Encryption Policy

Beyond

August 2023

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.9

Table 2: Document history

Date	Comment
Aug 14 2023	Initial document
Aug 18 2023	Initial review

1 Purpose and Scope

a. This policy defines organizational requirements for the use of cryptographic controls, as well as the requirements for cryptographic keys, in order to protect the confidentiality, integrity, authenticity and nonrepudiation of information.

b. This policy applies to all systems, equipment, facilities and information within the scope of Beyond's information security program.

c. All employees, contractors, part-time and temporary workers, service providers, and those employed by others to perform work on behalf of Beyond having to do with cryptographic systems, algorithms, or keying material are subject to this policy and must comply with it.

2 Background

a. This policy defines the high level objectives and implementation instructions for Beyond's use of cryptographic algorithms and keys, the specific algorithms approved for use, requirements for key management and protection, and requirements for using cryptography in cloud environments.

3 Policy

a. Beyond must protect individual systems or information by means of cryptographic controls as defined in Table 3:

Name of System/ Type of Info	**Cryptographic Tool**	**Encryption Algorithm**	**Key Size**
Server disk-level encryption	GCP Compute Engine	AES-256	256-bit key
Users endpoint Devices	FileVault & Bitlocker	XTS-AES AES-256	256-bit key
Virtual Private Network (VPN)	Wireguard	ChaCha20 & Others	
Application on public networks	nginx/OpenSSL	TLS v1.1+ EECDH/EDH/AES	

Table 3: Cryptographic Controls

a. Except where otherwise stated, keys must be managed by their owners.

b. Cryptographic keys must be protected against loss, change or destruction by applying appropriate access control mechanisms to prevent unauthorized use and backing up keys on a regular basis.

c. When required, customers of Beyond must be able to obtain information regarding:

   i. The cryptographic tools used to protect their information.

   ii. The identity of the countries where the cryptographic tools are used to store or transfer cloud service customers' data.

d. The use of organizationally-approved encryption must be governed in accordance with the laws of the country, region, or other regulating entity in which users perform their work. Encryption must not be used to violate any laws or regulations including import/export restrictions. The encryption used by the Company conforms to international standards and U.S. import/export requirements, and thus can be used across international boundaries for business purposes.

e. All key management must be performed using software that automatically manages access control, secure storage, backup and rotation of keys. Specifically:

f. The key management service must provide key access to specifically-designated users, with the ability to encrypt/decrypt information and generate data encryption keys.

g. The key management service must provide key administration access to specifically-designated users, with the ability to create, schedule delete, enable/disable rotation, and set usage policies for keys.

h. The key management service must store and backup keys for the entirety of their operational lifetime.