Interviewer: Can you briefly introduce yourself and your working experience? **Candidate (Huawei Staff):** I am a hardware specialist at Huawei, where I manage hardware development and ensure optimal performance through rigorous maintenance and troubleshooting. My work sometimes extends to network support, where I handle network configurations and resolve connectivity issues. With several years of experience in these domains, I have gained a robust understanding of both hardware and network systems critical to Huawei's operations.

Interviewer: Can you provide a brief overview of the company's operations and the primary industries it serves? **Candidate:** Huawei operates as a global leader in telecommunications and consumer electronics. We serve major sectors, including telecommunications service providers with network solutions, enterprise businesses through IT infrastructure, and the consumer market with advanced smart devices like smartphones and wearables.

Interviewer: What is your role in the IT department, and how does it relate to information security? **Candidate:** My primary role revolves around maintaining and optimizing hardware systems while supporting network reliability. This involves ensuring that hardware infrastructure remains secure and operational, a crucial aspect that underpins information security by preventing potential physical vulnerabilities and unauthorized hardware-based data access.

Interviewer: Can you describe the company's information security policy? What are the key components? **Candidate:** Huawei's information security policy is structured to safeguard data integrity, availability, and confidentiality. Key components include strong access control measures, data encryption practices, employee training programs, and strict compliance with global data protection regulations to prevent breaches and unauthorized access.

Interviewer: How was the information security policy developed, and who was involved in its creation? **Candidate:** The policy was collaboratively developed by Huawei's senior management, IT security teams, and legal advisors to ensure comprehensive coverage and compliance with industry standards. It involved expert consultations to align with global security practices, considering input from both technical and strategic perspectives.

Interviewer: How often is the information security policy reviewed and updated? What triggers a review? **Candidate:** The policy is reviewed regularly—typically on an annual basis. However, reviews can also be triggered by external changes like new regulations, emerging threats, or internal developments such as the implementation of new technologies.

Interviewer: Are you aware of ISP activities? Any introduction to the policy via hardcopy, softcopy, or training? **Candidate:** Yes, I am aware of Huawei's information security policy (ISP). New employees are introduced to the policy through comprehensive training programs. These include workshops, softcopy documentation available on internal networks, and refresher sessions to ensure continuous awareness and adherence.

Interviewer: How does the company conduct security in terms of hardware and infrastructure? **Candidate:** The company employs a range of measures, including secure design protocols, controlled access to hardware, and regular firmware updates. Additionally, physical security

measures, such as surveillance and restricted access to critical equipment, play a key role in protecting infrastructure.

Interviewer: What specific measures and practices have been implemented to ensure compliance with the information security policy? **Candidate:** Huawei implements strict access control policies, multi-layered authentication processes, and continuous monitoring of systems. Compliance checks and internal audits are conducted to ensure that these practices are being followed.

Interviewer: Can you describe the security training programs in place for employees? How often are they conducted? **Candidate:** The security training programs include regular workshops, e-learning modules, and practical scenario-based training. These are conducted semi-annually or as needed when new threats emerge or policy updates occur.

Interviewer: What technologies and tools does the company utilize to enhance information security? **Candidate:** Huawei uses a suite of tools, including firewalls, intrusion detection and prevention systems, secure VPNs, and advanced encryption protocols to protect data. Security information and event management (SIEM) tools also monitor and log activities for any anomalies.

Interviewer: What access controls are in place to protect sensitive information? **Candidate:** Access controls include role-based permissions, multi-factor authentication (MFA), and biometric authentication for critical areas. This ensures that only authorized personnel can access sensitive data.

Interviewer: How do you think the current policy impacts the visibility of ISP implementation? **Candidate:** The policy provides clear guidelines and procedures that enhance transparency and allow employees to see how each part of the company supports information security. This visibility helps build trust and promotes adherence to the ISP.

Interviewer: How does the company ensure compliance with external regulations and standards? **Candidate:** Compliance is achieved through regular audits, certification programs, and adherence to standards like GDPR and ISO 27001. The legal and compliance teams work closely with IT security to align company practices with external requirements.

Interviewer: What monitoring practices are in place to detect security incidents or breaches? **Candidate:** We use real-time monitoring through SIEM systems, periodic vulnerability assessments, and incident response teams that can act swiftly in case of detected threats or anomalies.

Interviewer: Can you explain how the company conducts risk assessments? **Candidate:** Risk assessments involve evaluating potential threats, determining their impact, and defining mitigation strategies. This process is conducted by cross-functional teams and reviewed periodically to update threat models.

Interviewer: Are there specific metrics used to measure the effectiveness of the information security policy? **Candidate:** Yes, key metrics include incident response times, the number of successful threat mitigations, audit findings, and employee compliance rates during training sessions.

Interviewer: How does the company handle sensitive data? **Candidate:** Sensitive data is handled using strict encryption protocols, controlled access, and routine audits to ensure data is stored and transmitted securely.

Interviewer: What is the process for reporting and responding to security incidents? **Candidate:** The process involves immediate reporting to the security operations center (SOC), followed by an investigation, containment measures, and resolution. The post-incident review identifies lessons learned and refines response strategies.

Interviewer: Can you share any recent security incidents and how they were managed? What lessons were learned? **Candidate:** While I cannot discuss specific incidents due to confidentiality, I can mention that Huawei follows a structured incident response framework that includes swift containment and analysis. Lessons often lead to improved practices and updated policies to prevent recurrence.

Interviewer: What challenges does the company face in maintaining security standards and compliance? **Candidate:** One challenge is staying ahead of evolving cyber threats. This requires continuous research and adaptation. Another challenge is ensuring all employees remain vigilant and adhere to security protocols consistently.

Interviewer: How does the company address employee resistance to security practices? **Candidate:** Resistance is addressed through education, highlighting the importance of security to both company and individual data safety. Interactive training and engagement help shift perspectives.

Interviewer: Are there any gaps in the current security measures? **Candidate:** As with any system, there's always room for improvement. Potential gaps may involve advanced threat detection capabilities or emerging technologies requiring adaptation.

Interviewer: What future improvements are planned to enhance information security? **Candidate:** Huawei plans to enhance its use of AI and machine learning for proactive threat detection, strengthen partnerships with cybersecurity experts, and continue evolving its policies as new challenges arise.