Cybersecurity – Protecting people in their digital lives, with security at the foundation of everything we do

To take the position as a trusted and secure provider in all markets, Telenor has to focus on customer data protection and defend our critical infrastructure.

The cyber security threat has increased significantly over the past few years due to the digitalisation of society and customers' use of digital networks and services. Extreme weather, human and technical errors or hostile acts that manipulate or paralyse networks and services are factors that make us vulnerable.

As a network operator and provider of digital services, cybersecurity has high priority at Telenor. The quality and reliability of our telecommunications services depends on the stability of our network and the networks of other service providers with which we interconnect. These networks are vulnerable to damage or service interruptions, some of which could be caused by cybersecurity attacks. Repeated, prolonged or complex network or IT system failures could damage our services and consequently weaken the trust our customers place in us as a reliable communications provider.

We depend on suppliers and third-party providers for supply and maintenance of equipment and services. Problems related to the supply chain may adversely affect our business and operations. We work closely with our suppliers to prevent any loss, misuse or unauthorised disclosure of confidential information. This includes placing high security demands on our suppliers, who must ensure adequate levels of privacy and security to stay in business. Telenor conducts a high degree of network monitoring and carries out announced and un-announced inspections of the work performed by third parties.

In the following we present our view on how to respond to the global cybersecurity challenge.

Telenor's Commitment

Telenor is committed to providing secure, well-functioning networks and services, and has a strong interest in doing so. Our customers and society in general should have confidence in Telenor as a trustworthy supplier of safe, reliable and secure telecommunications and digital services.

To meet the fast evolving threats in the cyber domain, Telenor has developed a holistic, Group-wide and long-term security strategy aiming at securing Telenor's global business. A key element in this strategy is to continue to build critical security capabilities and competencies in all Telenor companies, as well as establishing a global security operating model. To Telenor, security is our license to operate.

A secure infrastructure built on collaboration

At Telenor we are continuously developing governance, culture and competence in order to strengthen our ability to design, deploy and operate secure infrastructure and services, both internally and externally through collaboration with our suppliers and third-party providers. This includes developing and strengthening our security monitoring system and tools, our processes, organisation and people.

A key objective for Telenor is to protect people in their digital life with security at the foundation of everything we do. To accomplish this, we are investing in security competence across our own organisation as well as with our suppliers and third-party providers, to ensure the same level of

control over our data and infrastructure, independent of operating - or business model. Security is an integral part of Telenor's business strategy and new security capabilities are constantly developed through Telenor's digital transformation.

Although all of these initiatives are important, they are not enough on their own to stem the rising cybersecurity risks. All companies need to work closely with governments and authorities across borders in the fight against cyber threats. Open infrastructures, changes in technology and the rise of new threats and sources of attack require all involved to follow a proactive and collaborative approach.

Design of laws and regulation

New cybersecurity legislation has started to materialise across the world, covering a broad set of areas. In this position we highlight two areas: protecting customer data and protecting the security of our critical infrastructure.

As authorities update and develop new laws and regulations, we believe they should follow a risk based approach. This requires assessment of the necessity and proportionality of regulatory intervention and the risks involved. Such an approach will help safeguard customer data and at the same time allow the flexibility needed for innovation. An example is cross border data transfer, where restrictions and conditions on international data flows should be kept to a minimum to ensure innovation, competition and social and economic development.

Regarding legal requirements related to network security it should be recognised that compliance can be costly. While some requirements are easy to comply with, others present a true and substantial challenge and can limit our freedom of action in terms of optimisation of our business and technology. Laws and regulations should be flexible enough to deal with technological changes. As technology evolves there will be opportunities to rethink and redesign security and how it can be provided to the benefit of authorities, businesses and consumers. Finally, any regulatory measures should be applied consistently across all providers within the value chain in a service and technological-neutral manner.

Securing and protecting personal data

Across industries we see an increased focus on the protection of personal data of consumers. In Telenor, the privacy and business security functions have a key role in ascertaining whether our current controls are good enough in protecting personal data processed in our systems and infrastructure.

By reducing security gaps and ensuring adequate data protection we can give our customers the comfort to share information and allow them to reap the benefits of the data-driven economy. However, as digitalisation of our society increases, awareness and understanding of cybersecurity threats and risks need to be expanded beyond the boundaries of our business and into the basic fabric and culture of how we as humans interact. As telecom operators we are not able to protect our customers against all digital threats. There must be recognition among consumers of the importance of safeguarding their own cyber life. This requires that governments and policy makers continue and expand their focus on this important area to ensure that their citizens are adequately informed and equipped to deal with these issues.

Moving forward together

Telenor aims to take the position as a trusted and secure provider in all markets, recognised for our responsible business practices. To fulfil this ambition, close corporation with authorities and our suppliers and third-party providers is vital to address legitimate concerns about security and protect societies and consumers from cyber threats. Telenor is committed to cooperating with stakeholders as we strive to have security at the foundation of everything we do.