Encryption Management

Procedure

|  |  |
| --- | --- |
| Owner |  |
| Approver |  |
| Last Reviewed |  |

### Scope and applicability

The Encryption management procedure applies to all [Company Name]'s highly confidential and confidential information. Encryption protection must be applied at any storage means (servers, laptops, removable media) and while transmitting through any channels (web, internal network, etc.).

### Encryption standards Data Transmission

[Company Name] uses [Cloud Hosting Service] for its production infrastructure. The provider automatically encrypts all VM-to-VM traffic within a VPC network and peered VPC.

The Engineering team configures encryption of data channels of [Company Name]ʼs applications between end-users and applications backend, following the encryption standards:

|  |  |
| --- | --- |
| **Encryption method** | **[Company Name]ʼs standard** |
| Transport Layer Security | TLS 1.2 |
| Secure Copy Protocol | At least AES128 |
| Digital | DSA, with key size of at least 1024 |

|  |  |
| --- | --- |
| Signatures | RSA, with key size of at least 1024 |

## Data Storage

[Cloud Hosting Service], on which [Company Name]'s customers' data resides, encrypts all customer content stored at rest using AES256, except a small number of Persistent Disks created before 2015 that use AES128. Data for storage is split into chunks, and each chunk is encrypted with a unique data encryption key. These data encryption keys are stored with the data, encrypted with ("wrapped" by) key encryption keys exclusively stored and used inside [Cloud Hosting Service]'s central Key Management Service. [Cloud Hosting Service]'s Key Management Service is redundant and globally distributed.

The Engineering team configures additional encryption of data, following the encryption standards:

|  |  |
| --- | --- |
| **Encryption method** | **[Company Name]ʼs standard** |
| Advanced Encryption Standard AES | AES128 and AES256 |
| Secure Hash Algorithm  SHA | SHA 2 and SHA 3 |
| Secure Password Storing | bcrypt hashing function |

## Exceptions

Requests for an exception in the [Company Name]ʼs production environment must be submitted to the VP of Engineering for approval. Requests for an exception in [Company Name]ʼs IT environment must be submitted to the Director of Engineering, Operations. They record information about the approved exception in their teamsʼ working space.

# Key management standards

[Company Name] uses the cryptographic keys in the following cases:

**Responsibility**

**Case**

|  |  |
| --- | --- |
| To protect customersʼ data in [Cloud Hosting Service] | [Cloud Hosting Service] is responsible for key management |
| Web certificate for the [Company Name]ʼs website | Certification authority CA is responsible for key management |
| During usage of different vendorsʼ services | Vendors are responsible for key management |

Further, the procedure defines the requirements for key management for which [Company Name]ʼs internal teams are responsible.

## Keys generation and distribution

Engineers use [Company Name]ʼs internal application to generate SSH keys to access the production environment. Engineers use their own keys to authenticate to specific servers. The engineers do not obtain direct access to the keys.

## Keys revocation/destruction

Once the information has been re-keyed with a new key or keys are compromised, all copies must be destroyed.

## Keys storage

Tunnel SSH keys are stored within the [Company Name]ʼs internal application. Upon expiry, keys are automatically deleted.

Application security keys are backed up within key management systems used by [Company Name].

# Violations & Enforcement

Any known violations of this procedure should be reported to the VP of Engineering. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action according to company procedures, including termination of employment.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Author** | **Approved by** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |