the following:

i. established procedures for changing and revoking access rights and user IDs, without undue delay;

ii. established procedures for reporting and revoking compromised access credentials (passwords, tokens etc.);

iii. maintaining appropriate security logs including where applicable with userid and timestamp;

iv. synchronizing clocks with NTP; and

v. Logging the following minimum user access management events:

a. Authorization changes;

b. Failed and successful authentication and access attempts; and

c. Read and write operations.

6. Communications Security.

a. Network Security

i. WhatsApp will employ technology that is consistent with industry standards for network segregation.

ii. Remote network access to WhatsApp systems will require encrypted communication via secured protocols and use of multi-factor authentication.

b. Protection of Data in Transit

i. WhatsApp will enforce use of appropriate protocols designed to protect the confidentiality of data in transit over public networks.

7. Vulnerability Managment. WhatsApp has instituted and will maintain a vulnerability management program covering the Business Services that includes definitions of roles and responsibilities for vulnerability monitoring, vulnerability risk assessment, and patch deployment.

8. Security Incident Management

a. Security Incident Response. WhatsApp will maintain a security incident response plan for monitoring, detecting, and handling possible security incidents affecting Covered Data. The security incident response plan at least includes definitions of roles and responsibility, communication, and post-mortem reviews, including root cause analysis and remediation plans.

b. Monitoring. WhatsApp will monitor for any security breaches and malicious activity affecting Covered Data.

In the event of any express conflict between the Business Terms and these Data Security Terms, the Business Terms will govern solely with respect to your use of the Business Services and solely to the extent of the conflict. WhatsApp may update these Data Security Terms from time to time to reflect evolving security standards.