Systems Security Policy

Table of Contents

1   NEOnet Security Statement

At NEOnet, we are committed to safeguarding the data and systems that support our operations and our customers' needs. To ensure a robust and effective security posture, we have developed and implemented security policies based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

2   Key Highlights of Our Security Approach:

- **NIST Cybersecurity Framework (CSF) Alignment**: We follow the guidelines set by NIST to ensure a risk-based, adaptive, and comprehensive approach to cybersecurity. This framework helps us continuously identify, protect, detect, respond to, and recover from potential security threats.
- **Data Protection**: We prioritize the security of sensitive and personal data through encryption, access controls, and regular audits, ensuring compliance with regulatory requirements and best practices.
- **Risk Management**: By conducting regular risk assessments, we maintain awareness of evolving cyber threats and apply necessary controls to mitigate vulnerabilities across our network, systems, and processes.
- **Incident Response**: Our incident response plan is built on NIST guidelines, enabling quick identification and remediation of any security incidents while minimizing impact and ensuring timely communication with affected parties.
- **Continuous Improvement**: Security is not a one-time effort. We regularly update our policies and practices to stay ahead of emerging threats, leveraging NIST's guidance to foster a culture of continuous improvement and resilience.

3   Our Commitment

We are dedicated to protecting the privacy and security of the data entrusted to us. Our adherence to the NIST framework reflects our ongoing efforts to meet the highest standards of security and maintain trust with our stakeholders.

For further inquiries about our security policies, please contact the NEOnet helpdesk.