Baidu Security Management Measures

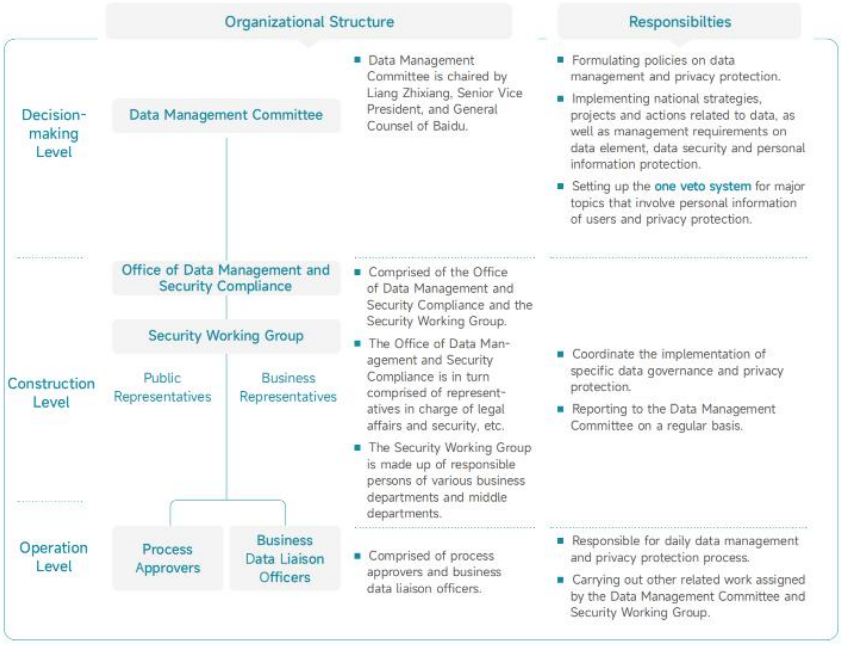
I. Baidu Security Management Principles

Baidu has established a comprehensive security management system around the three dimensions of Security, Safety, and Privacy, creating advanced all-around security technologies and solutions.

Mission	To make Baidu trustworthy and give users peace of mind with leadingsecurity technology.
Vision	The leader in the security field in the Al era.
Values	Adhere to technological belief and security bottom line, pragmatic, self-driven, global awareness, fully responsible.
Security Goals	Ensure data is effectively protected and legally utilized, while also havingthe capability to maintain a continuous state of security.
Overall policy ondata security	Legal and rational use,proactive prevention;comprehensive and deepperception, constant optimization and improvement; rapid handling of riskand data security protection.

II. Baidu Security Management System

Baidu has established a three-tier management structure with the Data Management Committee as the companys top-level data management decision-making body. Security indicators are incorporatedthe performance evaluations of senior executives and relevant staff, promoting the efficient implementation of data security management work.

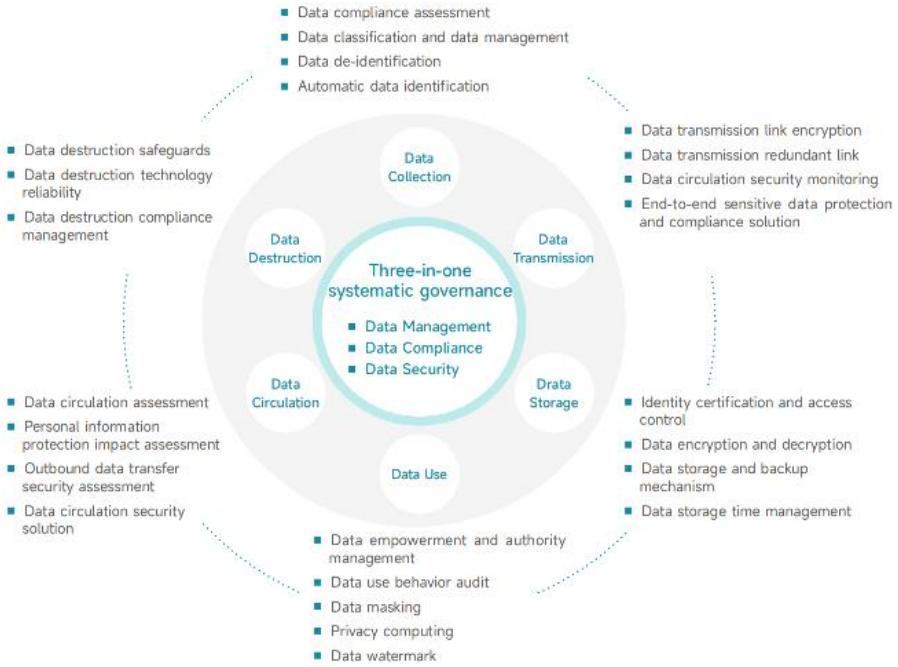


(P1: Security management organization and responsibilities)

III. Baidu Data Security Management Measures

1. Data full life cycle security management mechanism

In the context of the rapid development of large models, Baidu practices a data security management mechanism of "proactive identification in advance, flexible control during the event, and comprehensive tracking after the fact." We have formulated a data governance internal system led by the "Baidu Data Management Measures," established a data management platform, and strengthened data security governance through methods such as whole lifecycle management, Personal Information Protection Impact Assessment (PIA), data circulation evaluation and approval, strict protection of key information and sensitive data, hierarchical classification management, de-identified transmission, encrypted storage, personal information inventory, and security incident management. Baidu also regularly carries out updates and optimizations of management systems and processes to meet the developmental needs of generative artificial intelligence technology and achieve a win-win situation for all parties involved.



(P2:Data full life cycle security management mechanism)

2. Data Export Management Measures of Baidu

In regard to data export, Baidu strictly adheres to the "Cybersecurity Law of the Peoples Republic of China," the "Data Security Law of the Peoples Republic of China," the "Personal Information Protection Law of the Peoples Republic of China," the "Data Export Security Assessment Measures," and other laws and regulations. From the aspects of systems and technology, it maintains national security and public safety, protects the rights and interests of personal information subjects, and ensures the data security and legal rights of Baidu.

System	Coordinated by the Data Management Committee,in collaboration with relevant departments to form special working groups, strict implementation of the related normative requirements for data export, formulation of dataexport self-inspection and evaluation plans, supervision, and regular checkson the data export situation;
Regulation	Establishment of the "Baidu Group Data Export Security ManagementSystem," clarifying and standardizing Baidu's data export activities;
Technology	Regular conduct of data security risk assessments;
	Leveraging its many years of accumulation and advantages in the field ofcombined with theindustry-leading datasecurity technology,exportcompliance detectiontechnology,to formarisk cosed-loop control,solidifying data export risk governance effectiveness.

IV. Baidu Information Security and Privacy Protection Related Certifications

Baidu actively carries out certification work related to information security and privacy protection. In 2024, Baidu obtained and retained a total of 26 certifications related to privacy protection and information security. These certifications cover all of Baidu's business groups, including AI Cloud, Mobile Ecosystem, Intelligent Driving, Technology Platform and Xiaodu.

International Safety Certifications	· ISO/IEC 42001 Artificial Intelligence Management Systems · ISO/IEC 27001 Information Security Management Systems · ISO/IEC 27017 Information Security Management System for Cloud Services · ISO/IEC 27018 Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors · ISO/IEC 27701 Privacy Information Management System · ISO/IEC 27032 Cyberspace Security Management System · ISO/IEC 27040 Information Security Storage Management System · ISO/IEC 29151 Code of Practice for Personally Identifiable Information (PII) Protection · BS 10012 Personal Information Management System · ISO 22301 Business Continuity Management System · CSA-STAR Cloud Security Certification System, certified for some of ACG's IaaS, PaaS and SaaS products · PCIDSS Payment Card Industry Data Security Standard, certified for ACG (Financial Cloud) · AICPA SOC 1, SOC 2, and SOC 3 Reports (including Privacy Principles), certified for some of ACG's IaaS, PaaS and SaaS products
	· Baidu Netdisk: PIP (Personal Information Protection) Certification, the first PIP-certified cloud storage service for individuals · ACG Cloud Advisor: Data Security Maturity Level IV Certification (first in

Chinese Safety Certifications	China) · DCMM Level IV Certification · TPG (Baidu Data Management Platform): Data Security Management Certification (first in China) · Cloud-related products: "Trusted Cloud" Security Assessment · CCRC Information Security License · Baidu ABC Stack: Approval under national regulations for commercial cryptography applications

V. Baidu Security Management Services

Baidu Security builds a security ecosystem centered on AI, exporting capabilities and solutions to the entire industry.

1. Baidu Security Products

Leveraging its experience in security practices within the domain of large models, Baidu employs technologies such as blockchain, trusted computing, big data, and artificial intelligence to develop data security and privacy protection products covering the entire lifecycle of key aspects such as large model training, deployment, and business operations. These products empower industries including finance, government, automotive, education, and the internet.

Security Matrices	AI Security Mobile Security Cloud Security Data Security Business Security

2. Large Model Data Security Protection Products

Dianshi Federated Learning Platform	Based on Model Predictive Control (MPC) Federated Learning (FL), Differential Privacy(DP), and other technologies, it strictly confinesdata regions to protect privacy throughout theentire process.
Dianshi Confidential Computing Platform	Based on hardware to build a virtual secure area, it maintains close to full hardware performance while using encrypted computations, compatible with machine learning and deep learning algorithms for joint computation.
Dianshi Data Security Sandbox	Based on permission access control. data de-identification, sampling, and other technologies, it utilizes multiple isolation techniques to construct a data

	security zone, separating the real data environment from themodel base debugging environment, enablingdata owners to unilaterally open data to data processots.

VI. Baidu Security Audit

Baidu actively conducts internal and external security audits to ensure the effectiveness and reliability of the security management system: internally, Baidus internal audit department regularly carries out assessments and audits on the risks of personal information data and highly sensitive data; externally, Baidu invites third-party institutions with professional qualifications annually to audit and evaluate the companys data security policies, systems, processes, and governance.