Data masking

ISO 27002 Control 8.11

Control

Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration

Purpose

To limit the exposure of sensitive data including PII, and to comply with legal, statutory, regulatory and contractual requirements

Why is it important?

- Data masking protects sensitive data exposure, especially PII
- Anonymization irreversibly alters data, preventing identification
- Pseudonymization, while weaker, is useful for statistical research while protecting the alias algorithm
- Ensures compliance with legal requirements regarding data presentation

Which topics should be addressed ?

- Limiting the exposure of sensitive data including PII, using masking, pseudonymization, or anonymization techniques
- Compliance with legal, statutory, regulatory and contractual requirements (e.g., requiring masking of payment card information)
- Verifying that data has been adequately pseudonymized or anonymized (considering all elements)
- Access controls and restrictions on the usage of processed data (e.g., prohibiting collating to identify the PII principal)

How can it be implemented ?

- Establish a topic-specific policy on access control considering masking needs
- Implement data masking, pseudonymization or anonymization where protection of sensitive data is a concern
- Verify data is adequately anonymized or pseudonymized (considering all sensitive elements)
- Define access controls and agreements on usage of the processed data (e.g., prohibiting collating processed data with other information)

Link with other frameworks

- NIST 800-53 rev5 : AC-4(23), SI-19(4)
- NIST CSF 2.0 : NA

Renaud Dardenne
Asphalia Consulting