Data Security and Privacy Management Guidelines

작성자: Security Compliance Team

날짜: 2023-10-25

목차

1 Summary

This report outlines critical security measures to protect sensitive data and comply with regulatory standards. Key strategies include output minimization, secure credential management, encryption protocols, and structured data retrieval systems.

2 Key Security Measures

Implementing these protocols ensures minimal exposure of sensitive information while maintaining operational efficiency and regulatory adherence.

2.1 Minimizing Output Exposure

When printing personal information, limit output to essential fields and collect physical outputs immediately after printing to prevent unauthorized access.

2.2 Avoiding Predictable Credentials

Do not use sequential numbers, birthdays, phone numbers, or company names for passwords/IDs. Ensure passwords do not resemble user IDs to reduce guessability.

2.3 Secure Logging Practices

Prevent wallet keys, encryption keys, or passphrases from appearing in logs. Encrypt logs containing sensitive data if unavoidable.

2.4 Wallet Security Protocols

Ensure no user identification (resident numbers, member IDs) is included in logs. Protect wallet-related data during backups and audits.

2.5 Data Retrieval and Backup Controls

Implement dual-factor search conditions for data retrieval. Follow FATF guidelines on transaction size, profiles, and source of funds. Use full backup initially, then differential backups, and destroy sensitive data after a retention period.

3 Conclusion

Adhering to these guidelines minimizes data breach risks and ensures compliance with global financial regulations. Regular audits and staff training reinforce these critical security practices.