
Cryptographic Key
Management Policy
Vizle

by the ISO 27001 scope statement.

Cryptographic Key Management Policy

Principle

Cryptographic Key Management is based on the OWASP guidelines - https://cheatsheetseries.owasp.org/cheatsheets/Key_Management_Cheat_Sheet.html

Cryptographic keys are classified as Confidential.

Generation

Cryptographic keys shall be generated within cryptographic module with at least a FIPS 140-2 compliance. For explanatory purposes, consider the cryptographic module in which a key is generated to be the key-generating module.

Escrow and Backup

Data that has been encrypted with lost cryptographic keys will never be recovered. Therefore, it is essential that the application incorporate a secure key backup capability, especially for applications that support data at rest encryption for long-term data stores.

When backing up keys, ensure that the database that is used to store the keys is encrypted using at least a FIPS 140-2 validated module. It is sometimes useful to

escrow key material for use in investigations and for re-provisioning of key material to users if the key is lost or corrupted.

Key Compromise and Recovery

The compromise of a key has the following implications:

In general, the unauthorized disclosure of a key used to provide confidentiality protection (i.e., via encryption) means that all information encrypted by that key could be exposed or known by unauthorized entities. The disclosure of a Certificate of Authorities' private signature key means that an adversary can create fraudulent certificates and Certificate Revocation Lists (CRLs).

A compromise of the integrity of a key means that the key is incorrect - either that the key has been modified (either deliberately or accidentally), or that another key has been substituted; this includes a deletion (non-availability) of the key. The substitution or modification of a key used to provide integrity calls into question the integrity of all

Policy Compliance

Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions