Baidu Special Report on Data Security, Privacy Protection, and Content Management 2020

Table of Contents

Introduction

When the tide of digitalization is sweeping the globe, the digital economy has become a crucial force in promoting global development and social transformation. While the information technology brings intelligence and convenience, it also raises concerns about data security and privacy protection from all walks of life. How to use big data in a reasonable, lawful, orderly, and effective manner while protecting personal privacy has become a key issue for promoting stable and sustainable growth of the Internet industry.

Baidu always puts the interests of users first, adheres to the laws and regulations related to privacy and data security. Baidu has established a three-in-one comprehensive protection mechanism and strengthened content management and cybersecurity protection through institutionalized data protection strategies, standardized data processing flow, and intelligent data security technologies. We strive to provide users with an environment where “information is protected, choices are respected, and services are valuable” so that users can rest assured to enjoy the convenience and fulfillment delivered by Baidu.

Data privacy protection requires strong security technology capabilities as support. Through artificial intelligence and other technologies, Baidu strengthens the technical core of personal information protection in all aspects through prevention, protection, and post-tracing measures. The innovative “privacy computing” technology can break the information isolated island and allow deep learning and computing under the premise of privacy protection, realizing “data available but not visible” with the maximum value of data unleashed. Baidu promotes the productization of AI security, empowers ecological partners and helps them improve data security protection and compliance.

The rapidly expanding and more extensively connected data as well as the increasingly rich application scenarios set higher requirements for Baidu’s content management. We continue to improve our comprehensive management system, supervise and control the entire life cycle of content production, distribution, and assessment through open-source technologies and win-win cooperation. With these efforts, we provide users with safe, high-quality, and reliable products and services and create a clean and healthy network environment that is also harmonious and efficient.

While AI technology continues to improve data security, it also brings new challenges in social governance, ethics, and privacy protection. Baidu upholds the highest AI principle is to be “safe and controllable”. The value of AI is to teach people to learn and grow. Baidu will prevent the abuse of AI and enable technological innovation to better benefit mankind with more freedom and possibilities.

> "
> In the era of digital economy, personal information protection is not only closely related to the vital interests of individuals, but also the public interest of whole society. Baidu highly values personal information protection, regards protection of users' rights and interests as the core competency of its development, and strictly adheres to values of data privacy protection, namely Consent, Clarity, and Control.
>
> Technology is Baidu's faith. We use technology to change the world and solve the difficulties and problems in this course. In the age of AI, Baidu is continuously developing technological innovation products and tools for privacy risk detection, prevention, and protection, striving to secure privacy with technology.
>
> "
>
> ——Remarks by Victor Zhixiang Liang,
> Senior Vice President of Baidu

In the digital age, everyone at Baidu will have a deeper understanding of the importance of privacy protection and data security for users. We will embrace innovation with an open mind, conduct exchanges with a win-win attitude, and live up to the trust of every user to safeguard data security.

This report is prepared by the ESG working group and issued with approval of the ESG Committee. It aims to provide stakeholders with the disclosure of Baidu’s performance on data security, privacy protection, and content management from January 1, 2020 to December 31, 2020, as well as our reflections and responses to challenges and opportunities brought by the AI era. This is the first special report on data security, privacy protection, and content management released by Baidu. It is also one of multiple special reports under the *Baidu 2020 Environment, Society and Governance (ESG) Report*. We may release more reports of this nature in the future.

Chronicle of Events

In December 2010

Baidu launched the “Brightness Action” themed with “combating harmful Internet information to build a harmonious Internet environment”.

In March 2012

Baidu released the *Data Security Strategies* when data security was included in the building of Baidu Security management systems for the first time.

In May 2013

Baidu published the *Netizen Right Protection Plan* and became the first search engine company that announced to offer protection in advance for netizens.

In November 2015

Baidu established the Security Committee to strengthen the top-level design of Baidu's data security and deliver security responsibilities.

In September 2016

Baidu Security released *Baidu Security White Paper on Crackdown on the Internet Underground Industry,* which was the first one in the internet industry.

In May 2018

Baidu Chairman and CEO Robin Li proposed the four principles of AI ethics.

Baidu officially established the Data and Privacy Protection Committee, which is responsible for data compliance management and formulation of strategies and decisions on major issues concerning data privacy.

In October 2019

Baidu's self-driving information security protection platform was certified as an EAL level 4 security product, the highest level of security certification in the field of self-driving software security protection.

In June 2020

Two big data security products, Baidu Federated Computing Platform and MesaTEE Universal Secure Computing Platform were both awarded the “10th Batch of Big Data Product Competency Assessment Certificate” by the China Academy of Information and Communications Technology (CAICT).

In July 2020

Baidu, as one of the first key Internet enterprises and basic telecommunications enterprises, signed the *Telecom and Internet Industry Network Data Security Self-Regulation Convention*, making a solemn security commitment to users, the industry, and society.

Baidu AI Cloud once again upgraded its personal information data protection capabilities, completing the new ISO/IEC 27701: 2019 security standard certification upgrade when obtaining the international certification of protection of personally identifiable information in public clouds (ISO 27018), becoming the first cloud service provider receiving this certification in China.

In September 2020

Baidu Maps gained the first batch of Mobile Internet Application (App) Security Certification issued by the China Cybersecurity Review Technology and Certification Centre.

In November 2020

Baidu received the first batch of level 4 Quantitative Management certificate of the Data Management Capability Maturity (DCMM - National Standard), standing out as a national benchmark in data management capability.

Baidu was listed in the second collection of 2020 Excellent Examples for Network and Data Security Compliance Assessment, establishing the best practice and promoting it in the industry.

In December 2020

The Security and Privacy Compliance Platform of Baidu, the only Chinese nominee of its sort, won the second prize of the “2020 Excellent Examples for National Cybersecurity Standards”.

User Rights

Baidu fully respects and protects the legitimate rights and interests of users.

Protecting Users' Information and Respecting Users' Choices

Only after obtaining the users' consent will Baidu use their personal information reasonably and transparently while giving them full control. This convinces users that their information is protected, and their choices are respected. Users can visit Baidu's privacy protection platform at http://privacy.baidu.com or access the relevant product and service pages to read *Privacy Policy* to comprehensively understand Baidu's privacy protection values and principles.

Right to Know

- Users have the right to know and can be informed of the purposes for which Baidu collects personal information.
- Users can read Baidu's privacy policies on their website pages and read the important terms and conditions under the bolded font prompt to better understand how Baidu collects and uses data.

Right to Choose

- Users have the right to choose whether or not to provide personal information. Baidu's platforms will only collect information with user authorization and will never collect it forcefully. When the purpose of processing personal information is about to change, Baidu will prompt the user to authorize again through reasonable means in advance.

Right to Control

- Users have the right to modify and delete their personal information. Users may turn the authorization buttons on or off to grant or withdraw their consent at any time. The authorization control is usually designed to appear on the product pages and is easy to operate. At the valid request of the user or upon expiry of the retention period of the information, Baidu will delete the user's personal information or stop processing the personal information in accordance with the law.
- While using our products, users may edit their basic information, change passwords, add security information or add associate accounts through the one-stop account management platform at https://passport.baidu.com/. If users have any other questions about personal information protection, they may contact us through the special united platform for feedback at http://help.baidu.com/personalinformation, or portals of our product websites.

Responding to Users' Demands Timely with Convenient Accesses

Users can report any problems encountered when using the Baidu platforms at any time with the fastest response time of 20 seconds. Baidu continuously upgrades and perfects related products according to users' core demands when constantly improving the user experience.

In 2020

200
product lines accessed to the Baidu user feedback portal

Covering
1,231 products

Over
8,000 million
cases of user feedback handled

100%
user feedback processing rate

92%
user satisfaction rate for feedback processing

Diversified Feedback Channels

- When using the Baidu App, users can click on the "x" to realize "Reporting and Feedback", at the bottom right of the news or advertisements if they encounter low-quality information containing clickbait headlines, misspelled words, or false advertisements. Or they can give feedback and follow up on the status of handling through the "Help and Feedback" page in the personal center. Users can also report directly through the Baidu User Service Centre at http://help.baidu.com for one-stop reporting or contact Baidu's human customer service through the 400-921-3900 hotline for immediate response and assistance.

Figure: Users Reporting Problematic Content on the "Reporting and Feedback"

Figure: Users Can Ask Questions by Clicking "Ask Questions" or Leaving a Message by Clicking "Feedback and Advice"

Continual Optimization of Feedback Experience

- With a one-stop standard feedback handling process in Baidu, most users' problems can achieve deep analysis from multiple perspectives, multi-person synchronous handling, thus ensuring timely response to users' concerns.
- In 2020, Baidu further improved the user experience with the feedback approaches shifting from the traditional form of leaving a message to the online human customer service response. The feature was first applied in Baidu Netdisk after its launch, and some users can get real-time feedback through instant interaction with human customer service.

Assuring Users Safe Search with Full Advance Payment

Users can refer to the "Official" and "Protection" signs when searching for information or shopping online to quickly identify official websites and those covered by Baidu's protection policies, thus reducing search risks.

Figure:Search Results with a "Protection" Sign

- Users can claim compensation through the Baidu Netizen Rights Protection Plan if they suffer financial losses due to fake official websites or phishing scams after they log in to Baidu accounts and click the search results with signs of "Advertisement" and "Protection". Users will usually receive a response within two working days after submitting the feedback, a handling decision within five working days as well as their compensation payments within 20 working days if it is within the scope of the protection.If customer service is unable to resolve a dispute, Baidu will introduce a third-party organization, the People's Mediation Committee, to assist in online and offline service dispute resolution, so that users' rights and interests are better protected.
- In 2020, the initiative was upgraded and improved again, with coverage expanded and compensation payment increased in some industries.

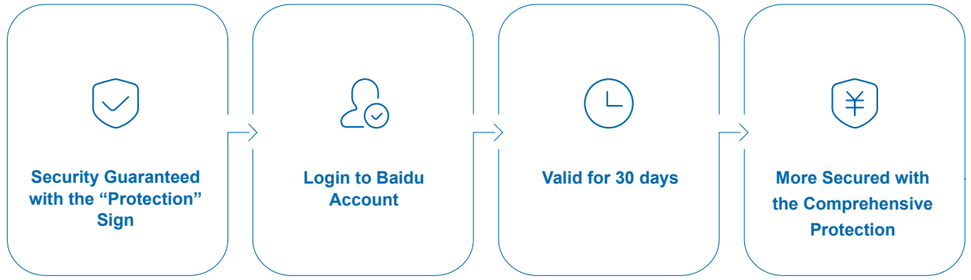


Figure:Netizen Rights Protection Plan

In 2020

users submitted more than **20,000** complaints through the Baidu Netizen Rights Protection Plan

Baidu coordinated with shops to refund users in over **16,110** cases

Refund totaling over CNY **7.21** million

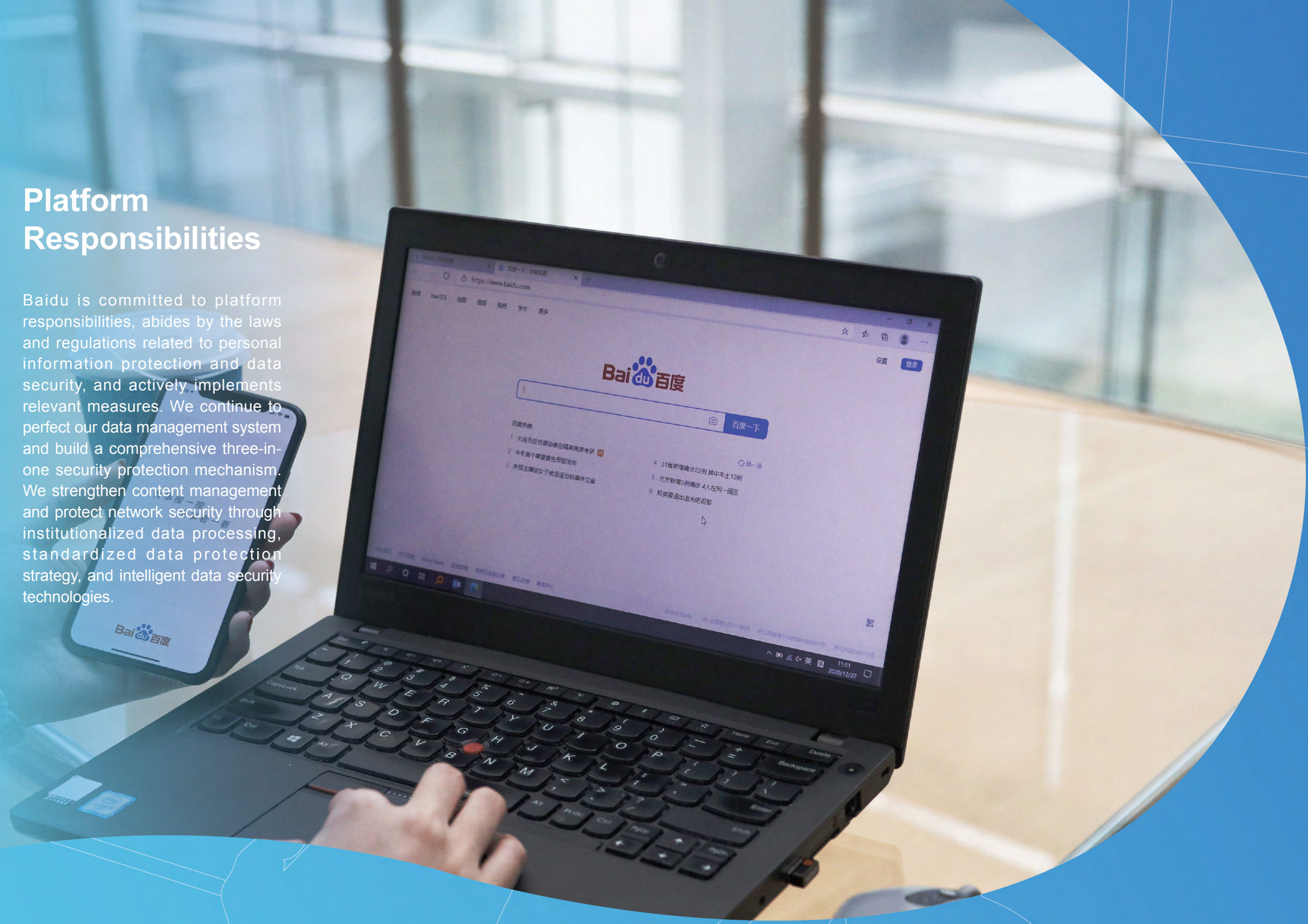
Case

Internet user scammed into buying Disney tickets receives CNY 3,380 in compensation

Ms. Lu found a shop selling ticket for Shanghai Disneyland on Baidu and bought a VIP Fast Pass ticket. However, when she arrived at Disneyland, she found that there was no fast pass service and the ticket was deemed invalid. At that time, she could not contact the seller. After realizing she had been scammed, Ms. Lu made a complaint through the Baidu Netizen Rights Protection Plan, gaining CNY 3,380 for compensation. Meanwhile, Baidu exposed its related information and then removed the fraudulent seller to avoid other users being scammed.

Platform Responsibilities

Baidu is committed to platform responsibilities, abides by the laws and regulations related to personal information protection and data security, and actively implements relevant measures. We continue to perfect our data management system and build a comprehensive three-in-one security protection mechanism. We strengthen content management and protect network security through institutionalized data processing, standardized data protection strategy, and intelligent data security technologies.



The Four Principles of Personal Information Protection

In the process of data collection, storage, processing, usage, and distribution, Baidu takes legality, legitimacy, and necessity as prerequisites. Baidu carries out privacy protection planning and business planning at the same time. Privacy impact assessment and privacy protection measures go hand in hand with personal information processing activities to ensure that the basic principles of continuous privacy protection throughout the data life cycle are met.

Informed Consent

- Baidu Apps will notify users explicitly and clearly of the purpose, method, and scope of personal information collection, and ensure that users fully understand the data processing rules of Baidu's software before giving consent and authority. Meanwhile, we provide users with an in-depth understanding of data processing through user-friendly page designs in certain innovative scenarios. If personal data sharing involved, Baidu will process the data within the authorization scope of users as we protect users' right to know in compliance with laws and regulations.

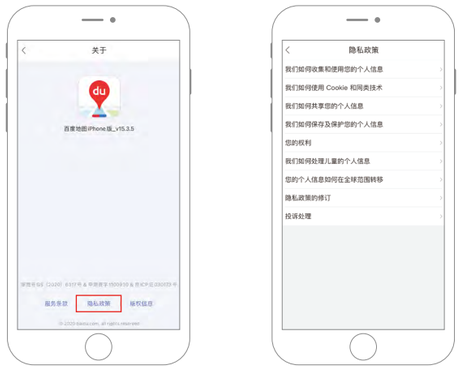


Figure: The Privacy Policy of Baidu Maps

Data Minimization

- Baidu ensures that personal data shall be adequate, relevant, and limited to what is necessary concerning the purposes for which they are processed.

User Experience

- Baidu strives to simplify information management tools and options. We display various controls to users such as information editing, permission and authorization, account association, and account cancellation to optimize users' experience.

Security Assurance

- We have formed a closed-loop internal management process covering the data asset identification, data categorization and classification, data application and authorization, behavior auditing, and reporting. In terms of implementation, process, we strictly observe the *Baidu Data Security Strategy* while focusing on Privacy by Design (PBD) and Privacy Impact Assessment (PIA) to build a consistent assessment mechanism. In terms of technology tools, Baidu uses desensitization, encryption and differential privacy protection, and other technical means to achieve data de-identification and protect private data during data processing. Moreover, in light of the processing of users' sensitive personal information, Baidu has achieved accurate personal identity authentication and access control at all levels including system, storage, and service.

The Multidimensional Comprehensive Protection Strategies

Baidu formulated a series of internal management regulations, covering all employees of Baidu and its branches, to ensure all-round and whole-process data security from aspects of top-level governance structure, security risk control system, and security audit mechanism.

The Committee Mechanism: Ensuring Efficient and Compliant Processes

- Baidu improves the organizational structure of cybersecurity governance consisting of the Security Committee of Baidu, the Data and Privacy Protection Committee, and the Data Assets Management Committee. They exercise their functions and restrict each other, to ensure the transparency and security of data applications and effective control of data security and privacy risks.

Data Security: The Security Committee

As the top-level security organization, the Security Committee of Baidu is responsible for risk control, decision-making, resource investment, and team coordination in information, product, data, and personal information security. It secures the information, products, and data of the company and ensures users' and customers' needs can be met securely. The chairman of the Security Committee of Baidu is Haifeng Wang, Baidu's Chief Technology Officer.

Privacy Protection: The Data and Privacy Protection Committee

Baidu has a top-down management system of privacy protection with the Data and Privacy Protection Committee at the highest level. On the one hand, it is responsible for making strategies and decisions on major data privacy issues. On the other hand, it monitors the compliance management of user data protection and cross-border data, ensuring that our data privacy-related measures comply with international treaties and national laws and policies.

Data Governance: The Data Assets Management Committee

At the level of our company's overall data construction, Baidu established the Data Asset Management Committee. The members of the committee are representatives of the Big Data Department, the Security Department, the Legal Department, and other lines of business such as the searching business line. The Data Assets Management Committee is responsible for the formulation, release, and decision-making of policies, management rules, mechanisms, and processes related to data assets.

Harmonizing Businesses and Functions to Fulfill Security Responsibilities

- Baidu established a three-level security structure, consisting of the Security Committee of Baidu, the Security Working Group, and heads of security departments, to effectively control security risks and improve management efficiency.

Basic defense

As the executive party and the first responsible party of Baidu information and product security, the heads of departments are in charge of security of their departments and are also responsible for implementing the company's information security-related strategies and measures.

Penetration testing and deterrence

As the security risk prevention and monitoring party, the security working group composed of the Security Department and other departments is responsible for coordinating security work at the company level and reporting to the Security Committee of Baidu regularly.

Inspection and internal audit

Based on the status quo of the company's information security management, the Internal Audit Department and Professional Ethics Department carry out audits and inspections for major information security risks. They are responsible for receiving, investigating, and dealing with security issues that involve violation of professional ethics and the company's information security-related policies and procedures.

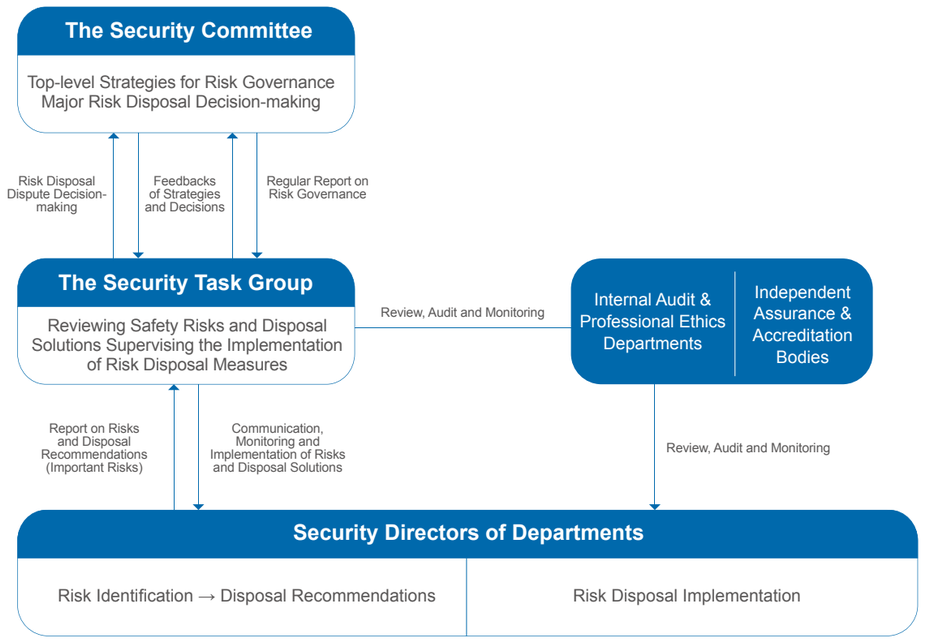


Figure:Organization Structure of Security Assurance

Improving Audit Mechanisms and Promoting Full Security Audit

- Baidu conducts security-related regular audits and third-party authentication and evaluation to achieve the objective assessment and comprehensive oversight of information security and data privacy protection measures.

Regular internal audit

The Internal Audit Department of Baidu carries out special audits on user privacy protection and data security, identifies defects and problems with risk warnings, and performs tracing audits on abnormal access behaviors.

Third-party certification audit

Baidu's core systems have been assessed by the qualified third-party as China's classified protection of information system security Level- 3, and some major systems are even assessed as Level-4. Besides, Baidu's main businesses and products, including Baidu AI Cloud and Baidu Netdisk, have been regularly assessed to privacy and information security-related ISO/IEC certifications.

Engaging Everyone into Creating a Security Culture

- Baidu continuously strengthens the security education for employees and develops multidimensional training mechanisms to enhance the security awareness, literacy, and skills of all employees (including management, employees, and informal staff such as interns and outsourced staff).

Third-Party security assessment

An independent and professional third-party security agency will conduct a double-blind test[1] or a blind test[2] annually under the premise of complying with moral ethics to test the weakness and operational effectiveness of the security defense and response system.

Training activities

Baidu conducts security training in the form of live streaming, online courses, and on-site lectures. Security Month is specially provided to promote safety knowledge through context promotion.

Awareness test

Baidu conducts at least one annual mandatory security and privacy awareness test that requires full marks to pass.

Penetration testing

Baidu regularly conducts network penetration tests to raise security awareness for all employees. The drills simulate external attacks to test employees' defense capabilities, enhancing their security awareness in a targeted manner.

In 2020

over **50,000** views of online security training program

over **100** online courses

32 security awareness training sessions for new employees

2 penetration tests

5,242 assessments of intensive training on the security awareness

1 Double-blind test: the assessment and testing method that does not provide any testing information to the observer or notify the subject of the time, locations, and assessed contents in advance.

2 Blind test: the assessment and testing method that does not notify the subject the time, locations and assessed contents in advance.

Strengthening the Security System with AI as the Core

Baidu has enhanced its technological approaches to improve its capacities for personal information protection and defense. Through AI and other technologies, we build a full life cycle of the Internet content management mechanism.

Building the AI Security Ecosystem from Three Dimensions of Security, Safety, and Privacy

- Baidu deepens its independent research and development, empowers the network security construction with technologies, and considers security issues from three dimensions: Security, Safety, and Privacy. Baidu has developed and deployed a set of multi-level data management and security protection scheme covering the cloud, pipeline, and end.

Security

Resolving misjudgements of AI system caused by attacks from physical and digital world

Examples of Security Technologies

OASES KARMA Hotfix Technologies for Kernel Vulnerabilities

Preventing security vulnerabilities caused by "habitat fragmentation" from being exploited by attackers

MesaLock Linux Memory-safe Operating System

Improving the ecological safety of Linux

HugeGraph Highly Scalable Graph Database

The second relational querying capabilities can be used for fraud detection, correlation analysis, knowledge graph, data governance, and other scenarios

Open RASP of Embedded Cloud Application Execution Engine

Monitoring and protecting the database

Deep Face Forgery Detection

Enhancing the accuracy of AI recognition, stopping telecom fraud and other illegal acts committed by abusing AI-powered face-swapping technology at the source

OTA Safety Technology

Providing intelligent equipment with full process solutions of cloud, pipeline, and end. Any system update, feature iteration, or vulnerability fixes can reach the equipment as soon as possible

Safety

Avoid negative impacts on model classification and prediction that caused by variable environmental factors, such as lighting, space, clarity, noise, and weather

Examples of Safety Technologies

Systematic Assessment Framework for Evaluation of Model Robustness

Creating assessment criteria and quantifying potential security threats according to the changing task scenarios and checking if the system has misjudgments in unforeseen task scenario

AdvBox Adversarial Example Toolbox

Optimizing mainstream machine learning platforms to quickly improve the model robustness

Privacy

Personal information protection covering the full life cycle of data collection, processing, circulation, and calculation

Examples of Privacy Technologies

MesaLink TLS Secure Communication Library

Avoiding privacy leakage caused by memory security vulnerabilities

The Next-generation Secure Trusted Computing Services Framework MesaTEE

Providing chip-scale protection for the integrity and confidentiality of data in the cloud

Baidu Federated Computing Platform

A joint computing platform based on various security technologies, providing security protection for tera-scale data conjoint analysis, joint risk control, and joint marketing.

Differential Privacy

Interfering with the data by adding noise before collecting or publishing data to hide real data and void attackers obtaining data by guessing.

AI Automatic Desensitization

Identifying the distribution of sensitive data assets quickly through intelligent scanning with the integration of advanced Baidu AI capabilities such as image identification and natural language processing; realizing the desensitization of multiple sensitive data through custom desensitization policies to support the protection of sensitive data in complex business scenarios.

Case

Building integrated and intelligent cloud security systems to secure data in the cloud

In cloud security, Baidu has introduced Privacy Enhanced Computing, Trusted Computing, and other AI security technologies, integrating advanced AI security capacities with Baidu AI cloud to enable intelligent, integrated security upgrades for enterprise defense systems on the cloud.

Baidu released AI Cloud Shield, which can provide the Internet Data Center (IDC) with comprehensive and convenient security infrastructure in combination with a series of technical capabilities, including rapid local detection, automated expansion of T-level cloud defense, hacker attack detection, real-time security defense, and threat intelligence. In the second half of 2020, we launched the “Intelligent Data Security Gateway” and the “Intelligent Threat Hunting Platform”, which can provide one-stop cloud-based sensitive information detection, desensitization, auditing, and other security management systems, thus effectively dealing with the penetration testing and other scenarios to better protect the cloud computing security.

Systematic Guarding of Network Security Operations

- With AI technology as its core and based on big data technology, Baidu has been improving its network security awareness, capacities for prevention, protection, and emergency response to create a secure and stable network environment.

Product Security and Quality

Baidu is a practitioner of DevSecOps[3] security concepts and can rovide solutions with full chain security in terms of the full life cycle of Baidu's product development and development tools. Through security collaboration, security front, security automation, and other measures, we can improve the efficiency of R&D and guarantee the security and quality of Baidu products in all aspects of product requirements design, coding, testing and launch.

Security Preplan and Drill

Organize regular security drill to ensure key stuff to effectively deal with security incidents, such as system vulneralbilities, network attacks, and network intrusions.

System Risk Identification

Conduct penetration testing to identify the defects and risks of the existing systems

Monitoring Alarms and Blocking

Monitoring and alerting of basic security and defense-in-depth threat detection capability can timely block anomalies and attacks

Abnormal Behavior Tracing

Detecte and audit core end-to-end data use behaviors as well as tracing abnormal behaviors

Safety Warnings and Labels

Identify securiy status with risk warnings of websites that may be hijacked, maliciously tampered with, have unstable access and other abnormalities to avoid risks to users

The Comprehensive Defense Scheme for Cybersecurity

3 DevOps Standard, also known as *“the DevOps Capability Maturity Model”*, is led by the China Institute of Information and Communications and jointly formulated by domestic or international experts from top enterprises and institutions in this industry. By far, it has officially been established in ITU-T, a standard organization directly under United Nations. DevOps Standard covers various assessments such as agile development management, continuous delivery, technical operation, application architecture, security and risk management, systems and tools. DevSecOps is the integration of security into emerging agile IT and DevOps development as seamlessly and as transparently as possible.

- In day-to-day operations, Baidu constructs and constantly optimizes the comprehensive defense scheme for network security to enhance our adaptability to vulnerabilities. In case of any network security incidents, the sophisticated emergency response mechanism established by Baidu can minimize the negative impacts.

- Baidu has established a set of standardized security incident management processes and contingency plans for security incidents that affect data security and have or may have an impact on personal information, such as initiation, response, reporting, mitigation, resolution, forensic analysis, and notification.

- Depending on the specific nature of the security incident, the response roles involve several specialist departments and teams of experts, adhering to the fundamental principle of "eliminating or mitigating the negative impact of the risk on the organization, the business, and the user or customer in the shortest possible time". Based on its impact, range, and controllability, the cyber incident can be classified into level 1, level 2, and level 3 from high to low. The responding process is set as follows:

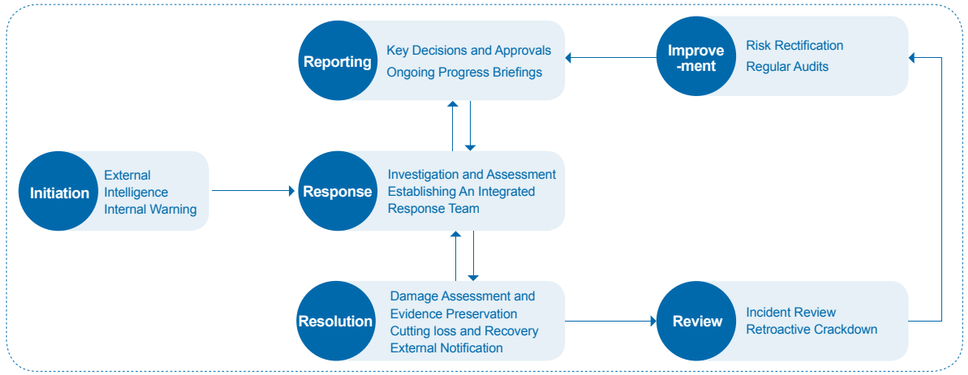


Figure: Security Incident Response Process Flow

- Baidu has established the Baidu Security website (https://anquan.baidu.com), the Baidu Security Forum (https://anquan.baidu.com/forum), and the Baidu Security Response Center (https://bsrc.baidu.com) to meet users' needs of acquiring security information and promote cooperation and exchange between security experts.

Case

BSRC as a bond between the industry and white hat

BSRC (https://bsrc.baidu.com/v2/#/home) is a vulnerability collection and emergency response platform established by Baidu dedicated to maintaining a healthy ecological environment on the Internet, safeguarding information security of products and business lines, and promoting cooperation and communication among security experts .

In recent years, the Baidu Security Response Center (BSRC) has organized Baidu Cybersecurity Skills Competition for College Students, the Annual Festival of Baidu Security Response Center, White Hat Night, Cybersecurity technology exchange in universities, and other exchange activities. The center, together with 41 major security response centers in China, launched the DEF CON CHINA volunteer program, providing a platform for the next generation of cybersecurity talents. Meanwhile, the Baidu Security Response Center also introduced several vulnerability rewards programs and a smart device security crowdsourcing challenge for new scenarios and risks in the AI era, with a maximum prize of CNY 1 million for high-quality vulnerabilities.

Comprehensive Governance of Illegal Information with "AI plus Human Intelligence"

- To ensure the effective disposition of illegal content and build a sound and benevolent online environment, Baidu continues strengthening the content management of product and business advertising and builds a full-life-cycle Internet content management mechanism.

Pre-monitoring, instant interception, and post-tracing processes

Baidu has built a risk control system of "AI inspection plus human double-check plus human patrol", which establishes a closed-loop defense mechanism through various algorithms and training models to improve users' search experience.

Stages	Content Risk Control	Business Advertising
Pre-monitoring	• Set up a security awareness system based on the searching ecosystem to gather information. Perform intelligent modeling and 7X24 monitoring. Filter, reject and remove illegal information involving pornography, gambling, drugs, false and exaggerated information, and privacy intrusion.	• Set up a pre-audit mechanism. Strictly review the entry qualification of advertisers, and improve the reviewing capabilities for the content of advertisements (AI + human intelligence) prohibit risky advertising. • Implement landing page hosting for high-risk industries. Intensify the audit of a landing page to avoid web page tampering.
Instant interception	• Combine technical identification with human patrol to review and manage the content. Identify malicious content and harmful information with resolution through rejection, risk labeling, blocking warnings, and search blocking.	• Conduct technical inspection of online advertisements and landing pages. Remove non-compliant content, review and filter content with multiple auditing approaches.
Post-tracing processes	• Employ Baidu deep learning model and knowledge map to track large-scale, systematic, and cross-border illegal content. • Take punitive measures to deal with illegal accounts, such as warning, refusing to publish, deleting information, restricting functions, suspending updates, etc.	• Carry out compliance verification to avoid any content tampering with advertisements. Remove harmful advertisements and suspend their accounts.

In 2020

Baidu blocked more than **51.62** billion pieces of illegal information involving pornography, gambling, and information endangering social security, among which over **51.54** billion were blocked by machines and over **80** million were deleted through manual patrol.

7.13
million illegal users suspended

24,700
malicious websites and

112,000
URL suspected of stealing citizens' personal information blocked

over
2.298
billion illegal advertisements rejected

9.39
million malicious web pages intercepted

28,031
illegal advertising accounts punished

4.93
million transactions of “ID cards and bank cards” cleared

Case

Key supervision on medical information to safeguard a sound medical environment

Baidu focuses on medical information management, strengthens technical inspections, and builds high-quality online consulting channels for users. Medical information can only be promoted after strict review and the authoritative medical information is shown at the top search results. In 2020, the official web pages of 146,000 public hospitals in total were displayed in Baidu's search channels with priority; Baidu adds risk warnings for 550,000 sensitive words relating to diseases, drugs, and medical institutions.

AI Core Technologies for Personal Privacy Protection

- In terms of privacy protection and data security, Baidu has applied a series of access control and privacy enhancement technologies in the full life cycle of data collection, storage, processing, usage, and distribution. This can unlock data value while protecting users’ privacy.
- Supported by advanced AI technologies and closely subject to national supervision standards, Baidu has built a Security and Privacy Compliance Platform and included the privacy benchmark testing into pre-launch testing processes. The Security and Privacy Compliance Platform, the first compliance risk detection and governance system for the collection and use of personal information by an App that provides services to the public, aims to help App development and operation enterprises benchmarking with national and industry security standards and rules, accurately identifying and detecting privacy compliance risks in privacy policy texts, collection and use of personal information by Apps, protection of Apps users' rights, etc. The platform ensures that the detection capabilities meet regulatory requirements, contributing to self-inspection and rectification to protect users’ privacy security. At present, the majority of Baidu Apps and SDK have accessed to the platform with internal testing completed.

Challenges and Opportunities of AI

In face of risks and challenges in the AI era, deepening understanding of AI ethics and building a safe and win-win ecosystem for the whole industry is the only way to address the coexistence of humans and AI, which is also the guidance and direction for the future development of Baidu.

Three-dimensional AI-oriented Company

In recent years, as AI core technologies have made various breakthroughs, challenges in the AI era follow in terms of social governance, ethics, and privacy protection. It is urgent to continuously conduct research and pre-judgments.

Laws and regulations

- The existing laws and regulations are inapplicable to some extent, so a complete set of AI laws and regulations remain to be established.

Standards

- General standards for data security and AI application sub-fields need to be improved immediately.

Enterprises

- The top-level design and rules for implementation of compliance requirements need to be completed with the integration of ethical awareness and culture into risk management systems.

Technologies

- Risk assessment capabilities need to be improved with immature technologies.

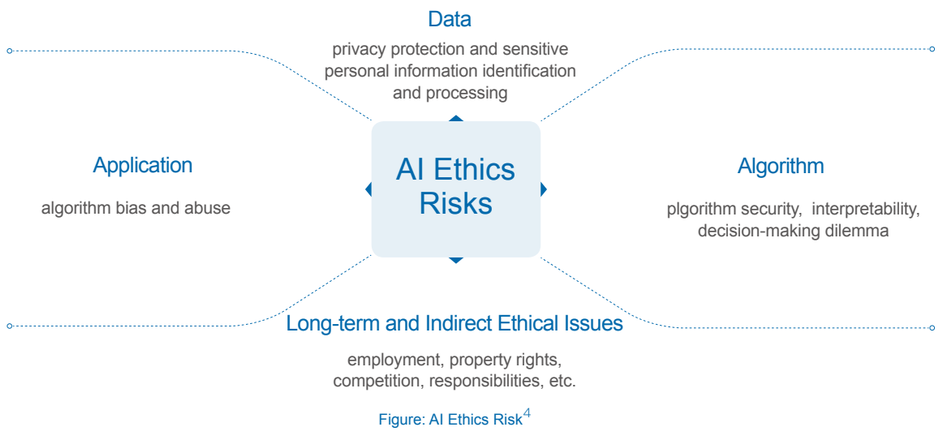


Figure: AI Ethics Risk[4]

- As a developer and user of AI technologies, Baidu is committed to the development of innovative AI technologies and closely follows the negative impacts and social issues that may be brought about by new AI technologies. Developing AI technologies that are trusted, controllable, and ultimately beneficial to humanity is a testimony of how Baidu honors its responsibilities and missions.

- Baidu Chairman and CEO Robin Li proposed the four principles of AI ethics. AI should be “safe and controllable”, which is the highest principle; AI’s innovative vision is to promote more equal access to technologies and abilities for humanity; the value of AI is to empower mankind to learn and grow instead of surpassing and replacing mankind; the ultimate ideal of AI is to bring more freedom and possibilities to humankind. These four principles aim to establish concepts and rules that the whole society follow in terms of all new AI products and technologies, so as to enable the co-existence between AI and humankind. Only by adhering to the highest principle of “safe and controllable”, establishing sound AI ethical norms, and accelerating the implementation of AI ethical principles can we use AI technologies to achieve multi-governance, benefit more groups, and realize sustainable social development.

4 Please see *Report on the Ethics Risks of Artificial Intelligence* of the National Artificial Intelligence Standardization Group.

- In response to the emerging risks posed by AI technologies, Baidu continues to strengthen internal compliance governance, promote social ethical and moral values, and develop targeted technical solutions such as anti-fraud and forgery detection to maximize the benefit and minimize the harm. Furthermore, to prevent the abuse of AI technologies, Baidu carries out a relevant risk assessment and sets risk defense for specific scenarios of AI applications, international cooperation, and technology exports to prevent abusing AI applications. By taking suitable risk defense and control measures, negative consequences can be controlled effectively.

- Regarding AI ethics and standards, we followed proposals related to standardization and joined in the preparation of the *Introduction of AI Ethics Risks* by the National Artificial Intelligence Standardization General Working Group. Baidu also collaborated with CAICT in formulating the *Research Report on Privacy and Security of Facial Recognition Technology in Applications* and participated in the development of Internet of *Vehicles Service —User Personal Information Protection Requirements*. In terms of international exchanges, we have actively joined AI4SDGs[5] research plans and international cooperation networks while funding their research projects, actively promoting the training of talent and the leveraging of technology in the AI area to build global consensus.

Case

Building Apollo autonomous driving system to safeguard Information Security

Information security is an ethical challenge, and also a barrier that must be overcome by self-driving technologies. Focusing on the key technologies of autonomous driving, Baidu has attached great importance to potential security risks. The core goal of Apollo information security defined by Baidu is “defending external intrusion, preventing leakage of core applications and private data, safeguarding vehicles’ control system”.

The Baidu Apollo Automotive Information Security Lab focuses on the analysis of automobile cybersecurity technology and its latest trend, covering more than ten aspects of the automobile cybersecurity area, such as data privacy protection and Signal Spoofing Resistance Test for Autonomous Vehicles. We apply AI technologies in building a full life cycle of a “detection-protection-response-recovery” informational security system for intelligent connected vehicles. Meanwhile, we concentrate on technological protection, data management, and policies and standards while accommodating protection for user’s driving data and personal information, and preventing the vehicle from being attacked or controlled by hackers.

Building an ecological security system for intelligent devices to protect user’s privacy data

In the era of intelligent voice where everything is interconnected, DuerOS has provided voice interactions over 6.2 billion times. Protecting user data has become the main focus for information security.

With the goal of “controllable, safe and reliable”, Baidu builds a multilayer defense-in-depth system covering the cloud, pipeline, and end. We have achieved process control before, during, and after the incident, by applying AI technologies and relying on security schemes such as a trusted execution environment, secure OTA (Over-the-Air Technology), and system hotfix. At the same time, we also accommodate equipment security and data security, and have established a closed-loop protection mechanism of “instant detection, fast blocking, secure updating”.

Baidu also actively participates in the formulation of industry standards for intelligent devices. Based on the smart hotel and interconnected scenarios, we establish the best safety practices to provide comprehensive protection for the ecosystem of intelligent devices and safeguard users’ privacy.

5 AI4SDGs: AI for Sustainable Development Goals.

Building an Open and Inclusive AI Ecosystem

Security challenges in the AI era have become more complicated compared with those in the past. Believing in the philosophy that "Everyone Can AI", Baidu is encouraged to open-source AI-related technology tools. The protection of network information is a shared responsibility of the whole society. With a more open mind, Baidu communicates and cooperates with the netizens, trade associations, scientific establishments, social institutions, and other stakeholders to seek win-win cooperation with openness, inclusiveness, diversity, and mutual learning. Therefore, we can jointly build a line of defense for network security and a sound cyber ecosystem for the AI era, contributing continuous efforts to the prosperity of AI field.

Participating in Industry Alliances and Industrial Standard Formulation

- Baidu actively participates in industry alliances and contributes Chinese wisdom to joinly building a secure ecosystem with industrial partners through multi-party cooperation with rich technical legacy.
- Baidu has joined ISO/IEC JTC1[6], ITU-T[7], IEEE-SA[8], TC28[9], TC260[10], CCSA[11], CCSA-TC601[12] and other domestic and international standard organizations successively. Under the organization of the National Information Security Standardization Technical Committee (TC260), Baidu was involved in developing over 30 national standards, including *Information security technology – Evaluation specification for personal information security in mobile internet applications, Information security technology – Basic specification for collecting personal information in mobile internet applications, Information security technology — General requirements for security of internet information services*, and *Information security technology – Cyberdata process security specification*. These standards cover a wide range of Network security fields, such as AI security, fighting network underground industry, App privacy compliance, data security, and privacy protection.
- As a member of CCSA-TC601, Baidu has been actively participating in developing *Data Asset Management White Paper, Big Data Service Capacity Maturity Model, White Paper on Management Practices in Data Standards*, and many more white papers and standards for the big data area. In November 2017, Baidu, along with Huawei and China Academy of Information and Communications Technology (CAICT), launched the Open AI System Security Alliance (OASES), working with industry partners to promote a secure ecosystem.
- For international standards, Baidu was deeply involved in the preparation of the world's first DevOps standard, which is the *DevOps Capability Maturity Model*, and was awarded as its member.

Promoting Industry–University Collaborations

- Baidu actively promotes collaboration and integration between industries and universities. Cooperating with Fudan University and other higher education institutions, we carry out researches on hot topics related to data security and privacy protection. We have made breakthroughs in various fields, including "analysis of biological information leakage in mobile applications" and "security vulnerability analysis of Baidu and its peripheral products".

6 International Organization for Standardization/International Electrotechnical Commission

7 International Telecommunication Union - Telecommunication Standardization Sector

8 The Institute of Electrical and Electronics Engineers Standards Association

9 China National Information Technology Standardization Technical Committee

10 China National Information Technology Standardization Technical Committee

11 China Communications Standards Association

12 China Communications Standards Association - the Big Data Technology and Standard Committee

- Represented by PaddlePaddle learning platform, Baidu's open-source AI platform serves as a basement for talent cultivation. So far, a comprehensive service system has been constructed, which covers learning, practice, competition, certification, and employment. This helps to train talents in practice and applies cutting-edge technologies in classes. As of December 2020, Baidu has trained more than 1 million AI talents. We plan to train another 5 million AI talents in the next five years, which will provide a workforce guarantee for the development of China's intelligent economy and intelligent society.

Case

Open-source PaddlePaddle empowers communities

PaddlePaddle, based on years' deep learning technology research and business application of Baidu, is the first seld-developed industry-scale deep learning platform in China with full functions and open sources. It integrates core training and inference of deep learning frameworks, basic model libraries, end-to-end development kits and abundant tools. It can continuously lower the threshold for learning so that developers and enterprises can implement their ideas about AI safely and quickly, which provides a solid foundation for the large-scale development of the AI industry.

At the Baidu Deep Learning Developer Conference Wave Summit 2020 held on December 20, 2020, PaddlePaddle unveiled its newest PaddleHelix Propeller bio computing platform, the first general heterogeneous parameter server architecture in the industry. Its open-sourced algorithm library is comprehensively updated with the number of official algorithms extending from 140+ to 200+. The number of PaddlePaddle hardware ecosystem partners has reached 20, with 30 chip/IP models adapted or in the process of being adapted, leading the domestic industry. Baidu will continue to build the hardware-software integrated AI-technology base that is independent and controllable, accelerating the construction of the AI industry ecosystem

Up to now, PaddlePaddle has seen a strong adoption of over 2.65 million developers, including more than 5,000 contributors to its open-source community. After rounds of selection, 97 outstanding developers have become PaddlePaddle Developers Experts (PPDE). Moreover, there are 7 special interest groups (PPSIG) founded by PaddlePaddle and 132 city-level or college-level self-organizing communities across the country that take the initiative to hold PaddlePaddle community events.

In terms of industrial applications, around 100,000 enterprises have used PaddlePaddle to create more than 340,000 models in various sectors such as finance, educational training and transportation.

For talent cultivation, PaddlePaddle's training programs for teachers cover 500 universities and support over 200 universities to offer AI courses with credits. Its AI competitions attracted contestants from 580 universities in 22 countries across five continents worldwide. Due to the pandemic, PaddlePaddle has increased the investment in online courses since 2020. A total of 2.9 million people has participated in 176 online courses provided on the AI Studio learning and training platform.

Training for Users and Suppliers

- To safeguard the legitimate rights and interests of users and encourage users to defend their rights by following the law, Baidu carries out online and offline network safety education to equip users with knowledge of network security and help them avoid cyber risks. Meanwhile, we highly focus on the network security knowledge level and risk management capabilities of our suppliers and require them to have the capacity to identify whether the data provided is legitimate.

Outlook

Baidu is Duty-bound to Safeguard Data Security, Privacy Protection and Strengthen Content Management

Protecting data and personal privacy remains a long-term battle. The digital era presents endless and complicated cybersecurity challenges, including how to extend the credit boundary of AI data collaboration with technologies, how to prevent the loss of data assets caused by data abuse, and how to reduce the risk of personal information leakage. These are serious challenges that Baidu faces, together with regulators, judicial authorities, research and academic institutions.

Looking into 2021, Baidu will abide by relevant laws conscientiously and strictly, pay close attention to the legislation update in data security and privacy protection compliance, and adjust corresponding product strategies, technical set, and information processing circulation to safeguard the healthy development of Network security.

Baidu will continue to strengthen the application of next-generation technologies in the comprehensive management of data security and content across the network through the research and development of innovative AI technologies and open source, to improve security protection capabilities as well as the effectiveness and accuracy of content identification. We will strengthen multi-level cooperation with governments, industries, and academic institutions with an open and win-win approach, forging the multi-level ecological governance of cybersecurity, and creating a clean Internet environment while creating value for users.

In face of major challenges posed by AI to laws, ethics, and the entire society, Baidu will stay committed to promoting industry Internet transformation with safer AI technologies. Supported by technology empowerment, standard motivation, and Internet ecology construction, we strive to build an open and safe AI ecosystem. In dealing with algorithm bias, privacy violation, data protection, cybersecurity, we will strengthen international cooperation and contribute our wisdom and experience.

"Do Better with Tech" is not only the value of science and technology, but also the goal that everyone at Baidu strives to pursue day and night. Through empowering data with new values, Baidu is willing to work together with users to rediscover and build this new era.

Appendix

Regulations for Data Security and Privacy Protection of Baidu

Baidu has formulated multiple regulations and rules that cover data security, privacy protection, content management, etc. All these policies are mandatory across the company as well as its branches.

Regulations for security red line and product security

Baidu strictly follows the *Cybersecurity Law of the People's Republic of China* and other applicable laws and regulations. Internally, Baidu established multiple regulations, including the *Baidu Information Security Red Lines*, the *Baidu Information and Product Security Punishment Measures, Baidu Office Network Security Policies, Security Standards for Application Acquisition and Outsourced Development*, and *Baidu General Principles for Handling Security Issues*. These regulations and rules cover security red line, office security, basic security, data security, and privacy, product security, third-party cooperation security, security management, and other aspects.

Regulations for data asset management

To protect data assets and users' personal information security, and to clarify the security management strategies and principles for the full life cycle of data, Baidu has developed a framework of data asset management specifications covering the entire product-service life cycle. The framework covers multiple institutional regulations in data governance policies, data permissions, metadata, data circulation, data value evaluation, data security, and data compliance, including *Baidu Management Rules for Data Permission*, *Baidu Metadata Standards*, and *Baidu Best Practices for Data Quality Governance*.

Regulations for privacy protection

To put privacy protection of products into practice, Baidu has developed regulations including the *Master Privacy Policy, Baidu General Compliance Principles on Users Personal Information Protection, and Desensitization Standards for Personal Information.* Baidu has formulated exclusive privacy policies for its products and services, such as Baidu Maps, Baidu Netdisk, Baidu Tieba, and Baidu Input.

Standards for content management

Baidu perfects relevant standards for content management with continuous efforts, providing content support to tackle harmful information. We have formulated stringent standards of review to ensure the accuracy, fairness, authenticity, and legitimacy of the content.

Business Risk Management	Product Content Risk Management
Baidu Advertising Bans Management Policies	*Baidu Content Ecosystem Management Standards*
Commercial Advertisement Submission Manual	*Baidu General Review Standards for Ecological Governance of Harmful Information*
Standards for Determining "False or not as Described" Clients in Baidu Advertising	*Baidu Content Information Security Management System*
The Advertising Content Review Management Rules	*Quality Content Promotion Mechanism*
The Information Issuance Review Rules	*The Information Issuance Review System*
	Baidu Real-Time Inspection Rules for Information and Content
	Rules for Internet Rumors Fighting and Refutation Rules
	Baidu Disposal Rules for Underground Network Industry Information

Recognized Security Certifications

Baidu obtained numerous international and national security certifications in an attempt to ensure Internet service compliance.

Certification type	Certifications
Data security and privacy protection certifications	ISO 27018 Personally Identifiable Information Protection Management System in Public Clouds ISO 29151 Personally Identifiable Information Protection Management System Data Protection Capability of Cloud Service Users (Public Cloud) Data Protection Capability of Cloud Service Users (Private Cloud) PCI-DSS (Financial Cloud) ISO 27701 Privacy Information Management System BS 10012 Personal Information Management System
Information security certifications	ISO 27001 Information Security Management System Classified Protection of Cybersecurity (Level 4) Classified Protection of Cybersecurity (Level 3) Classified Protection of Cybersecurity (Level 2) Classified Protection of Information System Security (Level 4) (Baidu Financial Cloud System) ISO 22301 Business Continuity Management System ISO 27017 Cloud Security Management System CSA Star International Certification of Cloud Security ISO 27032 Cyberspace Security Management System The Multi-Tier Cloud Security (MTCS) Standard for Singapore
Quality management system certifications	ISO 9001 Quality Management System ISO 20000 Information Technology Service Management System
Other certifications	SOC Type 1/2 Reporting System and Internal Control Report CMMI Certificate (Maturity Level 3 of Version 1.3) level 4 Quantitative Management certificate of the Data Management Capability Maturity (DCMM - National Standard) ITSS Level 2 Cloud Computing Service Capability Standards Compliance Certificate (Public Cloud) ITSS Level 2 Cloud Computing Service Capability Standards Compliance Certificate (Private Cloud) Risk Management Capability Evaluation for Cloud Computing EAL4 Product Security Certification

User FAQs

After comprehensively sorting out the relevant issues from users' feedback, Baidu has compiled the issues of concern of users in terms of privacy protection and data security as follows:

What information will Baidu collect, and for what?

Baidu will collect and utilize users' information in compliance with situations disclosed in privacy policies. For different products or services, the purposes of collecting and using user information may vary with the business functions. We suggest you read the specific privacy policy before using the product or service at https://privacy.baidu.com.

How to delete your Baidu account, and where is user information after deletion?

Please login to your account in the Baidu App, and click "Settings" -> "Account Management" -> "Delete Account", and the system will display whether the account can be deleted according to different situations. When the requirements are met, you can delete your account after verifying via your phone number or face recognition.

Within 15 working days, the request shall be verified and proceeded. After the account is deleted, Baidu will immediately delete or anonymize users' personal information in accordance with laws and regulations.

How to block the personalized news, ads, and other content?

Users can click the "x" button at the bottom right of the recommended content and select "Dislike", after which Baidu will reduce the relevant recommendations. For all types of advertisements, users can click "Settings" -> "Ad-block" to intelligently or manually block advertisements on a website; users can also use "Settings" -> " Privacy Settings"-> "Programmatic Ad Settings" to block third-party programmatic advertisements in the news feed.

How to delete search history?

Open the Baidu App, click the search bar on the home page to open the search history dropdown. Click the "dustbin" icon next to the search records to delete them. Once cleared, the search history cannot be recovered as search history is stored in the local server.

How can user defend their rights for infringement and plagiarism?

If your original work was plagiarized, prepare the relevant documents and make a complaint at the "Copyright Complaint" module at http://copyright.baidu.com. Baidu will handle your complaints as soon as possible.

Why are security warnings popping up when browsing a webpage? How to remove it?

Baidu sets up a security warning purposely to remind users of potential security problems. The warning cannot be completely deleted or closed. If security warnings pop up frequently on the web pages, users can submit the search term, screenshot, and link of the page to "My Account" -> "Help and Feedback" -> "Suggestions". Baidu will handle your request as soon as possible.

How to answer questions in Baidu Knows anonymously or hide your answers?

When submitting questions or answers in Baidu Knows, through both desktop and mobile applications, anonymous question and answers can be set by selecting the "Anonymous" checkbox under the edit field. The content of questions or answers will be displayed in an anonymous form or the user will be marked as an enthusiastic netizen. Besides, users can hide questions and answers by clicking on "Settings"-> "Privacy Settings" in the top right of the Baidu Knows App for the setting of "My Questions Visible / My Answers Invisible".

Printed on environmentally friendly paper

Baidu Special Report on Data Security, Privacy Protection, and Content Management 2020

Address: Baidu Campus, No.10 Shangdi 10th Street, Haidian District, Beijing
Zip Code: 100085
Email: esg@baidu.com