



This Cybersecurity & Data Protection statement explains how Inmarsat protects its systems, networks, and data from cybersecurity threats and ensures appropriate safeguards are in place when handling information.

1. Our Commitment to Security

We are committed to protecting the confidentiality, integrity, and availability of information across our operations. We implement appropriate technical and organisational measures to safeguard data against unauthorised access, loss, misuse, or alteration.

2. Security Measures

We maintain a range of security controls designed to protect our systems and data, including:

- Network security controls such as firewalls and intrusion detection and prevention systems
- Endpoint protection and regular patch management
- Role-based access controls and multi-factor authentication
- System monitoring, logging, and alerting
- Regular vulnerability assessments and risk management processes

These measures are regularly reviewed and updated to address evolving cybersecurity risks.

3. Maritime Systems Security

Given the nature of our services, we apply cybersecurity controls tailored to maritime environments. This includes securing onboard vessel IT infrastructure, protecting communications, and supporting compliance with applicable maritime cybersecurity guidance.

4. Data Protection

We process personal data in accordance with applicable data protection laws, including the UK General Data Protection Regulation (UK GDPR) and the EU General Data Protection Regulation (EU GDPR).

Our data protection principles include:

- Processing data lawfully, fairly, and transparently
- Collecting data only for specified and legitimate purposes
- Limiting data collection to what is necessary
- Maintaining data accuracy and integrity
- Retaining data only for as long as required
- Implementing appropriate security safeguards

For more information on how we process personal data, please refer to our Privacy Policy.

5. Incident Management

We have procedures in place to detect, investigate, and respond to cybersecurity incidents. Where required, we will notify affected parties and relevant authorities in accordance with applicable legal and regulatory obligations.

6. Business Continuity and Resilience

We maintain business continuity and disaster recovery processes designed to minimise disruption and ensure the ongoing availability of our services. This includes secure data backups and tested recovery procedures.

7. Third-Party Security

We require third-party service providers and partners to implement appropriate security measures where they process data on our behalf. Access to systems and data is controlled and governed by contractual obligations.

8. Training and Awareness

We provide regular cybersecurity and data protection training to our personnel to ensure awareness of security risks and responsibilities.

9. Updates to this Statement

We may update this Cybersecurity & Data Protection statement from time to time to reflect changes in our practices, technologies, or legal requirements. Any updates will be published on this page.

10. Contact

If you have any questions about this statement or our cybersecurity practices, please contact us via the details provided on our website: www.inmarserv.com

Latest update date Jan 15, 2026

No changes to main policy