

ZETACUBE INC Security and Data Management Guidelines



작성자: ZETACUBE INC

날짜: April 17, 2025

목차

1	Summary	2
2	Security and Data Management Guidelines	3
2.1	Personal Data Handling Procedures	3
2.2	Software Development Security Requirements	3
2.3	Data Backup and Review Protocols	3
2.4	Business Continuity Assurance	3
2.5	Internal Control and Compliance	4
3	Conclusion	5



1 Summary

This report outlines security and data management protocols for ZETACUBE INC, focusing on minimizing personal data exposure, ensuring software development standards, and safeguarding business continuity through robust data practices.



2 Security and Data Management Guidelines

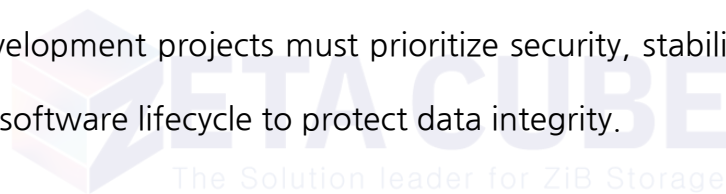
ZETACUBE INC mandates strict adherence to security protocols during software development and data handling to protect sensitive information and ensure operational resilience.

2.1 Personal Data Handling Procedures

Outputs containing personal data must be minimized to job-related information and collected immediately to prevent unauthorized access.

2.2 Software Development Security Requirements

All software development projects must prioritize security, stability, and reliability throughout the software lifecycle to protect data integrity.



2.3 Data Backup and Review Protocols

Regular reviews and backups of information system logs and data are essential to ensure data integrity and recovery capabilities.

2.4 Business Continuity Assurance

Strategies to maintain uninterrupted business operations during disruptions are critical to minimizing potential losses.

2.5 Internal Control and Compliance

Strict access controls and regulatory compliance are enforced to safeguard sensitive information and maintain organizational trust.



3 Conclusion

By implementing these guidelines, ZETACUBE INC ensures secure software development, effective data management, and operational resilience, aligning with industry standards and legal requirements.

