Data Security and Privacy Compliance Guidelines

작성자: Anonymous Author

날짜: 2023-10-25

목차

ZETA CUBE
The Solution leader for ZiB Storage

1 Summary

This report outlines critical guidelines for safeguarding personal information, adhering to regulatory standards, and enhancing system security to prevent data breaches.

ZETA CUBE
The Solution leader for ZiB Storage

2 Data Security Measures

Effective data security requires a multi-layered approach, balancing compliance with operational efficiency.

2.1 Output Minimization and Immediate Collection

When printing sensitive data, limit output fields to essential business needs and retrieve printed materials immediately to reduce exposure risk.

2.2 Avoiding Guessable Passwords and Identifiers

Reject sequential numbers, birthdays, or company/test names as passwords or identifiers. Enforce complex, unique credentials to prevent brute-force attacks.

ZETA CUBE
The Solution leader for ZiB Storage

2.3 Preventing Data Inference

Avoid exposing easily traceable data points like company names in logs. Use hashing or pseudonymization to obscure sensitive information during testing.

2.4 Secure System Configurations

Implement multi-condition search filters (e.g., date + name) for data retrieval systems. Encrypt wallet keys (private keys, passphrases) in logs if unavoidable.

2.5 FATF Transaction Monitoring

Adhere to FATF guidelines by scrutinizing transactions for anomalies (e.g., high-value/low-frequency transfers) and verifying sender/receiver profiles and fund sources.

ZETA CUBE
The Solution leader for ZiB Storage

3 Conclusion

By integrating these measures, organizations can mitigate risks while maintaining regulatory compliance. Continuous monitoring and employee training are essential for sustained security.

ZETA CUBE
The Solution leader for ZiB Storage