GUIDANCE

# 10 Steps to Cyber Security

**Guidance on how organisations can protect themselves in cyberspace.**

IN THIS GUIDANCE

**PUBLISHED**

11 May 2021

**REVIEWED**

11 May 2021

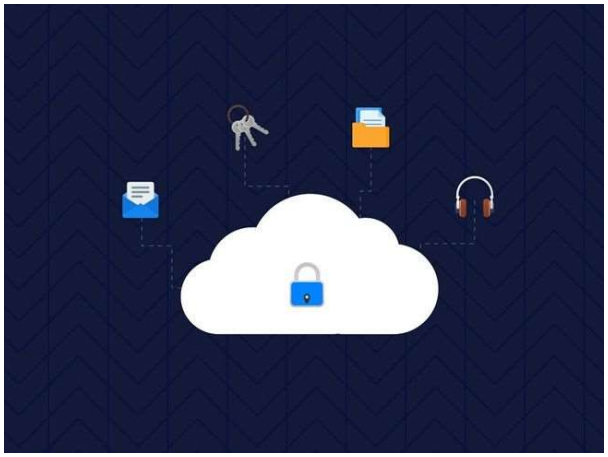
**VERSION**

1.0

**WRITTEN FOR**

Cyber security professionals

## Data security



### Protect data where it is vulnerable.

Data needs to be protected from unauthorised access, modification, or deletion. This involves ensuring data is protected **in transit**, **at rest**, and at **end of life** (that is, effectively sanitising or destroying storage media after use). In many cases data will be outside your direct control, so it important to consider the protections that you

can apply as well as the assurances you may need from third parties. With the rise in increasingly tailored ransomware attacks preventing organisations from accessing their systems and data stored on them, other relevant security measures should include maintaining up-to-date, isolated, offline backup copies of all important data.

---

## What are the benefits?

- **Being able to have confidence that your data is appropriately protected, wherever it is**
- **Being able to restore important data and systems quicker with practised backups (if access is disrupted for any reason)**
- **Enabling storage media to be reused or disposed of with confidence, by ensuring that sensitive data cannot be recovered from decommissioned or re-purposed devices**

---

## What should you do?

**Protect data in accordance with the risks**

- Ensure you know what data you have, where it is stored and what you consider most sensitive, and apply protections based on the risks you have identified. Avoid storing data that you don't need, and consolidate data where possible to make it easier to secure and manage. Where there is a requirement for data to be replicated or cached, ensure that all copies are sufficiently protected. Data that is dispersed (for example, files on users' desktops) can be easier for attackers to find and harder to audit.
- Ensure that data is appropriately protected in transit to ensure data is not inappropriately viewed or interfered with. Unencrypted communications can provide opportunities for attackers to capture sensitive data or move laterally on 'trusted' networks by spoofing a service or making it easier to spoof authentication to another system. You should use secure, encrypted and authenticated, application protocols

wherever possible and use network layer encryption such as Virtual Private Networks (VPNs) where needed.

- Ensure that data is protected at rest. Implement physical and logical access controls so that only authorised users can access and/or modify your data. Disk encryption should be used where there is a risk of physical theft, such as laptop computers and removable media. Disk encryption does not protect data on running systems, so they also need to be secured to protect access to the data. File encryption and Digital rights management solutions can help restrict who can access data, particularly when data needs to be shared externally.
- Use current standardised cryptographic algorithms to protect your data. Old algorithms or those that haven't been accepted as standards will provide less protection and could result in a false sense of security. Our guidance for TLS and IPSec describes recommended cryptographic profiles for these purposes. Ensure where cryptography is used, you also protect the cryptographic material (such as certificates and keys) from unauthorised access.
- Ensure interfaces that enable access to sensitive data are well defined and expose only the necessary functionality to reduce the opportunity for an attacker to abuse them. Access to bulk datasets should be rate-limited. Only grant the ability to run arbitrary queries over sensitive datasets to users if there is a legitimate business need and it's carefully monitored. This should be considered a privileged role.
- Log accesses to data and monitor for unusual queries, attempted bulk exports of data, and administrative access to detect possible compromises.
- Consider where you are relying on others to protect your data, such as in cloud services, in your supply chain or on staff's personal devices. Understand what measures you can take to protect your data, and what assurances you need to seek from the third parties.
- Understand your legal responsibilities, including any regulations applicable to your

sector. Our GDPR security outcomes guidance, developed jointly between the Information Commissioner's Office (ICO) and the NCSC, describes a set of technical security outcomes that are considered to represent appropriate measures for the protection of personal data under the Data Protection Act 2018.

**Back up your data**

- Ensure you backup any data that is essential for running your business. This should include your business data as well as configuration data required to operate your systems. Having suitable backups will help you recover in the event of an incident, whether an accidental file deletion or a major cyber attack.
- Have multiple backups of important files stored in different locations. The '3-2-1' rule is a popular strategy that can be used in most scenarios; at least 3 copies, on 2 devices, and 1 offsite backup. This helps ensure that if one copy is compromised, there is at least one other copy intact. This is a key mitigation against ransomware as up-to-date backups will enable you to recover your data.
- Ensure that an offline backup is kept separate from your network, or in a cloud service designed for this purpose. Restrict access to credentials and servers used for backups because attackers may target your backups, either as a way to obtain your data or to destroy your ability to recover them. You should also ensure that previous versions of files are protected from accidental or malicious deletion, for example when using cloud synchronisation services for backups. You should also ensure that previous versions of files are protected from accidental or malicious deletion, for example when using cloud synchronisation services for backups.
- Retain backups for a period of time, rather than just have a single rolling backup as this does not provide much protection if an infection/damage isn't noticed before the backup is overwritten. Consider how long it may be before something is detected and ensure your backups are kept for longer (at least a month).
- Test your backups regularly and ensure you know how to restore files from a backup

before you have to do it for real. Ensure you can gain access to your backups in the event of a complete system failure.

- Reduce the risk of re-infection when restoring data from backups by re-installing executables from trusted sources instead of backup, and ensuring operating systems and application software is up to date on the target systems. Malware may persist in backups, so you should ensure files are scanned using up to date antivirus software when they are being restored.

**Securely sanitise storage media when no longer needed for its designated purpose**

- You should have a policy for the re-use, repair, disposal and destruction of storage media and any devices that could store data, (including office equipment such as printers and photocopiers, monitors and TVs). If your data is not properly sanitised, there is a risk that it could be recovered and viewed at a later date without your knowledge. Our secure sanitisation of storage media guidance gives more information on how to sanitise different types of media.
- Plan for sanitisation when you are procuring equipment, including understanding what you will need to do and the associated costs. Ensure sanitisation methods chosen for your data storage devices and/or media are proportionate to the risk of unauthorised access for that data, including reputational risk if it were to be publicised. This will help you avoid unexpected costs and risk when you come to dispose or re-use storage media. For example, Solid State Disks (SSDs) can be difficult to sanitise reliably, so you should consider destroying them.
- Before disposal, ensure all labels or markings that indicate ownership of the device (or the nature of the data contained) are removed. If using trusted third parties for destruction hold them to recognised standards and obtain destruction certificates.
- Periodically verify that your data is being sanitised appropriately, and test destruction processes and equipment.

---

## Learn more

[GDPR security outcomes]
This guidance describes a set of technical security outcomes that are considered to represent appropriate measures under the GDPR.

[Protecting bulk personal data]
15 good practice measures for the protection of bulk data held by digital services.

[Design pattern: safely exporting data]
How to implement a secure end-to-end data export solution.

[Secure sanitisation of storage media]
Why sanitisation is necessary, the risks to manage, and how to sanitise affordably.

[Cloud security guidance]
Guidance on how to configure, deploy and use cloud services securely.

[Mobile Device Guidance: Bring Your Own Device]
Guidance for organisations on enabling staff to use their own smartphones, tablets, laptops and desktop PCs to access work information.

← Identity and acce...

Logging and monitoring →

## Topics

Operational security  Risk management

**PUBLISHED**

11 May 2021

**REVIEWED**

11 May 2021

**VERSION**

1.0

**WRITTEN FOR**

Cyber security professionals

## Also see


**Weekly Threat Report 23rd July 2021**

The NCSC's weekly threat report is drawn from recent open source...

Report
23 July 2021


**The first Certified Cyber Professional (CCP) Specialism is now live!**

'Risk Management' is the first certifiable specialism under the...

Blog Post
8 July 2021

**NCSC statement on Kaseya incident**

The NCSC's official statement on the Kaseya cyber incident.

News
5 July 2021