# Secure Design Report: SK Telecom Data Breach

# Luke Matsui | COSE354: Information Security | October 30, 2025

## 1) Violation of Security Principles

### Plain-text Credential Storage

The investigation revealed systematic plain-text credential storage, where "Server A held—in unencrypted form—the IDs and passwords of other management-subnet hosts" and "Server B, in turn, stored plain-text admin credentials for the HSS management server" (MSIT, 2025). This failure allowed attackers to easily harvest and reuse credentials across multiple systems, enabling the breach to escalate from initial access to critical authentication systems.

**Principle Violations:**

* **Safe Defaults:** Systems defaulted to storing credentials in plain text rather than encrypted form as the baseline security posture
* **Complete Mediation:** Credential validation mechanisms did not enforce proper protection throughout the credential lifecycle, allowing stolen credentials to be reused across system boundaries
* **Open Design**: Security relied on secrecy of data storage locations rather than proper cryptographic protection of the data itself

According to MITRE CWE-256/312, plain-text storage of credentials violates fundamental security practices by exposing sensitive authentication data to unauthorized access, creating a single point of failure that can compromise entire systems.

### Inadequate Security Governance and Access Control

The investigation found "fragmented governance" where "SK Telecom's CISO covered only the IT domain (57% of assets), leaving the network domain (43%) under separate supervision" (MSIT, 2025).

**Principle Violations:**

* **Separation of Duties:** Security responsibilities were improperly divided without clear accountability structures
* **Least Privilege:** The attacker maintained “long-term persistence” because “administrative passwords had no expiry and had not been rotated for years.”

## 2) Design Suggestions Based on Security Principles

### Comprehensive Credential Management System

**Safe Defaults Implementation:**

* As MSIT recommended, "restrict any recording of passwords and, if unavoidable, store them in encrypted form while introducing multi-factor authentication" (MSIT, 2025)
* Additionally, following CWE-798 recommendations, eliminate hard-coded credentials and implement secure credential management systems with proper key rotation and maximum lifespan policies to prevent credential reuse attacks.

### Data Protection by Design

**Safe Defaults and Open Design:**

* Encrypt all sensitive data including USIM authentication keys using industry-standard algorithms as the default configuration.
* Implement proper key management with regular rotation schedules and hardware security modules for master key protection.

### Unified Security Governance Framework

**Separation of Duties and Least Privilege:**

* Establish single CISO with enterprise-wide authority and direct CEO reporting as required by "Article 45-3 of the Network Act" (MSIT, 2025)
* Implement role-based access control with minimum necessary privileges across all domains, preventing credential reuse across system boundaries
* Develop zero-trust architecture with continuous authentication validation to enforce complete mediation of all access attempts

## Conclusion

The SK Telecom breach shows catastrophic failures across multiple security principles, but most severely and importantly in Safe Defaults and Complete Mediation. The massive scale of this breach, which affected nearly 27 million subscribers, highlights the huge importance of proper security design in telecommunications infrastructure. By addressing the root causes identified in the official investigation and implementing security by design principles, organizations like SK Telecom can build resilient security architectures that prevent similar breaches. The incident serves as a reminder that, as one analysis noted, "market dominance demands heightened accountability and customer care" (Law and Ethics in Tech, 2025), requiring robust security practices regardless of market position.

## Works Cited

MSIT. "MSIT Releases Final Investigation Results on SK Telecom Data Breach." Ministry of Science and ICT, 2025, https://www.msit.go.kr/eng/bbs/view.do;jsessionid=A2aV3fQR4zqYv-G8cJpkDgnrgrACDgREHvXAqG5l.AP\_msit\_2?sCode=eng&nttSeqNo=1139&bbsSeqNo=42&mId=4&mPid=2

Law and Ethics in Tech. "Lessons from the SKT Hack: A Wake-Up Call for Digital Security and Corporate Responsibility." Medium, 2025, https://lawnethicsintech.medium.com/lessons-from-the-skt-hack-a-wake-up-call-for-digital-security-and-corporate-responsibility-9aa90b3ced41

MITRE Corporation. "CWE-256: Plaintext Storage of Credentials." Common Weakness Enumeration, https://cwe.mitre.org/data/definitions/256.html

MITRE Corporation. "CWE-312: Cleartext Storage of Sensitive Information." Common Weakness Enumeration, https://cwe.mitre.org/data/definitions/312.html

MITRE Corporation. "CWE-798: Use of Hard-coded Credentials." Common Weakness Enumeration, https://cwe.mitre.org/data/definitions/798.html