



ETHOS Data Security Protection Toolkit Certification

Implementing the 10 Data
Security Standards

ETHOS Cyber Security Services

If you operate within the UK Health and Social Care Sector you will probably have already been asked if you have the Data Security and Protection Toolkit certification. This is a core certification that is needed to operate in this sector.

ETHOS comprehensive certification service generates all the documentation and evidence you require to meet the 56 DSPT mandatory requirements set against the 10 National Data Guardian Data Security Standards. To become DSPT certified for “Standards Met” you will need to meet 56 mandatory requirements.

What are the 10 National Data Guardian Data Security Standards?

The National Data Guardian publishes these standards, organised under three leadership obligations:

People, Process and Technology

These 10 data standards are published on the NHS Digital website and are:

1. All staff ensure that personal confidential data is handled, stored, and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.
2. All staff understand their responsibilities under the National Data Guardian’s Data Security Standards including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.
4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access data to personal confidential data on IT systems can be attributed to individuals.
5. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
6. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.
8. No unsupported operating systems, software or internet browsers are used within the IT estate.
9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian’s Data Security Standards.

ETHOS utilises a model of elapsed implementation, with an expected timeframe of three weeks in which to manage the assessment process, with only limited input from you and your team. This delivers efficiencies for your business, leaving us to handle your certification process.

We will:

- ✓ Register you with the ICO and request an ODS code from the NHS if you do not already have these.
- ✓ Quickly generate your Record of Processing Activities (ROPA) and Information Asset Register (IAR)
- ✓ Develop the policies and procedures required to meet the standard Including Data Security, Data Quality, Data Protection, Network Security and GDPR compliant Privacy Police where they do not already exist.
- ✓ Generate the additional evidence records required to meet the standard including Training Matrix and Confidentially Audit
- ✓ Generate any Forms your will need to meet the standard but do not have yet, including Portable Devices Assignment Form, Data Protection Impact Assessment Form and Data Breach Impact Assessment Form
- ✓ Complete all the assertions and submit associated evidence through the DSPT Portal and once complete, we will publish your assessment.

What are the 10 National Data Guardian Data Security Standards?

ETHOS has taken many organisations through the DSPT certification Process. We understand the standard implicitly and know exactly how to generate your evidence to allow you to meet all the mandatory requirements.

NHS digital estimate the process takes most organisations an average of seven weeks elapsed to compete, but ETHOS team typically deliver in three.

Our price for this service includes:

- ✓ The documentation and evidence that needs to be generated for your business
- ✓ A professional handover at the end of the process to ensure you understand what has been created for you, what has been submitted on your behalf and how to ensure re-certification in 12 months
- ✓ Complement your DSPT Certification with a Cyber Essentials or Cyber Essentials Plus certification within the same elapsed timeline if you so wish, under an additional work package.

What evidence and documentation are required?

Whilst the exact documentation and associated evidence required to become DSPT Certified can vary slightly from one organisation to another, our experience is that most organisations require the documentation set out below. We can produce it all for you and provide advice and guidance on how to implement it, as needed.

- DSP Toolkit Staff Awareness Questions
- Record of Processing Activity (ROPA)
- Information Asset Register (IAR)
- Device and Software Allocation Record
- Data Security Policy
- Data Quality Policy
- Network Security Policy (optional, depends on the organisation)
- Record Keeping Policy
- Data Protection Policy
- Privacy Policy
- Password Policy
- Bring Your Own Device (BYOD) Policy
- Training Matrix
- Portable Devices Assignment Form
- Data Protection Impact Assessment Form
- Data Breach Impact Assessment Form
- Confidentiality Audit Log Template
- Confidentiality Audit Log
- Confidentiality Clause for staff contracts (only where you do not already have this)

ETHOS is available to answer any questions you may have about the DSPT Certification process or to provide a fixed price quote and a more detailed explanation of how we intend to approach your certification.

For more information about ETHOS safety and innovation work please find us on:



[@LtdETHOS](#)



[linkedin.com/company/ethos-ltd](https://www.linkedin.com/company/ethos-ltd)

or email us at: info@ethos.co.im