SAPPHIRE™

Protect Security And Privacy By Complying With The Telecommunications (Security) Act 2021

Over the last decade, the telecommunications security landscape has changed, primarily driven by technological advancements, new protocols, increased connectivity and the emergence of more sophisticated cyber threats.

The rise of interconnected devices, such as the Internet of Things, drastically expands the existing attack surface, with more vulnerabilities now readily exposed in telecommunications networks.

With many telecommunications infrastructures playing critical roles in areas such as national security and daily life in many sectors, it is more important than ever to protect the security and privacy of all consumers in these environments.

The Telecommunications (Security) Act 2021

The Telecommunications (Security) Act 2021, or TSA for short, is a piece of legislation in the United Kingdom that aims at enhancing the security of the nation's telecommunications infrastructure. It was specifically enacted to address the evolving cyber threat landscape and to safeguard critical communication networks, aligning with the Government's Cyber Security Strategy.

Real-world examples underscore the urgency of addressing security vulnerabilities within the telecommunications sector. Incidents include state-sponsored cyber-attacks, compromises of critical infrastructure and large-scale data breaches, all of which can cause havoc on a nation-wide scale if inadequate security measures remain in place. Examples of insufficient security measures include, but are not limited to:

- Supply Chain Compromise
  - Poor Security of Third-Party Suppliers
- Network Vulnerabilities
- Lack of Security Training
- Poor Physical Security

TSA establishes a robust framework for managing cyber security risks within the telecommunications sector, recognising the critical role they play in the country. The act addresses supply chain risks, mandates the implementation of rigorous security measures and technologies, and establishes a legal foundation for managing security in the telecommunications sector. The act applies to anyone in the telecommunications sector, including:

- Telecommunications Service Providers
- National Regulatory Authorities
- Critical Network Providers
- Suppliers of Telecommunications Equipment

To comply with TSA, responsible entities must implement a series of measures to enhance security and resilience.

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001

Risk Assessment and Management

Comprehensive risk assessments should be carried out to identify and evaluate security risks to networks, critical infrastructure and the entire supply chain, prioritising the most critical vendors. Risk management strategies should be implemented to mitigate identified threats effectively.

Supply Chain Security

Adopt secure supply chain best practices to ensure the integrity of telecommunications equipment and services. Verify your assurance in third-party vendors, such as using thorough third-party risk management solutions.

Incident Response Management

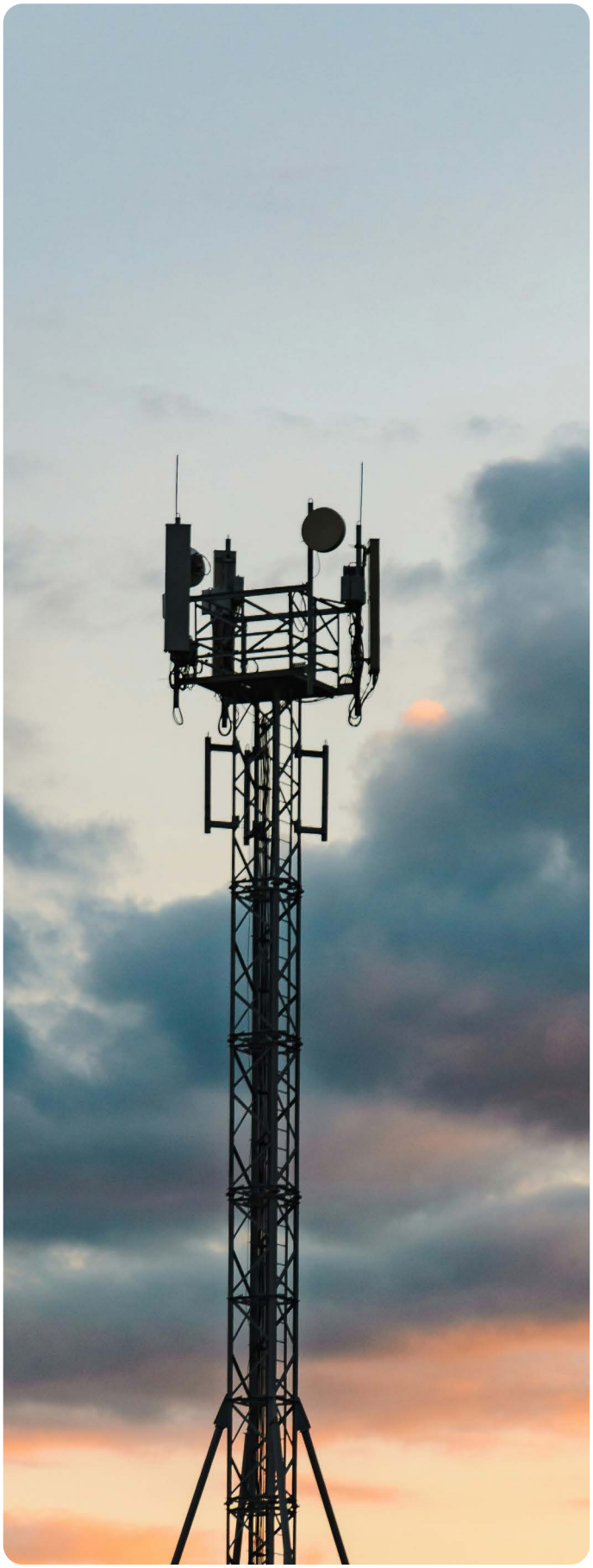
Develop and regularly test incident response plans to respond efficiently and reliably to security incidents. Establish well-defined and tested communication protocols, coordinating with relevant authorities, minimising the potential of data breaches and mitigating their impacts.

Governance and Compliance

Establish mechanisms for ensuring continuous compliance with TSA, leveraging regular audits and assessments to identify failures in compliance and/or areas of improvement. Furthermore, audits will also help verify the effectiveness of implemented security measures. Ensure business continuity and security improvement plans are in place and regularly reviewed to keep up to date with compliance with TSA and stay ahead of future changes.

Threat Intelligence and Testing

Use profound threat intelligence to receive guidance on emerging threats and enhance your security posture. Regularly conduct penetration testing and manage existing vulnerabilities to identify weaknesses in your critical infrastructure and networks. Couple this with regular patching and secure your configurations for critical assets (i.e., access management) to build a more resilient telecommunications ecosystem.



To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001

Service /Offering	Foundation	Enhanced	Advanced
Security Risk Assessment	✓	✓	✓
Security Policy Review & Development	✓	✓	✓
Supply Chain / Third-Party Risk Management	✓	✓	✓
Third-Party Risk Assessments Of Critical Suppliers	✓	✓	✓
Third-Party Threat Intelligence		✓	✓
On-Site Visits			✓
Penetration Testing	✓	✓	✓
Vulnerability Assessment	✓	✓	✓
Legislation Compliance Assessment	✓	✓	✓
Risk Assessment	✓	✓	✓
IT/OT Asset Discovery	✓	✓	✓
Security & Awareness Training	✓	✓	✓
Crisis/Disaster Response & Recovery		✓	✓
Business Continuity Planning & Testing		✓	✓
Network Security & Configuration Review		✓	✓
Identity & Access Control Management		✓	✓
Incident Management, Response & Reporting		✓	✓
Patch Configuration & Management			✓
Internal Audits			✓
Physical Security Audit			✓

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001