Compliance Brief

Complying with Security Management Guidelines for Cloud Computing Services Handling National Core Technologies in Korea

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

As digital transformation accelerates, public institutions that possess and manage national core technologies (hereinafter referred to as "national core technology") are increasingly adopting cloud computing services to improve operational efficiency. The Ministry of Industry and the National Intelligence Service in Korea formed the National Core Technology Cloud Council in 2023 to review conditions for using cloud computing services with various experts, they also gathered opinions and discussed with national core technology-holding institutions and cloud computing service providers. The Security Management Guidelines for Cloud Computing Services Handling National Core Technologies were prepared in April 2025.

What are the Security Management Guidelines for Cloud Computing Services Handling National Core Technologies in Korea?

The Security Management Guidelines for Cloud Computing Services Handling National Core Technologies in Korea establishes security standards for cloud computing services handling South Korea's National Core technologies by:

- Defining security controls for storing/processing sensitive industrial data in the cloud.
- Preventing technology leaks via cloud environments.
- Ensuring secure cloud adoption by organizations and research institutions.

The Security Management Guidelines consist of 3 chapters:

- **Chapter 1:** General overview of the Security Management Guide for the use of Cloud Computing Services for National Core Technologies
- **Chapter 2:** The **security management items** that national core technology organizations and cloud computing service providers must comply with when **storing and processing information** related to national core technology in the cloud computing service environment
- **Chapter 3:** The **security management items** that national core technology holding organizations and cloud computing service providers must comply with **when granting access, viewing and using information** related to national core technology stored in the cloud computing services to foreign companies.

Requirements:

- When a national core technologies institution wants to use cloud computing services, it must comply with the Industrial Technology Protection Act, the Industrial Technology Protection Guidelines and the Industrial Technology Protection Guidelines.
- If the contents of this guideline and relevant laws and regulations are inconsistent, the provisions of the Industrial Technology Protection Act, the Industrial Technology Protection Guidelines, and the Industrial Technology Protection Guidelines shall take precedence over this guidelines.
- National core technologies institutions and cloud computing service providers must comply with the Industrial Technology Protection Act, the Industrial Technology Protection Guidelines, this guide, and other relevant laws and regulations pertaining to cloud computing services.

Who needs to comply?

1. Organizations Handling National Core Technologies

- **Industries Covered:**
  - Semiconductors & displays
  - Secondary batteries (e.g., EV batteries)
  - Advanced materials, biotechnology, aerospace
  - AI, quantum tech, and other National Strategic Technologies (under the Industrial Technology Protection Act).

2. Cloud Service Providers (CSPs)

1) Domestic CSPs: Naver Cloud, KT Cloud, NHN Cloud, etc.

2) Foreign CSPs: AWS, Microsoft Azure, Google Cloud (if used by Korean firms for sensitive data).

3. Research Institutions & Universities: Entities involved **in government-funded R&D** (e.g., KAIST, ETRI) using cloud infrastructure.

4. Government Agencies & Contractors: Public-sector bodies storing industrial/defense-related data in the cloud.

How Thales can help:

Thales' solutions can help National Core Technologies institutions and CSPs address the Security Management Guidelines for Cloud Computing Services by simplifying and automating security, reducing the burden on security and compliance teams.

- **Data-centric**
  - Data-centric security protects the data, which is the most valuable asset of the institutions, regardless of the applications using the data, the environments where the data resides, or the networks the data crosses.
- **High assurance**
  - **Encryption and key management** systems employed deliver the highest levels of availability and performance, as well as certified, proven security. Key Management such as

Hold Your Own Key (HYOK) offers a stronger separation of duty for the encryption keys, and organizations can maintain control of their keys instead of entrusting them to the CSP. With HYOK, organizations can achieve explicit and unambiguous delineation/ demarcation of responsibilities for all activities of the cloud services with CSP.

- Adopting a **quantum-safe solution** using HSM and HSE to prevent data from being "Harvest Now and Decrypt Later" allows institutions to safeguard sensitive information, ensure compliance, and maintain trust in a post-quantum world.
- **Access management** needs to enforce access controls at every access point, allowing only verified administrators to access privileged accounts while enforcing less stringent access controls for less sensitive applications and regular users.

Guidelines	How Thales Helps	Solution Areas
Chapter 2		
1. Basic Principles		
USER When taking measures to dispose of information related to national core technology due to termination or transfer of cloud computing services, request the provider to **dispose of all related information**, and confirm that the disposed information has been deleted so that it cannot be recovered through the cooperation of the provider.	• Remove keys from CipherTrust Manager can ensure secure deletion, digitally shredding all instances of the data.	**Data Security** Cloud Key Manager Transparent Encryption
PUBLIC The user shall **encrypt and manage the data** by utilizing the **unique key** that is stored and managed in a **separate safe place** separated from the cloud computing service, and further encrypt (double encrypt) the data by utilizing the unique key of the provider to store the data. The Provider shall provide the necessary environment so that the User can perform additional encryption (double encryption) on the encrypted data by utilizing the key held separately by the User.	• Encrypt data at rest on-premises, across clouds, and in big data or container environments. • Protect cryptographic keys in a FIPS 140-2 Level 3 environment on-premises. • Centralize key management across hybrid, single- and multi-cloud environments, including key discovery, management of native cloud keys and automated key rotation. • Manage encryption key requests from cloud providers and support many emerging Hold Your Own Key (HYOK) offerings, for example, Microsoft DKE, Google EKM, AWS XKS and more. • Protect your time as well as your data with a single pane of glass view across regions for cloud native, BYOK and HYOK keys and one straightforward UI to manage all cloud Key Management Services.	**Data Security** Cloud Key Manager Hardware Security Modules Transparent Encryption

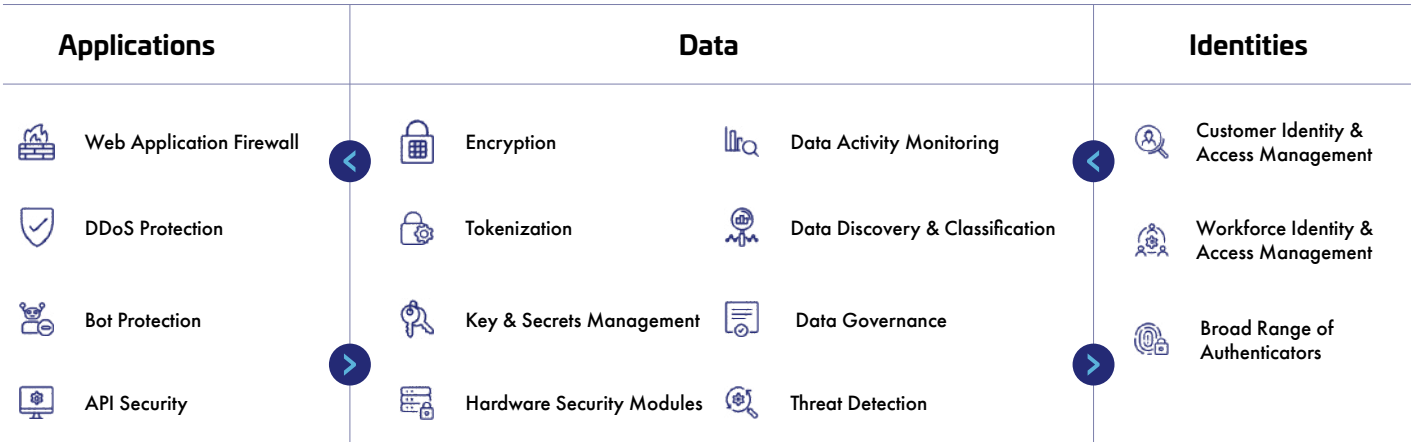
Guidelines	How Thales Helps	Solution Areas
2. Administrative Security		
2) Policy		
PUBLIC The user shall check the r**esults of security vulnerability improvement** on the overall operation management of cloud computing services performed by the provider or a sub-specialized organization, and The **provider** shall regularly **perform security vulnerability checks** on the overall operation management and provide the results of the checks and improvements to the user.	• Run assessment tests on data stores to scan for known vulnerabilities.	**Data Security** Data Activity Monitoring
4) Assets		
PROVIDER Establish **asset classification standards for information assets** (information, information systems, information protection systems, etc.) used in cloud computing services, and create and manage a list of identified assets. Designate a responsible person and manager for each identified asset to clarify the source of responsibility. Assign **a security classification to assets** in consideration of confidentiality, integrity, availability, and legal requirements, and manage them according to the handling procedures for each security class.	• Discover and classify all of your data stores and categorize it based on sensitivity and value. • Classify file content to understand what it means to the organizations from a security or privacy perspective.	**Data Security** Data Discovery & Classification
PROVIDER Continuously **monitor changes to assets** (facilities, equipment, software, etc.) used in cloud computing services to detect unauthorized changes, and maintain the latest change history. In accordance with the risk management method and plan, **risk identification and evaluation** of all areas of security shall be performed regularly, and acceptable risk levels shall be set and managed according to the results.	• Limit access to systems and data based on roles and context with policies. • Provide a comprehensive view of data usage and identify risky behavior. • Monitor and analyze database activity to identify potential threats and vulnerabilities.	**Identity & Access Management** Workforce Access Management **Data Security** Data Activity Monitoring Data Risk Analytics Transparent Encryption
3. Physical Security		
1) Protected Area		
PROVIDER Physical protected areas must be equipped with **access control facilities** to ensure that only authorized persons can access them, and access and access history must be reviewed regularly.	• Leverage smart cards for implementing physical access to sensitive facilities of critical infrastructure.	**Identity & Access Management** Workforce Access Management PKI and FIDO Authenticators

Guidelines	How Thales Helps	Solution Areas
4. Technical Security		
1) Data		
PUBLIC The **provider** shall provide the user with **protection functions for information processing**, such as access control to national critical technology-related information and forgery and tampering prevention, and the user shall confirm this. In consultation with the provider, the **user** shall prepare and implement policies on **encryption objects, encryption strength (complexity), key management, and password use** to protect national critical technology-related information stored or transmitted in the cloud computing service. In consultation with the provider, the **user** shall establish **encryption key management procedures** that include the generation, use, storage, distribution, and destruction of encryption keys, and the user's encryption keys shall be stored and backed up on a separate physically separated server that can be controlled by the user, and the user shall be granted minimal access rights.	• Encrypt data-at-rest on-premises, across clouds, and in big data or container environments. • Pseudonymize sensitive information in databases. • Protect cryptographic keys in a FIPS 140-2 Level 3 environment on-premises. • Streamline key management in cloud and on-premises environments with key lifecycle management. • Store encrypted data and its encryption key in different places for the separation of duties principle • Adopt Post-Quantum Agility to deal with the threats from quantum computing. • Limit the access of internal and external users to systems and data based on roles and context with policies. • Apply contextual security measures based on risk scoring. • Prevent password fatigue with Smart Single Sign-On with conditional access.	**Data Security** Cloud Key Management Hardware Security Modules Tokenization Transparent Encryption **Identity & Access Management** Workforce Access Management Adaptive access
USERS **Classify and manage information** according to the type of information, legal requirements, sensitivity, and importance of information related to national critical technologies. The ownership of information related to national critical technology should be clearly specified at the contract stage with the provider. Security requirements for the **encryption level** of national critical technology-related information should be derived and reflected in the contract, and technical measures for storing, processing, and receiving generated national critical technology-related information should be provided to the provider.	• Discover and classify all of your data stores and categorize it based on sensitivity and value. • Classify file content to understand what it means to the organizations from a security or privacy perspective.	**Data Security** Data Discovery & Classification

Guidelines	How Thales Helps	Solution Areas
2) Authentication and authorization		
PUBLIC The **user** shall apply a **separate individual authentication and access contro**l method separate from the cloud computing service and manage it safely, including regular access records and minimum authorization management review; the provider shall provide all necessary environments. **Users** shall use certificate **(PKI)-based, multi-factor authentication** such as OTP, fingerprint, etc. for cloud computing services and providers shall make arrangements to provide such authentication. Define the object of **access records, record them** in a form that ensures service control, management, and traceability of responsibility for incidents, and maintain them (for at least one year).	• Enable multi-factor authentication (MFA) with the broadest range of hardware and software methods. • Build and deploy adaptive authentication policies based on the sensitivity of the data/ application. • Protect against phishing and man-in-the-middle attacks. • Centralize access policies and enforcement to multiple hybrid environments in a single pane of glass. • Produce audit trail and reports of all access events to all systems, and stream logs to external SIEM systems.	**Identity & Access Management** Multi-Factor Authentication Risk-Based Authentication PKI and FIDO Authenticators
USERS Access to cloud computing services shall be controlled by **secure user authentication procedures**, including user authentication, authorization by access entity, limiting the number of logins, and warning of illegal login attempts.		
3) Network		
PROVIDER **Encrypted communication channels** must be used for the sections where information related to national core technology moves in the cloud computing service.	• Protect data in motion with high-speed encryption.	**Data Security** High Speed Encryption
PROVIDER **Monitor and control the network** to prevent service interruption due to external attacks (DDoS, hacking, unauthorized access, etc.) and leakage of information related to national core technology. In addition, if abnormal signs are found, the user shall be notified immediately and take action. Operate an information security system (firewall, IPS, IDS, VPN, etc.) to protect internal and external networks related to cloud computing services The Company shall use **encrypted communication channels** such as for the sections where important information moves in the cloud system.	• Detect and prevent cyber threats with web application firewall, ensuring seamless operations and peace of mind. • Safeguard critical network assets from DDoS attacks and Bad Bots while continuing to allow legitimate traffic. • Secure data-in-transit with future-proof encryption technologies to avoid "Harvest now, decrypt later".	**Application Security** Bot Protection DDoS Protection Web Application Firewall **Data Security** High Speed Encryption
5) Virtualization		
PROVIDER Regularly analyze **security vulnerabilities of interfaces and APIs** for accessing virtual environments (virtual PCs, virtual servers, virtual software, etc.), and prepare and implement protection measures for them.	• Protect apps from runtime exploitation, while integrating with tools in the CI/CD pipeline. • Detect and prevent cyber threats with web application firewall.	**Application Security** API Protection Web Application Firewall

Guidelines	How Thales Helps	Solution Areas
6) System Development and Introduction Security		
PROVIDER Implement cloud systems according to **secure coding methods**, and perform tests to confirm that the security requirements derived from the analysis and design process have been applied to the information system In order to prevent **operational data leakage during the system test process**, procedures regarding the creation, use and management, destruction, and technical protection measures of test data shall be established and implemented.	• Protect apps from runtime exploitation, while integrating with tools in the CI/CD pipeline. • Detect and prevent cyber threats with web application firewall. • Safeguard critical network assets from DDoS attacks and Bad Bots while continuing to allow legitimate traffic. • Deploy data protection controls in hybrid and multi-cloud applications to protect DevSecOps. • Protect and automate access to secrets across DevOps tools. • Easily access data security solutions through online marketplaces. • Encrypt sensitive data once it is created and make sure cleartext data will not be processed or stored by unauthorized applications and personnel.	**Application Security** API Protection Bot Protection DDoS Protection Web Application Firewall **Data Security** Community Edition DPOD Marketplace Tokenization Secrets Management
Chapter 3		
Security Management: Resources - Data		
USER It shall be restricted from directly storing information related to national core technology on the device accessed by foreign companies and other persons authorized to access it. If information related to national core technology must be stored directly on the accessed device, it must be stored in an **encrypted form using a unique key** that is stored and managed in a separate safe place that can be controlled by a user separated from the cloud computing service.	• Encrypt data-at-rest on-premises, across clouds, and in big data or container environments. • Streamline key management in cloud and on-premises environments. • Protect cryptographic keys in a FIPS 140-2 Level 3 environment.	**Data Security** Cloud Key Manager Hardware Security Modules Transparent Encryption
PUBLIC The user shall use **enhanced authentication methods** through multi-factor authentication for access authorized by foreign companies, etc. The provider shall provide the necessary environment for this.	• Enable Multi-factor Authentication (MFA) with the broadest range of hardware and software methods and form factors. • Build and deploy adaptive authentication policies based on the sensitivity of the data/ application. • Apply contextual security measures based on risk scoring. • Prevent password fatigue with Smart Single Sign-On with conditional access.	**Identity & Access Management** Multi-Factor Authentication Risk-based authentication PKI and FIDO Authenticators
Security Management: Network		
Users During the period of allowing access rights to foreign companies, etc., real-time monitoring of abnormal behavior such as accounts, access, logs (granting, viewing, use, etc.) shall be performed, and if abnormal signs are found, measures shall be taken.	• Monitor API activity, track usage, detect anomalies, and identify potential unauthorized access attempts. • Alert or block database attacks and abnormal access requests in real time. • Monitor file activity overtime to set up alerts on activity that can put financial institutions at risk. • Continuously monitor processes for abnormal I/O activity and alerts or blocks malicious activity.	**Application Security** API Security **Data Security** Data Activity Monitoring Transparent Encryption Ransomware Protection

Thales provides comprehensive cybersecurity solutions in three key areas of cybersecurity: Application Security, Data Security, and Identity & Access Management.



Application Security: Protect applications and APIs at scale in the cloud, on-premises, or in a hybrid model. Our market leading product suite includes Web Application Firewall (WAF) protection against Distributed Denial of Service (DDoS) and malicious BOT attacks, security for APIs and a secure Content Delivery Network (CDN).

Data Security: Discover and classify sensitive data across hybrid IT and automatically protect it anywhere, whether at rest, in motion, or in use, using encryption, tokenization, and key management. Thales solutions also identify, evaluate, and prioritize potential risks for accurate risk assessment. They also identify anomalous behaviour and monitor activity to identify potential threats and verify compliance, allowing organizations to prioritize where to allocate their efforts.

Identity & Access Management: Provide seamless, secure, and trusted access to applications and digital services for customers, employees, and partners. Our solutions limit the access of internal and external users based on their roles and context with granular access policies and multi-factor authentication that help ensure that the right user is granted access to the right resource at the right time.

Organizations can leverage Thales' suite of identity, application and data security solutions available on a single unified platform to become compliant today and stay compliant in the future. Contact us now!

About Thales

Thales is a global leader in data security, trusted by governments and the most recognized companies around the world to help them protect their most sensitive data. The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.