NET-DEFENCE

Welcome to Net-Defence

Wherever you are on your business journey,
Net-Defence has a solution tailored to you.

Defence, Protection, Security.

I lead the organisation at Net-Defence, providing IT (MSP), telephony, cyber security & resilience services to our customers. We aim to protect, provide support and help keep your organisation secure and resilient today, and in the future.

Since 2018, I have worked for the business, and in 2020 stepped into the role of Managing Director, building a team of skilled professionals, focusing on what is right for the business and the client and keeping resilience front of mind.

As an SME ourselves, we strive to understand our customer's concerns and frustrations. We endeavour to put our customers at the heart of our business, working with individuals to truly understand their position and provide solutions that are tailored to the individual needs of a business.

We promise to provide bespoke advice without the jargon, business resilience without the worry, and give your organisation the very best in protection, connectivity & support. With a vast amount of information available online, we are passionate about simplifying IT, telephony and cyber resilience making it affordable, attainable, and available to all.

Partnering with our specialists allows you to reduce your threat risk level, protect your organisation from the most common threats, attain appropriate certifications and safeguard your data.

Debra Cairns
Managing Director

Cyber Essentials

Get certified. Protect your organisation from the most common cyber threats.

The National Cyber Security Centre (NCSC) operates Cyber Essentials (CE), a UK Government scheme designed to defend your business from common cyber threats.

As an IASME certifying body, we manage your certification process end-to-end and in-house, helping to simplify the accreditation process.

Cyber Essentials is aimed at helping you to safeguard your business from the most common cyber threats while ensuring the application of best practices across your entire IT infrastructure.

Most attacks are simple by design, but the state of play is constantly changing and evolving. As a result, threats can come in many disguises all with the same end goal; to exploit weaknesses in your infrastructure. Completing and maintaining your CE accreditation reduces your threat risk and helps safeguard your organisation's processes, people, customers and finances.

Cyber Essentials – what does it cover?

- Focuses on assessing technical controls.
- Demonstrates proactive management of cyber threats.
- Involves a self-assessment questionnaire.
- Provides certification eligibility for Cyber Liability Insurance for UK organisations with a turnover of less than £20m.

Cyber Essentials Plus – what does it cover?

- Our certified CE+ assessor will audit your controls on-site and we will collaborate with you to highlight any areas that require improvement to achieve your accreditation.
- A remote assessment is also available.
- To obtain this accreditation you must demonstrate to your employees, customers, and stakeholders that you take cyber security and Information Security Standards seriously.

Cyber Assurance

IASME Cyber Insurance - affordable, achievable cyber security standard.

IASME Cyber Assurance – a Cyber Security Standard developed through a government-funded project, provides an alternative to ISO27001 for smaller organisations.

This standard focuses on your Information Security Management System (ISMS) and through a risk-based approach, assesses your people, processes, technology and assets demonstrating the level of cyber security, privacy & data protection across your organisation.

This standard enables compliance with many UK Laws, legislation and regulations, centred on protecting the three key aspects of your information known as the CIA Triad – Confidentiality, Integrity and Availability.

Certification levels:

- Level 1: Risk-based appraisal of key security aspects.
- Level 2: Independent audit of processes and procedures.

When combined with Cyber Essentials, these certifications:

- Protect from common cyber threats.
- Provide assurances of industry best practices.
- Reduce the risk of cybercrime through data compliance.
- Demonstrate commitment to Information Security, Quality Assurance, and Security Standards.
- Ensure compliance with legislation, regulations & best practices.

ISO 27001 Certification

ISO27001: The Gold Standard in IT security, cyber security & privacy protection.

In the ever-changing landscape of information security and cyber threats, safeguarding your organisation's data and ensuring robust cyber security measures is paramount.

Our services include the ISO 27001 certification, offering a comprehensive and internationally recognised framework for managing information security.

Key Features:

- Risk Management: Identify and manage information security risks effectively.
- Legal Compliance: Ensure compliance with relevant laws, regulations, and contractual obligations.
- Data Protection: Safeguard sensitive data from unauthorised access or disclosure.
- Continuous Improvement: Establish a culture of continuous improvement in information security practices.
- Global Recognition: Gain international recognition for your commitment to information security.

Our ISO 27001 Services:

- Gap Analysis: Assess your current information security practices against ISO 27001 requirements.
- Implementation Support: Expert guidance to implement the necessary controls and processes.
- Risk Assessment: Comprehensive risk assessments to identify and mitigate potential threats.
- Certification Assistance: Navigate the certification process smoothly with our support.

Compliance

Empower your business with confidence:
achieve compliance excellence.

Education is key to business resilience in the world of cyber security. Conducting regular testing and implementing training programmes to raise awareness in your organisation can help to form a robust defence against cyber threats.

Security Testing

We can help protect your organisation with security testing designed to detect vulnerabilities within systems and infrastructures. Our services encompass perimeter and web application penetration testing and vulnerability testing, backed up by the provision of full, comprehensive reports for risk mitigationWith new threats are emerging every day, we are here to help you build the best defence possible. Get in touch with one of our specialists to understand more about how we can help you and your organisation.

Training

As with most things in life, awareness is key. The weakest link in your organisation is potentially your employees. Email-based cyber attacks pose a significant risk. Our phishing simulation and cyber security awareness platform provide education in a straightforward, easy, and agile manner.

PCI DSS

In the constantly evolving digital transactions landscape, it is crucial to ensure the security of payment card data. Our PCI DSS (Payment Card Industry Data Security Standard) certification services provide a robust framework to safeguard cardholder information and maintain a secure payment environment.

Key Features:

- Cardholder Data Protection: Implements measures to secure and protect cardholder information.
- Secure Payment Processing: Ensures secure handling of payment transactions and data.
- Access Controls: Restricts access to cardholder data on a need-to-know basis.
- Regular Monitoring: Implements ongoing monitoring and testing of security controls.
- Incident Response: Develops and maintains an incident response plan for security breaches.

CIS Benchmarking

Modern businesses rely heavily on Software-as-a-Service (SaaS) platforms to streamline operations. But with this increased reliance comes a heightened need for security.

Our CIS Benchmarking service offers a simple, effective solution. By following globally recognised security standards, we can help you identify and address vulnerabilities in your SaaS environment, reducing your risk of cyberattacks and data breaches.

Security Operations Centre (SOC)

Vigilant security and proactive defence to keep your business running securely.

A Security Operations Centre (SOC) provides an additional layer of vigilant security in the dynamic cyber security landscape.

Providing real-time monitoring, threat detection, and rapid response we can help maintain the integrity and resilience of your digital infrastructure keeping your business running efficiently, effectively and securely.

Why use our Security Operations Centre?

- 24/7 Monitoring: continuous surveillance to detect and respond to potential threats around the clock.
- Threat Intelligence: using the latest threat intelligence to stay ahead of evolving cyber threats.
- Incident Response: rapid and effective response strategies to mitigate and neutralise security incidents.
- Advanced Analytics: utilising cutting-edge analytics for in-depth threat analysis and proactive defence.
- Real-time Monitoring: continuous surveillance of networks, systems, and data to identify anomalies.
- Incident Detection and Analysis: swift identification and thorough analysis of security incidents.
- Threat Hunting: proactive search for hidden threats within the network to enhance security posture.
- Incident Response Planning: developing and implementing effective strategies for rapid incident response.
- Log Management and Analysis: comprehensive analysis of logs to identify potential security events.

Benefits of SOC Services – how will they help your business?

- Proactive Threat Mitigation: identify and neutralise threats before they impact your business.
- Enhanced Incident Response: rapid response to security incidents, minimising potential damage.
- Continuous Security Improvement: learn from incidents to enhance overall cybersecurity measures.
- Compliance Assurance: align SOC services with regulatory requirements for robust compliance.
- Our Security Operations Centre is not just a service; it's your proactive defence against the evolving threat landscape. Partner with us to build your digital frontier and stay one step ahead.

Cyber Security & Resilience Bundles

Bringing together relevant certifications to prevent cybercrime.

Cyber resilience bundles, bringing together certifications to protect and defend your business from cybercriminals, while delivering cost and effort savings.

Your best allies in your battle against cybercrime are prevention and preparation. When you don't know where to start, these bundles are a clear pathway to reducing risk and protecting your business operations.

The most effective prevention approach is obtaining certifications that provide you and your customers with assurance that you have taken appropriate steps to reduce your risk, demonstrate your compliance, and protect your data and information.

The most well-known is the Cyber Essentials Certification, aiming to safeguard your business from the most common cyber threats while ensuring the application of best practices across your IT infrastructure. Cyber Essentials Plus is a higher-level certification that gives the added reassurance of an independent assessment.

Beginner Bundle:

- Cyber Essentials
- Cyber Asxsurance
- Basic Policies

Advanced Bundle:

- Cyber Essentials
- Cyber Assurance Level 1
- Cyber Essentials Plus
- Cyber Assurance Level 2
- Basic Vulnerability Testing
- Basic Policies
- Cyber Assurance Toolkit

Value & Outcome

Independent attestations, recognised across the UK, that demonstrate your commitment to protecting your business operations, data and assets. Delivering additional value through:

- Demonstrating to your employees, stakeholders, and the external world that you prioritise information & cybersecurity controls.
- Assuring that you are compliant with all legislation, regulations & best practices for securing your data and information.
- Competitive advantage over your peers.
- Access to new public and private sector customers who often require this as a mandatory expectation.
- Significantly reducing your threat from outside and internal attack.

IT Support MSP

IT support services designed to meet your business needs today and tomorrow.

Our IT support services are designed to meet your operational business needs. From service desk and end-user support to managing your IT infrastructure, we're here to offer advice and deliver continuity, resilience, and security to protect your business operations.

End User Support

- End user & device support & management.
- Remote monitoring & management.
- Backup solution (end user documents).

Infrastructure Management

- Hourly cloud-based backup and restoration testing.
- Remote monitoring.
- Patching and security management.
- Advanced anti-virus and EDR management.

Why use us for infrastructure management help and support?

- With us as your partners, you'll receive as standard:
- A simple structured support plan with clear success measures.
- A service where all data backed up securely and encrypted at source.
- Restoration from backup is tested.
- Access to our certified subject matter experts.
- Confirmation that all devices are protected, compliant and secure.
- An annual service and technology recommendation review.
- No long-term contracts.

Backup & Recovery

Ensuring your backup is timely and tested for actual recover to protect your data.

No matter the size of your organisation or the area you work in, there is one thing we all have in common. Without access to IT and communication systems and information, as businesses we will be unable to operate.

Data loss can come from many sources, including cyberattacks, ransomware, fire, flood, and malicious damage to name a few. Your ability to recover is reliant on the quality of and frequency of your data backup.

Your data is invaluable to you, therefore, ensuring that your backup is timely, accurate, and tested for actual recovery is critical. As your requirements are specific to you, we have designed a range of options to meet your requirements.

Virtual Server Package *(*bespoke options)*

- 2000GB included as standard, and additional GB is available if required.
- Daily off-site backup.
- 30-day retention.
- Monthly backup archive.
- Hardware or any additional hardware is not included.
- *Hourly to 4 hourly off-site backups.
- *Monthly restoration test of off-site backup.
- *Daily restore to on-site location.
- *Daily test of on-site restore.
- *Set retention period.
- *Backup archive.
- *Rapid recovery on-site backup.

Physical Server Package

- 2000GB included as standard, and additional GB is available if required.
- Daily off-site backup.
- 30-day retention.
- Monthly backup archive.
- Hardware or any additional hardware is not included

M365 Server Package

- Control retention and recoverability.
- Fully individual mailbox backup and restore.
- Keep Microsoft 365 backups in the region.
- Backup Exchange, Teams, SharePoint and OneDrive.
- Physical and Virtual Server Backup Benefits.
- Efficient backup: unique methods allow you to back up more frequently and retain data for longer while using the same amount of storage and network bandwidth.
- Security through separation: your data backup is stored entirely separate from your infrastructure; both physically and digitally. This means should you suffer a cyber attack your backup is not accessible to the attacker.
- Cloud storage built for security. Our data centres meet ISO compliance, and our solutions use AES 256-bit encryption to protect your backup data in transit and at rest.
- Comprehensive platform support – With support for Microsoft Windows, Linux, Mac OS X, VMware vSphere, and Microsoft Hyper-V, your backup is engineered to cover your entire network.

Secure Hosting

Securing your infrastructure to ensure the right access to data.

Ensuring the confidentiality, integrity, and availability of your data and applications is a critical component of modern digital infrastructure.

Whether you're running a single website, hosting sensitive information, or managing large data sets, a secure environment is essential.

Hosting

Cloud Hosting – AWS (Amazon Web Services) & Azure:

- Easy to use: designed to allow easy migration from your on-premises infrastructure and applications to cloud-hosted.
- Flexible: you can select the functionality and setup that matches your organisation's requirements.
- Cost-effective: you pay only for the computing power, storage, and other resources you use, with no long-term contracts or up-front commitments.
- Reliable: you take advantage of a scalable, reliable, and secure global computing infrastructure.
- Secure: utilising an end-to-end approach to secure and harden your infrastructure, including physical, operational, and software measures.

Net-Defence's secure server room hosting:

- Easy to use: designed to allow easy migration from your on-premises infrastructure and applications to our hosted secure server room.
- Flexible: you can select the functionality and setup that matches your organisation's requirements.
- Cost-Effective: you pay only for the services required.

Telephony Services

Find the communication solution that is right for your organisation.

In December 2025, BT Openreach, which owns and manages the current traditional telephone network that the ISDN/analogue system operates on, will be switching off.

This means you will have to move to a VoIP (voice over internet protocol) cloud-based solution to meet your telephony needs.

What if you wait for the PSTN switch-off?

Our advice, don't wait! You should begin reviewing your communication infrastructure now. If you wait until 2025, demand for VoIP services will be very high which could result in installation delays. There is also the possibility that some of your services may not be easy to transition and you could risk the continuity of your business operations.

What are your options to get ready for the PSTN switch-off?

VoIP will become the technology behind your communication infrastructure. This will allow you to communicate over the internet via voice, video, images, and files. Part of your communication may already be using this technology if you are using applications such as Teams, Zoom, WhatsApp and FaceTime for calls and video.

The benefits of the cloud-based system include:

- Cost savings.
- No hardware to purchase and maintain.
- Potential reduction in your current monthly charges.
- No call charges (all inclusive).
- Protects business continuity (99.999% uptime) and continued connectivity in disaster situations (all inbound calls can be diverted).
- Enables remote working and collaboration from anywhere on any device.
- Simple, user-friendly platform for voice, video and messaging.
- Scalable and customisable without the need to buy extra equipment.
- Agile and instant self-service call management; call diverts, voicemail etc.
- No physical back-end system to purchase or maintain.
- Continued local end-user support from Net-Defence.

Cabling Installations

Durability and reliability with bespoke cabling solutions.

The backbone of your IT infrastructure and communication systems.

Having a more organised cabling infrastructure can provide:

- Long-term cost reduction and return on investment.
- Greater business continuity.
- Resilience across your organisation.

We can offer two types of cabling installations – Structured and Point-to-Point.

Network Cabling requires a fair amount of strategic planning and implementation. This means that Structured Cabling is always recommended over Point-to-Point Cabling. As a data transmission system, structured cabling supports data, video, multiple voices, and various management systems such as security access and energy systems.

Structured Cabling is a planned cabling system that systematically sets your fundamental communication mediums. This includes video, multimedia, voice, data security and control for the present and the future.

Copper and Fibre cabling is always recommended over Point-to-Point cabling, which is a far more basic system that connects one point of communication to another.

With Structured Cabling, you can easily make changes to your system, this allows maximum performance, availability, and inbuilt redundancy.

Satellite Internet

No 4G connection or fibre broadband – no problem.

Broadband connectivity continues to be a real business headache in areas with no 4G signal or fibre services. We already support our customers with traditional broadband and 4/5G connectivity and have been working with our sister companies to find a solution for areas where traditional connectivity does not work or is not available.

The answer – broadband satellite internet services!

Leveraging satellite technology, we have been able to provide a cost-effective and reliable internet service. Using a low-to-Earth orbiting satellite constellation, reduces the time for data to circulate between the user and the satellite (known as latency). This type of connectivity can now deliver high-speed internet capable of supporting video calls, streaming and online gaming, something that isn't possible with traditional satellite constellations.

The upfront costs are low and there are no long-term contract tie-ins, we offer a 30-day rolling contract.

Our recent installations:

Ogilvie Construction was ready to break ground on a site in a remote area of Aberdeen. As this was the very first phase of construction there was no fibre in the area and 3G mobile connectivity was unstable. Without connectivity, the start of the project would have been delayed. We were able to install satellite broadband within a working week. The installation of a new instance of fibre broadband can take up to three months and incurs substantial costs (thousands of pounds).

First Vehicle Leasing, the latest addition to the Ogilvie Group, moved to brand new offices and required immediate connectivity and unfortunately, 4G connectivity was weak and unreliable in the area. We installed satellite broadband and the site was up and running within two weeks. Once the permanent fibre broadband is installed the satellite system will stay in place, and will be used for backup resilience. As this connection will only be used if the primary line fails, there is no cost while the connection is dormant. If required, the connection can be activated remotely.

Benefits:

- High speed, reliable internet service.
- Small upfront costs (hardware).
- Short lead time for installation, and immediate activation.
- 30-day rolling contract, when active.
- No cost for retaining resilience backup to primary connection.
- Immediate remote re-activation (once hardware is installed).

Mobiles and Mobile Phone Security

Embrace streamlined workplace communication.

Mobile phone solutions for your business

Offering unmatched convenience, reliability and accessibility, mobile phones offer a suitable alternative to VoIP systems. Creating a customisable mobile phone plan for your business generates a flexible, cost-effective solution that aligns with the needs of your business while reducing unnecessary expenses.

A flexible alternative to VoIP for better communication at work.

Attractive cost savings thanks to strong provider relationships.

Take control of your data and prevent unexpected bills.

Customise your contract depending on the needs of your business.

Mobile phone security including two-factor verification.

Comprehensive account management helping to free up your time.

How can Net-Defence help?

- Preferential pricing through our mobile communication partners.
- Flexible contract terms using major networks such as O2, Vodafone and EE.
- Access to the latest handsets from all major manufacturers including Apple, Samsung and Google.
- Fully customisable contracts, allowing you to pool mobile data, roaming bolt-ons, calls and text bundles to prevent unexpected bills.

Mobile Device Management

Mobile Device Management (MDM) allows businesses to manage, monitor, and secure mobile devices from a centralised point, ensuring compliance, enhancing security, and boosting productivity.

This protects sensitive data via encryption on a company device, remote wiping, and password enforcement while simplifying IT management. *

**Note: Personally owned devices should remain out of scope for MDM deployments unless your organisation runs a BYOD policy.*

Business Resilience as a Service

Our new service enables you to blend our core and supplementary services into one manageable solution that suits your business needs.

This new all-in-one support solution ensures your business is secure, connected and prepared for the most common cyber threats.

By combining our core services with cyber accreditations and secure network solutions, this package helps you to create a resilient infrastructure that safeguards your operations with no upfront costs.

Why choose BRaaS?

- Savings with no capital upfront costs
- Seamless support from one reliable contact
- Timesaving within your team so you can focus on the day-to-day
- Streamlined operations with a flexible range of core and supplementary services
- A one-stop turnkey solution for business resilience
- A hand-picked package tailored to your exact business needs
- Next level prevention, detection, and connectivity.

Core Services

Cyber Essentials
The Cyber Essentials certification is designed to help you safeguard your business from common cyber threats.

IT MSP
Our IT Managed Service Provider Support assists end-users with device management and backup solutions.

Education and Awareness
Through IT Infrastructure Management, we pro-actively safeguard your IT environment and your company data.

IT Infrastructure
Prepare your workforce and prevent human error through our training and phishing simulation service.

Supplementary Services

Cyber Assurance

Telecommunications

Mobiles

Security Operations Centre

Connectivity and Networks

Licensing and Hardware

Ogilvie House, 200 Glasgow Road, Stirling FK7 8ES

Ogilvie House, Team Valley Trading Estate, Gateshead NE11 0NF

Tel: 03300 241 666 · **Web:** net-defence.com

Registered in Scotland No. 116592 · VAT No. 400892864