Data Security and Privacy Compliance Protocols

ZETA CUBE

The Solution leader for ZiB Storage

작성자: Security Compliance Team

날짜: 2023-10-05

목차

1 Summary 2

2 Key Compliance Measures 3

2.1 Output Management 3

2.2 Password Security 3

2.3 Data Redaction 3

2.4 Log Encryption 3

2.5 Data Retrieval Controls 4

3 Conclusion 5

1 Summary

This report outlines critical measures for safeguarding personal information and ensuring regulatory compliance. Key areas include output management, password security, data redaction, log encryption, and data retrieval controls.

2 Key Compliance Measures

The following subsections detail essential protocols to prevent data breaches and ensure privacy adherence.

2.1 Output Management

When printing documents containing personal data, limit output to essential information and collect materials immediately to reduce exposure risks.

2.2 Password Security

Avoid using predictable passwords (e.g., birthdays, phone numbers) and ensure credentials are not similar to user IDs to enhance account security.

2.3 Data Redaction

Prevent unauthorized inference by avoiding test names, company names, or other easily guessable identifiers in sensitive contexts.

2.4 Log Encryption

Encrypt wallet-related keys (e.g., private keys, passphrases) in system logs to protect against unauthorized access if logs are exposed.

2.5 Data Retrieval Controls

Implement multi-condition searches (e.g., two-factor verification) to restrict access to sensitive user data and prevent over-fetching.

3 Conclusion

Adherence to these protocols is critical for maintaining trust and compliance with global standards like FATF guidelines. Regular audits and incremental backups ensure data integrity and recovery readiness.