



Cyber Assurance

As a trusted provider of MSP IT, Telephony and Cybersecurity Resilience services, Net-Defence is committed to maintaining the highest standards of information security and safeguarding our clients from evolving cyber threats. This attestation statement outlines the measures and certifications we have in place to protect your organisation:

1. **ISO/IEC 27001 Certification:** Net-Defence operates an Information Security Management System (ISMS) certified to the ISO/IEC 27001 standard. This certification demonstrates our systematic approach to managing sensitive information and ensuring its confidentiality, integrity, and availability. We undergo external audits annually to maintain this certification.
2. **ISO 9001 Certification:** Net-Defence holds ISO 9001 certification, signifying our commitment to quality management principles, including strong customer focus, effective processes, and continuous improvement in delivering services. We are externally audited on an annual basis to ensure compliance.
3. **Cyber Essentials and Cyber Essentials Plus Certifications:** We have achieved both Cyber Essentials and Cyber Essentials Plus certifications. These attest to our robust technical controls and processes that defend against a wide range of common cyber-attacks. External audits are conducted annually to uphold these certifications.
4. **Cyber Assurance Level 2 Certification:** Our attainment of the Cyber Assurance Level 2 certification reflects our commitment to advanced cybersecurity practices. We undergo external audits annually to ensure compliance and to maintain this certification. This certification highlights our proactive approach to risk management and our ability to respond effectively to sophisticated cyber threats.
5. **Threat Monitoring and Mitigation:** We manage and maintain a comprehensive threat detection, monitoring, and mitigation measures to protect our clients' data and systems. These include:
 - Regular risk assessments and vulnerability management.
 - Endpoint detection and response (EDR) solutions.
 - Security awareness training for our team to ensure adherence to best practices.
6. **Incident Response:** In the event of a cybersecurity incident, we have an established Incident Response Plan designed to mitigate impacts, ensure rapid recovery, and comply with regulatory and contractual obligations. We continuously improve our response capabilities through regular reviews, training, and incorporating lessons learned from past incidents.
7. **ScotlandIS ITMSP Best Practice Charter:** As a signatory of the ScotlandIS IT Managed Service Provider (ITMSP) Best Practice Charter, we adhere to its essential and enhanced standards. These include secure configuration, asset management, and regular monitoring, as well as fostering cyber resilience throughout the Scottish digital ecosystem.

We remain committed to transparency and continuous improvement in our cybersecurity posture. If you require additional information or specific details about our security measures, please do not hesitate to [contact us](#).