



Cryptographic Key Management Policy

Vizle





<https://vizle.offnote.co>

Contact us: vizle@offnote.co

This document was generated automatically by **Vizle**

Your **Personal Video Reader Assistant**

Learn from Videos **Faster** and **Smarter**

VIZLE PRO / BIZ

- Convert *entire* videos ^{PDF, PPT}
- *Customize* to retain all essential content
- Include Spoken *Transcripts*
- Customer support

Visit <https://vizle.offnote.co/pricing> to learn more

VIZLE FREE PLAN

- Convert videos *partially* ^{PDF only}
- Slides may be *skipped**
- Usage restrictions
- No Customer support

Visit <https://vizle.offnote.co> to try free

Login to Vizle to unlock more slides*



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.

Last Reviewed: [Last Reviewed] Page 5 of 15

Document Owner: [Document Owner]



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

Last Reviewed: [Last Reviewed]

Page 7 of 15

Document Owner: [Document Owner]



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



Microsoft Word interface showing a document titled "CRYPTOGRAPHIC KEY MANAGEMENT POLICY".

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

Last Reviewed: [Last Reviewed] Page 10 of 15
Document Owner: [Document Owner]

Vizle

CRYPTOGRAPHIC KEY MANAGEMENT POLICY
Version: [Version Number] Classification: Internal



Microsoft Word interface showing a document titled "CRYPTOGRAPHIC KEY MANAGEMENT POLICY".

Page 14 of 15

Last Reviewed: [Last Reviewed]

Document Owner: [Document Owner]

CRYPTOGRAPHIC KEY MANAGEMENT POLICY

Version: [Version Number] Classification: Internal

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

Vizle logo watermark is visible across the page.



<https://vizle.offnote.co>

Contact us: vizle@offnote.co

This document was generated automatically by **Vizle**

Your **Personal Video Reader Assistant**

Learn from Videos **Faster** and **Smarter**

VIZLE PRO / BIZ

- Convert *entire* videos ^{PDF, PPT}
- *Customize* to retain all essential content
- Include Spoken *Transcripts*
- Customer support

Visit <https://vizle.offnote.co/pricing> to learn more

VIZLE FREE PLAN

- Convert videos *partially* ^{PDF only}
- Slides may be *skipped**
- Usage restrictions
- No Customer support

Visit <https://vizle.offnote.co> to try free

Login to Vizle to unlock more slides*