Cybersecurity and Privacy Protection Policy

Contents

VNET Group, Inc. (hereinafter referred to as "VNET", "the Group", "we", "us" or "our") upholds the management principles of “professionalism, innovation, efficiency, and security”, earnestly implements cybersecurity requirements, abides by norms for compliant use of data, and builds a solid barrier for protecting users' privacy. VNET remains committed to working collaboratively with all stakeholders to address cybersecurity and privacy protection challenges, safeguard user rights and interests, and contribute to the sustainable development of both the enterprise and society.

I. Scope of Application

This policy applies to the Group, its subsidiaries and all affiliated entities. We encourage business partners, suppliers, customers, and others to refer to this policy and make commitments to enhance cybersecurity and privacy protection capabilities when cooperating with VNET.

II. Cybersecurity and Privacy Protection Governance

VNET has established a comprehensive governance framework for cybersecurity and privacy protection to ensure effective oversight and implementation. The Board of Directors delegates cybersecurity risk management oversight to the audit committee. The management operates under the supervision of the audit committee and regularly reports on cybersecurity matters. Our cybersecurity programs are under the direction of our Chief Information Security Officer (CISO). In addition, we have set up the cybersecurity and information system security leading group and the cybersecurity and information system security task force to coordinate cybersecurity and privacy protection efforts.

III. Cybersecurity and Privacy Protection Commitments

We fully recognize the importance of cybersecurity and privacy protection. We remain firmly committed to safeguarding user privacy and ensuring that our networks are secure, stable, efficient and highly available. Guided by the Group’s security objectives and applicable laws and regulations, we make the following commitments:

- Comply with the *Cybersecurity Law of the People's Republic of China*, the *Data Security Law of the People's Republic of China*, the *Personal Information Protection Law of the People's Republic of China*, and other applicable laws and regulations, as well as relevant regulatory requirements.

Implement the Multi-Level Protection Scheme and adopt industry-standard and reasonable protective measures to safeguard user information and network data, and to prevent incidents related to privacy breaches and cybersecurity threats.

- Regard cybersecurity and privacy protection as integral components of the Group's compliance and risk management framework. Conduct regular compliance reviews of cybersecurity and privacy protection, carry out internal and external security audits, and continuously improve the cybersecurity system and enhance the overall management of network and data security.
- Conduct regular risk assessments and security testing to identify and address compliance and information security risks. Promote the continuous updating of managerial and technical safeguards to adapt to the evolving threat landscape and effectively address emerging risks and challenges.
- Implement standardized and systematic management and enforce technical safeguards to ensure the confidentiality, integrity and availability of information. Establish, maintain, and continuously optimize the effective operation of management systems such as the Information Security Management System (ISO/IEC 27001) and the Business Continuity Management System (ISO 22301).
- Establish an emergency response mechanism to enhance incident management capabilities and ensure rapid response.
- In accordance with management documents such as the *Employee Handbook* and *Information Security Management Requirements*, regulate employees' behavior and enhance their security awareness. Continuously conduct ongoing monitoring of policy implementation to promptly identify and rectify deviations, fostering a closed-loop management mechanism to embed security into daily and routine operations.
- Establish an incentive mechanism to recognize and reward teams and individuals who make outstanding contributions to cybersecurity and privacy protection. At the same time, a "zero-tolerance" policy is enforced for actions such as the disclosure of private information or compromising network security. Those who delay, falsify, conceal, or omit reporting security incidents, or engage in dereliction of duty, shall be subject to corresponding disciplinary actions or penalties.
- Establish an internal employee reporting mechanism for employees to report and provide feedback on information security incidents, vulnerabilities, or suspicious content via internal communication platforms, email or telephone. A designated department is responsible for reviewing and handling reported information and its sources.
- Keep enhancing employees' awareness and capabilities in cybersecurity and privacy protection. Deliver role-specific training programs tailored to differentiated data security risks inherent in distinct positions.
- Develop the *Supplier Code of Conduct* to ensure that suppliers comply with applicable cybersecurity and privacy protection laws and regulations in the countries and regions where they operate. Suppliers are also required to participate in cybersecurity or privacy-related training provided by VNET as appropriate. We sign the relevant document, including the *Confidentiality*

Agreement, with suppliers who have confirmed their partnership with us to clarify confidentiality obligations regarding information and privacy. When necessary, the specific information security assessment shall be conducted for applicable categories of suppliers to comprehensively examine their performance and capabilities in cybersecurity and privacy protection.

- Place a high priority on protecting the personal information of employees, users, and other relevant information subjects. Continuously optimize privacy protection measures throughout the lifecycle of personal information, including its collection, storage, use, transfer, provision, and deletion. For details concerning user privacy protection, please refer to the *Privacy Statement*.

IV. Supplementary Provisions

The release and implementation of this policy is reviewed and approved by the Board of Directors. The Group will review this policy periodically, and revise it as necessary.

Matters not covered herein shall be implemented in accordance with the relevant laws, regulations, and the provisions and guidelines issued by the respective stock exchanges. VNET reserves the right to interpret the terms of this Policy.