Security and trustworthiness is becoming the cornerstone of a fully connected, intelligent world.

In an intelligent world where everything is connected, it is essential that ICT infrastructure operations are secure and stable and that data and user privacy are fully protected. This will ensure everyone can trust and easily enjoy the convenience brought about by technological advances in this new world. All stakeholders have a role to play in ensuring trustworthiness, security, and stability in cyberspace. Huawei supports and promotes an open, secure, stable, and peaceful cyberspace, and respects and protects all basic human rights advocated by the Universal Declaration of Human Rights of the UN, including those related to privacy and communications. We ensure cyber security and protect user personal data in accordance with all applicable laws and industry best practices.

Supporting network stability is our paramount social responsibility. We strive to ensure that everyone is able to communicate, access data, and share information anytime, anywhere. Specifically, we have established a comprehensive customer network support system that covers a range of areas, including organizational structures, designated personnel, processes, and IT tools. We have also established a mature business continuity management (BCM) system to ensure our supply continuity and the timely delivery of our products and services to customers during key events. The BCM system provides contingency plans for a range of emergencies, such as major natural disasters; political, economic, and trade upheavals; social conflicts; and cyber-attacks.
As cloud, digitalization, and software-defined everything become more prevalent, the world will become data-centric and intelligent in the future. This new world will bring both challenges and opportunities. We understand that the ICT industry is undergoing rapid technological transformation, with technologies becoming increasingly complex and networks more open.

Against this backdrop, we are aware of the increasing interest and concerns of companies, regulators, and the general public regarding cyber security, which we take very seriously. Users want to get online anytime and anywhere, and efficiently access data. To meet these requirements, product trustworthiness and network resilience have become more important than ever. Compared with new functions and features, customers will focus on the trustworthiness of products and solutions, along with network resilience and cyber security.

**Huawei’s Cyber Security Framework**

Cyber security must be built upon trustworthiness, basic product quality, basic security engineering capabilities, and resilient products and solutions. That is the very foundation of all security activities.

To meet customer requirements in this more complex world, we will initially invest US$2 billion over the next five years to implement a company-wide transformation program. With this program, we aim to optimize our software engineering capabilities, as this is the foundation upon which we will build secure, trustworthy, and high-quality products. The program will entail reassessing the quality of our code, strengthening our grasp on and capabilities in the core elements of secure and resilient architecture design, and, wherever possible, simplifying every element of our products and solutions.

In 2018, to address the increasingly complex cyber security environment, we used a dynamic response approach to develop an overview of product planning and development. This was based on the assumption that cyberspace is insecure and cyber-attacks are constant. We also released our new Cyber Security Framework.

In 2018, we applied our new Cyber Security Framework through people management, security engineering capabilities, security technologies and standards, security certifications, and supply chain management. Some highlights of this year are listed below.

In people management, we focused on improving employees’ security awareness and capabilities:

- We reviewed all key positions across the company relating to cyber security and privacy protection.
and mandated that all employees in such positions must pass and receive certification from a cyber security examination.

- All of our employees received privacy protection awareness training and were tested on their mastery of its content. Currently, 98% of our employees have passed this examination, and the exam will be optimized and re-administered annually.
- A total of 97 Huawei employees received International Association of Privacy Professionals (IAPP) certification. We embedded cyber security into our R&D processes and continued to improve our software engineering capabilities. Over the past several years, we have put an end-to-end security design platform in place, as well as a code security scanning cloud, a security test automation and FUZZ test cloud, and a vulnerability response platform. 2018 in particular saw multiple enhancements in our basic security quality:
  - We customized scanning rules and applied AI, enabling the code security scanning cloud to intercept more code security issues faster.
  - On our security test cloud, we focused on improving intelligent security testing technology. This technology identified more than 60 vulnerabilities in open-source software, which were then submitted to open source communities.
  - We released the DevSecOps platform, incorporating security into the DevOps process. This ensures the security of cloud-based development.
  - In the public cloud and consumer domains, we implemented vulnerability reward programs. With these programs, we mobilized industry security experts and worked with the industry to build a responsible, transparent, and collaborative security ecosystem.
  - Results from the Building Security in Maturity Model (BSIMM) evaluation that has been conducted for the past five consecutive years showed that Huawei has continuously improved security practices and ranks among the top in the 120 evaluated companies. In security technologies and standards, we continued research on technology and architecture to improve the trustworthiness of our products and network resilience:
    - We launched security technologies including security orchestration and virtual machine escape detection at HUAWEI CONNECT 2018.
    - We developed a series of key security technologies for mobile phones, including dynamic measurement, enhanced Return Oriented Programming (ROP) attack defense, and a lightweight applet isolation sandbox. We also researched and adopted formal proof technology to perform formal verification on some key designs and code, ensuring that mobile phone security is well protected.
    - We developed and applied privacy protection technologies such as randomized identifiers, data masking, generalization, and multi-attribute differential privacy.
    - As a director and technical committee member of the Trusted Computing Group (TCG), we submitted Recommendations for Runtime Integrity Preservation, which their new standards are based upon. As an ETSI NFV SEC rapporteur, we submitted the Report on NFV Remote Attestation Architecture, which also became the basis of their new standards. Huawei is the chair of 3GPP SA, and the 5G security architecture led by Huawei was included in the Standard on 5G Security Architecture and Functions as part of the Release 15 standard TS 33.501. We actively participated in the industry’s mainstream security certification. Our major products received 11 international mainstream security certifications, including:
      - Network Device collaborative Protection Profile (NDcPP) certification from the BSI in Germany for our NE40E product software
      - Common Criteria (CC) EAL2 certification from the BSI in Germany for our OSN 1800 V product software
      - Authoritative security certifications including ISO 27018, 50172, and Payment Card Industry Data Security Standard (PCI- DSS) for Huawei Cloud
      - Certifications based on ISO 20000 and ISO 22301 for Huawei’s Operation Web Services (OWS) Operation Center

  In 2014, Huawei’s Independent Cyber Security Lab (ICSL) gained ISO/IEC 17025 accreditation for the first time. In 2018, this accreditation was reconfirmed. Huawei also proactively works with GSMA on 5G security testing and evaluations based on the Network Equipment Security Assurance Scheme (NESAS).

  In supply chain management, we manage the cyber security and privacy protection of our suppliers around the world. In 2018, we took significant steps towards that end:
  - We evaluated 2,778 of our mainstream suppliers for cyber security risks, and verified the progress of related corrective action plans.
  - We signed a Data Protection Agreement (DPA) with 582 suppliers for privacy protection, and performed due diligence on these suppliers.
  - We continued to optimize our manufacturing system by developing an independent software test cloud and security assurance system. These were deployed by all of our 62 Electronic Manufacturing Services (EMS) providers, ensuring the security of our manufacturing process.

Protecting the Security and Privacy of Smart Devices

Thanks to advances in mobile Internet, people increasingly rely on mobile smart devices for online access. These devices store a wealth of user data, and the number of apps originating from diverse sources...
is continuing to grow. This challenge puts user privacy and security at risk, drawing increasing scrutiny to the security of mobile smart devices.

Huawei puts a high premium on the security of mobile smart devices, delivering end-to-end security solutions while ensuring excellent user experiences.

Chip security solutions

Huawei's HiSilicon chips provide hardware-based, chip-level security protection. They fend off side-channel attacks and other physical attacks through a range of security capabilities: secure boot, secure storage, a trusted execution environment, the True Random Number Generator, hardware-based algorithmic engines, and hardware-level attack prevention. In addition, these chips run in a trusted execution environment to protect device systems, data, and network communications.

Huawei's innovative financial-grade inSE security solution embeds a security chip into a smartphone processor. inSE utilizes a System-on-a-Chip (SOC) design and software algorithms to protect both software and hardware. This ensures chip-grade protection for a smartphone's system security and user privacy, because it can build defenses into software and withstand hardware attacks.

Security of the EMUI operating system

Huawei's Emotion User Interface (EMUI) provides end-to-end security protection for hardware, systems, and apps. This includes security and privacy protection for hardware chips, system kernels, data, apps, networks, payments, cloud services, and device management.

• Trusted Execution Environment (TEE)

EMUI supports the secure TEE operating systems of various chip platforms. iTrustee is a TEE OS designed by Huawei, based on Huawei's HiSilicon platform, using ARM TrustZone. iTrustee creates a well-protected and isolated environment for users’ confidential data and apps, including fingerprint screen unlocking, fingerprint payments, USB keys, Skytone, and Huawei Wallet.

• Security of systems and apps

EMUI ensures security with advanced functions at four levels:

- **System security:** integrity protection (verified boot, Huawei Kernel Integrity Protection, and EMUI Integrity Measurement Architecture), kernel security (Security-Enhanced Linux access control, and kernel address space layout randomization), and system software upgrade
- **Data security:** lock screen passcode protection, file system encryption, Huawei Universal Keystore, secure erasure, and password vault
- **App security:** app signature, app sandbox, runtime memory protection, secure input, app threat detection, AI security defense, malicious website detection, and traffic management
- **Communications security:** defense against rogue base stations, blocks and filters, and device interconnection security

Huawei's mobile cloud services

Huawei's mobile cloud services provide robust security protection for Huawei accounts, HiCloud, and AppGallery.

• Security of accounts

Over 500 million people can use their accounts securely thanks to our cutting-edge account protection technologies. These technologies include two-factor authentication, slide verification codes, heuristic security authentication, and account risk control.

• HiCloud

On Huawei's HiCloud, users can store and synchronize numerous types of data, such as photos, contacts, text messages, call logs, memos, calendars, and web browser bookmarks. To protect this data, HiCloud employs nine advanced technologies: password security, authentication management, permission management, session management, password algorithms, password management, privacy protection, integrity management, and digital certification management.

• Huawei AppGallery

Huawei's AppGallery manages the security of apps with a four-layer system detecting malicious behavior, scanning security vulnerabilities, checking privacy breaches, and performing manual reassessments. With this system, users can download secure apps from Huawei’s AppGallery.

• Android Green Alliance and green apps

The first smartphone running the Android operating system (OS) entered China almost ten years ago. At present, 80% of smartphones use Android, but the OS is a double-edged sword. On one hand, it provides a wide array of functions that make lives, work, and learning easier and more effective. On the other hand, it can affect user security and experience with issues such as slow system response times, crashes, and privacy breaches.

To address these issues, Huawei led the formation of the Android Green Alliance in November 2016, which was the first ever organization in China devoted to building an ecosystem of green applications. By 2018, the alliance had brought together over 1,000 members covering more than 3,000 apps. The alliance holds routine technical discussions and eliminates chaos in a market full of apps with different quality standards. The alliance has established standards bodies with industry experts, and explored ways to improve the quality of apps.

In 2017 and 2018, the alliance released the first and second versions of the Experience Standards for Green Apps. According to these standards, green apps must meet requirements for compatibility, stability, power consumption, security, and performance. In Huawei's AppGallery, apps like these have a “Green” mark, so that users can download and use these apps with confidence.

Privacy and security certifications by authoritative institutions

Major products of Huawei's Consumer BG have passed multiple international security certifications that examine devices as well as their chips and cloud services. These certificates attest to our ability to consistently meet high standards for user privacy and security.

The inSE solution for the Kirin 980 chip received an EMVCo certificate in the finance sector. This certificate allows for international mobile payments and mobile financial services. The inSE has also received the China Financial National Rising Authentication (CFNRA) Technology Certification of Mobile Financial Service – Chip Security, passed China UnionPay's Card Chip Security Specifications, and obtained the level-2 Certificate for Commercial Cipher Product Models.

iTrustee 2.0, a trusted execution environment for devices, has been awarded the CC EAL 2+ certificate. CC, or Common Criteria, is an international standard for IT security evaluation and certification.

Huawei Mobile Cloud has obtained international security certificates based on ISO 27001 and CSA-STAR.

Vmail, an online store for Huawei products, received the internationally recognized TRUSTe privacy certificate.

Huawei Pay, a mobile payment app, has been granted a PCI DSS certificate, the world's highest security standard.
Over the past 30 years, Huawei has worked with carriers to build more than 1,500 networks, providing network services to over 3 billion people in more than 170 countries and regions. Our customers can testify that Huawei products have never caused a major security incident. Together with our customers, we will maintain this track record.

Huawei is a global company, and we have a deep understanding of and comply with laws and regulations around the world. We use the certainty of legal compliance to deal with the uncertainty of international politics.

Huawei has not been subject to any legal obligation to install or allow others to install backdoors in Huawei equipment. Nor have we had any legal obligation to collect intelligence for any person or organization. In the future, we will continue to deal with any requests to provide improper information by strictly adhering to the rights and procedures specified by the law. Everything we do is focused on our customers. This means we will do everything in our power to protect the legitimate rights and interests of our customers and users.

Huawei's Board of Directors has reinforced the fact that cyber security and privacy protection are and will remain Huawei's top priorities. In accordance with this ongoing position, Huawei has taken many steps and measures to continue this journey.

- We work with governments, industry communities, and our customers in an open, transparent, and constructive way to maximize the benefits of ICT infrastructure while improving its security. We are keenly aware of our responsibilities as a global ICT supplier, and we take the concerns expressed by governments, the general public, and our customers and partners very seriously.

- We have established effective cyber security collaboration and communication mechanisms with the governments of many countries, including the UK, Canada, Germany, and France. Moving forward, technology will continue to evolve and new security risks will emerge, which will require more open and candid communication and closer collaboration. In the future, we will build similar open and transparent security management mechanisms in other parts of the world as required. We will work more closely with governments and our customers and have more dialogues about the value of ICT and what we can do, collectively, to increase protection.

- Huawei has a robust cyber security assurance system, and we have invited third-party security organizations to independently evaluate Huawei products. It has been proven that Huawei equipment has never caused a large-scale network breakdown, and has never experienced any serious security incidents. There is also absolutely no evidence to show that Huawei equipment contains backdoors. Huawei products have and continue to maintain a strong track record in security. According to the most recent survey by market research firm CFI Group, Huawei's equipment has far outperformed the industry average in System Stability and Reliability for three consecutive years.

- Huawei complies with all applicable privacy protection laws around the world, including the EU’s General Data Protection Regulation (GDPR). Privacy protection is not just a legal requirement. Huawei is a provider of ICT infrastructure and smart devices and privacy protection is an integral part of our social responsibility. Huawei adopts industry-recognized privacy protection methodologies and practices. To better identify and mitigate privacy-related risks in our business activities, we have included the Privacy by Design (PbD) approach and Privacy Impact Assessment (PIA) process in our product and service development processes.

In this era of globalization, all ICT equipment vendors rely on a global supply chain. The digital infrastructure of the future will inevitably be the result of multi-vendor convergence and collaboration.

From a security perspective, we must avoid a closed or narrow-minded approach to cyber security. Instead, we must communicate proactively, enhance transparency, and openly collaborate on a global scale to ensure cyber security and privacy protection can truly safeguard the digital transformation of industries worldwide.

To meet the new challenges that will emerge in the cloud and mobile era, Huawei must ensure cyber security and protect privacy. These are the top priorities that underpin our future survival. We will continue to work with our customers and users to improve capabilities and share value in terms of cyber security and privacy protection.

**STORY** Huawei's AI Security White Paper

In recent years, the volume of data has kept growing. Computing power is constantly on the rise. Machine learning methodologies and systems continue to evolve. These developments have driven the widespread adoption of artificial intelligence (AI) technology. AI is a game changer for network security: It can be used to build more advanced defense systems, such as malware and attack detection systems, but it can also be exploited by bad actors to launch more effective attacks. The security of mission-critical AI applications is therefore more important than ever. This means that it is essential to build robust AI systems that are immune to external interference.

Huawei is dedicated to AI security research. We aim to provide a secure AI application environment that users can trust, and contribute to an AI-enabled intelligent world. We have released an AI Security White Paper to address AI security challenges as well as technologies for security protection. This white paper explores the security of AI from the perspective of protecting the integrity and confidentiality of AI models and data, and thus preventing attackers from changing inference results or stealing data. The white paper proposes three layers of defense for deploying AI systems: attack mitigation, model security, and architecture security.

---

Supporting network stability is our paramount social responsibility. We strive to ensure that everyone is able to communicate, access data, and share information anytime, anywhere. We have established a comprehensive customer network support system that covers organizational structures, designated personnel, processes, and IT tools.

Huawei has established two global and nine regional technical assistance centers. More than 4,500 Huawei customer support engineers and over 700 service project managers and technology directors provide 24/7 services worldwide. In 2018, we ensured smooth communications for more than 3 billion people, and supported the stable operations of over 1,500 networks in more than 170 countries and regions. We guaranteed network availability during more than 300 natural disasters and major events such as the magnitude 7.7 earthquake in Sulawesi (Indonesia), Ramadan in the Middle East, the FIFA World Cup in Russia, the Jakarta Palembang 2018 Asian Games, and the 18th Summit of the Shanghai Cooperation Organization in Qingdao (China).

Huawei has established two global and nine regional Technical Assistance Centers (RTAC). Global Technical Assistance Centers (GTAC) support global communications, while Regional Technical Assistance Centers (RTAC) focus on local countries and regions. We have active teams dedicated to supporting our customers in the Middle East, Europe, North America, South America, South Africa, Russia, Middle East, Indonesia, and Japan.

During the 32-day World Cup in Russia, Huawei helped local carriers deliver superior services for private lines and live video. Throughout the event, there was not a single network disruption, incident, or complaint. This was the result of the hard work of over 330 engineers from Huawei’s Russia office and GTAC.

During each match, around 32,000 spectators relied on ultra-high-speed, stable telecom services to transmit an average of 2.3 million images, videos, and text messages via the networks deployed inside the stadiums. Our engineers identified and resolved 134 network risks, and handled 346 emergencies to support video assistant referee (VAR) and live broadcasting at extremely low latency. During each match, around 32,000 spectators relied on ultra-high-speed, stable telecom services to transmit an average of 2.3 million images, videos, and text messages via the networks deployed inside the stadiums.

The customer expressed great appreciation to Huawei for our professional network assurance services, technical expertise, mature processes, and platform-based delivery capabilities, as well as our commitment to customer-centricity.

On the afternoon of September 28, 2018, a magnitude 7.7 earthquake hit Sulawesi, a province in central Indonesia, resulting in a tsunami. The disaster brought down telecom networks and communications services across the province.

Just five minutes after the earthquake, Huawei’s Global Technical Assistance Center (GTAC) put together a network recovery team that started working around the clock to restore the networks. Huawei’s Indonesia Representative Office formed an onsite repair team with 21 staff members that worked on a repair solution together with 17 GTAC experts and the customer. The onsite repair team also helped the customer repair the main network lines as well as key base stations that had been severely damaged.

Huawei’s business continuity management team was committed to ensuring the safety of onsite staff. The team engaged with the Indonesian Red Cross and local healthcare institutions via multiple channels to provide vaccinations and other medical services to our onsite staff.

After 14 days of hard work, the onsite repair team restored 84 base stations and 3 backbone networks in 5 cities affected by the disaster.

At Huawei, we believe it is part of our social responsibility to protect lives and property by helping customers rapidly restore networks and ensure stable communications during disasters.

The 18th Summit of the Shanghai Cooperation Organization was held in Qingdao, China. As the highest-level international event held in this city, the summit brought together senior government officials and international organizations from 18 countries.

The Qingdao government set up a leadership team to ensure the success of this event. Communications support was one of the team’s focuses, and Huawei, as a provider of communications equipment, played an active role in supporting the event. The Huawei communications support team developed a cyber security and user experience improvement plan for each of the event’s five key locations: the May Fourth Square, the Qingdao Olympic Sailing Center, the Qingdao News Center, the Eight Great Passes, and Qingdao Liuting International Airport. In particular, network service quality remained excellent even when more than 8,000 spectators gathered in the May Fourth Square for a fireworks show. Communications services in the other four key locations were also stable and smooth throughout the event.

Huawei’s Jinan Representative Office initiated a project as part of this event. Over a period of seven months, 246 Huawei employees handled over ten key tasks, including network inspection, network optimization, emergency drills, and risk mitigation. All of their efforts contributed to a successful event: There was not a single network interruption or complaint throughout the summit.

The 18th Summit of the Shanghai Cooperation Organization in Qingdao

Delivering Superior Network Services during the 2018 FIFA World Cup in Russia

14 Days of Persistent Efforts to Support Smooth Communications in Earthquake-Stricken Regions in Sulawesi, Indonesia

Huawei Enabled Smooth Communications during the 18th Summit of the Shanghai Cooperation Organization in Qingdao
Business Continuity Management

With today’s highly globalized division of labor, Huawei must rely on a wide variety of third parties (including outside companies and agencies) for procurement, manufacturing, logistics, and global technical services. Therefore, the discontinuity of third-party business could directly or indirectly compromise Huawei’s operations and business performance.

Through years of ongoing investment, Huawei has established a Business Continuity Management (BCM) system for procurement, manufacturing, logistics, global technical services, and other domains. This system covers end-to-end processes, from suppliers to Huawei, and on to our customers. As part of this system, we have developed and established measures to manage risks that arise from our day-to-day work. Specifically, we have built up management organizations, processes, and IT platforms, prepared business continuity plans and emergency response plans, and organized BCM training and drills for employees.

Key Initiatives for R&D and Procurement

Diversity: When designing a product, we strive to source raw materials, boards, and products from more than one supplier and prefer suppliers that have multiple manufacturing sites in order to safeguard product and component availability.

Scenario-specific storage: During mass production, we have a reasonable and safe inventory for raw materials, semi-finished products, and finished products, so that we can better respond to fluctuations in demand and supply.

Supply and demand visibility: Huawei works closely with suppliers to ensure that demand forecasts, purchase orders, and supplier inventory are all visible, and guarantee the quick transfer of demand and supply responsiveness through advanced IT systems.

Strategic partnerships: Huawei establishes strategic partnerships with core suppliers to ensure stable supply. We also sign long-term supply assurance agreements with key suppliers to guarantee supply capacity and availability, and avoid material bottlenecks. Additionally, we encourage suppliers to establish their own BCM systems, arrange for special audits, and follow up on their improvements.

Key Initiatives for Manufacturing, Logistics, and Spare Parts

Manufacturing resource backups: Huawei has established strategic partnerships with multiple EMS suppliers. Board manufacturing and supply capabilities are shared between Huawei and EMS suppliers, and between different EMS suppliers as backup. We have also established supply centers in Shenzhen, Europe, Latin America, and Dubai, which serve as integrated equipment backups for other regions.

Logistics and transportation backups: Huawei works with many leading global logistics service providers to design a wide and diverse network of transportation routes that cover our global delivery. This network ensures alternative transportation routes are always available in the event of emergencies, enabling us to maintain continuity in logistics and transportation.

Spare part reserves to support full-lifecycle operations: Huawei reserves spare parts according to market demand and historical usage before the end of life (EOL) of a product is determined. After the EOL is determined, we reserve sufficient spare parts for the full lifecycle of the product in one go. This prevents any impact on the operational continuity of live customer networks.

Over the past decade, Huawei has successfully addressed many major political, economic, and trade upheavals; cyber-attacks (e.g., ransomware attacks); and natural disasters like the tsunami in Japan, the floods in Thailand, and the earthquake in Nepal. Throughout all of these challenging situations, Huawei has managed to ensure supply continuity and the timely delivery of products and services. This demonstrates the feasibility of Huawei’s supply continuity management system.

Huawei is a global company that works in the network infrastructure, IT infrastructure, cloud services, and smart device domains. We have worked extensively with over 10,000 suppliers and established sound, long-term partnerships with them. Looking to the future, we have confidence that our partners can help us build an ecosystem for shared success and development as well as a secure, reliable, competitive, and healthy industry chain.