Get Cyber Certified

MSP security questionnaire

Questions for a managed service provider, based on the NCSC's guidance for SMEs

To the managed service provider

We're reviewing who supports our IT. The National Cyber Security Centre (NCSC) advises small and medium-sized organisations to check an MSP's certifications, services, security and contract terms before choosing one. These questions follow that guidance: Choosing a managed service provider (MSP).

Please answer each question and return this form by the date below. You can type straight into this PDF and save it, or attach your own documents (such as an SLA or a responsibilities matrix) and refer to them in your answer.

Our organisation

Our contact (name and email)

Please reply by

Date sent

Your organisation (registered legal name)

Companies House number

Your contact name and role

Email and phone

1. Certification

The NCSC advises choosing an MSP that holds a recognised certification. Cyber Essentials is the UK government-backed certification scheme; Cyber Essentials Plus adds a hands-on technical audit. We'll check any certificate on the official NCSC certificate search.

1.1 Do you hold a current Cyber Essentials certificate?

☐ Cyber Essentials ☐ Cyber Essentials Plus ☐ Not yet

Certificate number

Legal name on the certificate

Expiry date

1.2 Does your certificate cover your whole organisation, including the devices and accounts your staff use to support clients? If it covers only part, which part?

If you hold Cyber Essentials that covers the devices you use to reach our systems, that also helps us confirm those devices for our own Cyber Essentials (IASME's guide to working with contractors, Option A).

1.3 Do you hold any other certifications, such as ISO 27001 or SOC 2, or follow another security standard?

1.4 If you don't hold Cyber Essentials yet, do you plan to, and when?

2. References and track record

2.1 Please give two references from clients of a similar size or sector to us.

2.2 Briefly describe how you handled a security incident affecting a client (anonymised is fine).

3. Security services

The NCSC suggests agreeing these measures up front, checking which carry an extra charge, and writing what you agree into the contract.

3.1 Security updates (patching)

What's your update policy? How quickly do you apply critical and high-risk security updates (the NCSC recommends, and Cyber Essentials requires, within 14 days of release)? Does it cover computers, servers, phones and tablets, network equipment, firmware and cloud services?

3.2 Backups and recovery

What would you back up for us, how often and where (including any copy held off-site or offline)? Who can access the backups? How often do you test a restore, and how would you get us running again after a ransomware attack?

3.3 Your access to our systems

How do your staff connect to our systems (remote tools, VPN, restricted IP ranges) and is that access monitored? Does every account your staff use with us have its own named login with 2-step verification (2SV/MFA)? How do you keep admin rights to a minimum, protect admin credentials, and remove access when one of your staff leaves or our contract ends?

3.4 Logging and monitoring

Do you keep logs for security purposes? How long are they kept, and can we (or an incident response provider we appoint) access them?

3.5 Incident response

Do you have a tested incident response plan? How, and how quickly, would you tell us about an incident affecting our systems or data, including one that starts in your own systems?

3.6 End-of-life systems

Who tracks when our hardware and software stop receiving security updates, and advises us before support ends?

3.7 Your own suppliers

Which third parties or subcontractors would have access to our systems or data, and how do you check their security?

3.8 Staff training

How do you train your own staff on security, and how often?

4. Contract and service levels

4.1 Response and resolution times

What response and resolution times would your SLA give us? (As a starting point, the NCSC suggests a response within 1 business day for minor issues and under 1 hour for urgent ones, and 2 to 3 business days to resolve routine issues.)

4.2 Do you provide a responsibilities matrix showing what you do and what we do?

☐ Yes (attached) ☐ Yes, on request ☐ No

4.3 How does the contract set out liability for vulnerabilities, damage and the impact of incidents?

4.4 Reporting and reviews

What regular reports would we receive (for example patch compliance, backup success, security alerts, uptime), and how often would we review the service together? Insurers may ask for these reports after a claim.

4.5 Term, renewal and exit

How long is the agreement, how does renewal work, and what notice is needed to leave? On exit, how would you hand back our data, admin accounts, credentials and documentation, and remove your access?

4.6 Which of the services above are included in your price, and which would cost extra?

5. Completed by

Name

Role

Date

☐ I confirm these answers are accurate to the best of my knowledge.

About this questionnaire. Prepared by Get Cyber Certified, an IASME-licensed Certification Body, from the NCSC's guidance Choosing a managed service provider (MSP) (version 1.0, 24 November 2025). It isn't produced or endorsed by the NCSC or IASME, and we don't recommend or endorse any MSP. Free to use and share.

For MSPs without Cyber Essentials: we certify IT providers too, and eligible organisations with fewer than 250 employees can get 75% off a first certificate through the government's First Step Fund. See getcybercertified.uk/for-it-partners.html.