PacketFront Software

UK Telecom Security Act

Ensure compliance with UK TSA

UK Telecom Security Act

Ensuring compliance with TSA is a complex undertaking, which is why support is being implemented gradually. BECS® network orchestrator helps you to tick many of the boxes to comply with UK Telecom Security Act. Here is a short summary of the requirements and how we can assist in compliance.

Telecom Security Act in short

Telecom Security Bill passed the legislation in December 2021 and will be implemented between 2024 and 2028. Non-compliance can mean hefty penalties of up to £100,000 per day or £10m for not complying with the Code of Practice.

The law requires network and service providers to use best practices to prevent security risks by taking pre-emptive actions when designing, constructing, documenting, and maintaining the network. It also requires operators to protect the data as well as prohibit unauthorised access and manipulation of the network and data.

Besides doing preventive actions operators are obliged to monitor the network and services for any security compromises, and in case of a security breach have measures to remediate and recover from the incident.

Are you a Tier 3 operator?

Providers with less than £50m in turnover are currently exempted from details in the Code of Practice, but here are some of the reasons why you should consider compliance:

You can come a long way in your TSA implementation 'for free' as an additional benefit of a cost saving network automation project.

- Tier 3 providers must continue to take appropriate measures to comply with the Act.
- If you supply services, like connectivity, to Tier 1 or 2 operators you are part of their supply chain and need to comply.
- In merger and acquisition situations compliance means your assets have a higher valuation.
- And last but not least: The requirements in TSA are sensible. The security is ultimately for your benefit, so don't wait until somebody hacks into your network.

Vsaagatan 10
P.O. Box 575
SE-101 31
Stockholm, Sweden

Email: sales@pfsw.com
Email: info@pfsw.com

www.pfsw.com

PacketFront and Telecom Security Act

PacketFront is analysing the effects of the Telecom Security Act (TSA) in close cooperation with a number of carriers and legal experts. As a result of this analysis, we have concluded that the functionality already available in BECS Network Orchestrator fullfils many of the requirements presented in the Statutory Instruments (SI), but that we also need to complement with new features.

For example, BECS has a unique capability to store the desired state of all devices in its control. To fully utilise this for TSA compliance, we have implemented functionality that enables network wide configuration audits, which allow operators to identify and remedy any unauthorised changes.

In the following chapters we introduce the topics of the preliminary SI and how BECS can help you to comply.

Competency

Si: A network provider must ensure that persons given responsibility are competent and are given appropriate powers and resources.

In manually operated networks the competence is typically in the hands (or rather heads) of a few key employees. This makes it challenging to onboard new personnel leading to errors and, ultimately, security risks. When using BECS, the network is standardised and documented, this ensures that employees can quickly understand the network structure and service delivery.

In addition, PacketFront provides extensive training making sure that your personnel understand the system they are working with.

Protection of data and network functions

Si: A network provider must protect sensitive data and functions of the network.

By centralising and automating the network management you limit your exposure, as manual access to the network can be highly restricted, making it easier to control and protect. Passwords and the communication with devices as well as the system configuration are encrypted. This means you can further limit the number of employees with access to sensitive data, even when they have the permission to operate the network. Besides limiting access, automation eliminates manually introduced errors reducing the number of unintended security vulnerabilities.

Network architecture

Si: A network provider must design, construct and maintain the network In a manner which reduces the risks of security compromises.

We have been assisting carriers in building networks for more than 20 years. We, together with the hardware vendors, can advise you of best practices on how to build a robust and secure network. Designing the network, however, is just the start of the journey, maintaining it over time is more challenging - typically leading to deviation from network design as well as poor and lacking documentation.

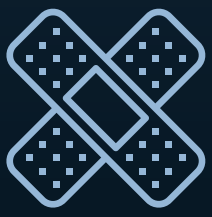
The benefit of using BECS network orchestrator is that you enforce the design rules for the network structure all the way down to individual configuration lines. This makes sure that policies are enforced - reducing the risk of security compromises.

Prevention of unauthorised access or interference

Si: A network provider must take measures to prevent the occurrence of security compromises that consist of unauthorised access.

With the help of BECS network orchestrator you can limit and control read/write access to the network by providing individual or group level user rights based on factors like geography or network hierarchy.

Even if the SI specifically recommends automation as means of preventing security compromises, it is difficult to eliminate all manual changes. However, if these changes are done via BECS, it will show what the consequences of a change are prior to committing them into the network.



Remediation and recovery

Si: A network provider must take measures to limit the adverse effects of and recover from security compromises.

If the worst does happen, due to human error or malicious act, and the network is changed in an unintended or unauthorised manner, BECS can restore the parts of the network it is managing to the last approved state as it has a database with an always current desired state of the network.

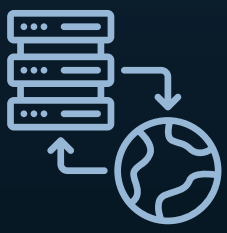
The required copies of the network configuration can easily be achieved with regular backups of the BECS database.

Monitoring and analysis

Si: A network provider must monitor, analyse, and audit the use of the Network or service to identify security compromises.

Using BECS network orchestrator means that you have full control and traceability of who has accessed the network, when they did it and what they have changed. As the changes are executed, the system automatically becomes your documentation, meaning that you have a real-time picture of your network down to details.

If an internal or external actor does manage to bypass BECS and perform changes in the network directly, the network orchestrator's audit tools will detect the changes and report them for further analysis. If deemed appropriate, it can also automatically rollback the changes.



Supply chain

Si: A network provider must identify and reduce the risks of security compromises due to third party suppliers.

The SI requires operators to reduce dependencies on single suppliers and be able to securely change a supplier, if required.

BECS multi-vendor capabilities helps you secure the supply chain, whatever happens in the commercial, technical or political spheres. It gives you full flexibility to choose hardware suppliers, and to swiftly transit between suppliers without affecting your existing services or business logic. You simply download a new 'Element Manager', as we call them.

This is good news not only from the supply perspective, but gives procurement a powerful tool when comparing suppliers offers without technical lock-ins.

Governance and reviews

Si: A network provider must ensure appropriate management of persons given responsibility for the taking of measures on behalf of the provider.

A network provider must undertake regular reviews of the security measures.

The SI defines how operators should manage and create best practices for security related administration, i.e. manage business procedures, roles, user rights and responsibilities.

The security measures should be reviewed annually to evaluate risks and results.

Testing and Assistance

Si: A network provider must carry out appropriate security tests to assess the resilience of the network or service. A service provider must not do anything which impedes the network provider to comply with the regulations and provide proportionate assistance.

Testing the security is the ultimate proof that you are compliant to Telecom Security Act.

Whether the testing is executed by your own employees or 3rd parties, the key personnel may not be aware of the tests in advance. Service providers must also give reasonable assistance to you and other relevant network providers in their testing and all parties must share information about security compromises.

Patching and Updates

Si: A network provider must deploy any security related patches or mitigations within appropriate time considering the severity of the risk. A network provider must undertake regular reviews of the security measures.

The SI specifies a 14-day time limit for deploying patches for security compromises. This can be challenging to achieve if a patch is for devices that have been widely deployed in the network. It can also be difficult to know, or prove, that all devices are running the right firmware. With BECS you can perform fast and controlled upgrades and at the same time make sure that all devices connected to the network are using the intended firmware version.

And lastly: Remember that the penalties will not be applied as long as you can prove that you have taken appropriate and reasonable preventive actions.

BECS Benefits:

- Tiered user rights and complete change logs.
- Network wide device configuration audits and reporting.
- On-line and off-line device configuration backups.
- Multi-vendor solution supporting fast changes in supply chain.
- Automated Firmware Management.

PacketFront Software

Get compliant:

Contact us for a demo, consultancy or enquiries:

Head office

Street:
Vasagatan 10, 111 20,
Stockholm, Sweden

Postal address:
P.O. Box 575,
SE-101 31, Stockholm

Email:
sales@pfsw.com

UK representatives

Phone:
+44 7718 175 652

Email:
sales-uk@pfsw.com

Poland office

Street:
Jana Pawla II 22,
00-133 Warszawa, Poland

Phone:
+48 22 487 56 25

Email:
office@poland.pfsw.com
info@pfsw.com