ZetaCube Data Security and Privacy Control Policies

작성자: Anonymous

날짜: April 17, 2025

목차

1 Summary

This report outlines ZetaCube's policies for securing and managing information systems, emphasizing the minimization of personal data exposure, password security, and controlled access to sensitive data to ensure business continuity and mitigate risks.

2 Key Policies and Measures

The guidelines focus on safeguarding company data by restricting personal information in outputs, enforcing strong password practices, and controlling access to system logs and backups.

2.1 Minimizing Personal Information in Outputs

Outputs containing personal data must be limited to essential business needs, and materials should be collected immediately after use to prevent unauthorized access.

2.2 Avoiding Guessable Passwords

Passwords should not resemble user IDs, sequential numbers, birthdays, or phone numbers to reduce vulnerability to brute-force attacks.

2.3 Access Control to Logs and Data

Access to system logs and data is restricted to authorized personnel, with controls in place to ensure data integrity and prevent unauthorized modifications.

2.4 Anonymizing User Identification

Logs must exclude user identifiers such as resident registration numbers or membership IDs to protect individual privacy.

2.5 Immediate Collection of Output Materials

Physical or digital outputs containing sensitive data must be retrieved promptly after use to minimize exposure risks.

3 Conclusion

ZetaCube's policies prioritize data security through strict access controls, password hygiene, and minimization of personal information exposure, ensuring compliance with privacy standards and operational resilience.