Secure Data Management for Utility Surveys

Best practice guidance (Revised August 2026)

From the Utilities and Subsurface Mapping Panel
Chartered Institution of Civil Engineering Surveyors

Contact
Chief Executive Officer
Chartered Institution of Civil Engineering Surveyors
ceo@cices.org

Endorsed by

Introduction

The civil engineering surveying profession is often told that ‘data is the new oil’, but do we care for and protect data in a way that reflects this value? With building information modelling (BIM) and digital engineering increasingly becoming business-as-usual, the data collected and managed by utility surveyors is both essential and valuable. As well as being of value to the client, contractor and project operators, utility survey data can be used beneficially for research, nationwide mapping initiatives, education and training. However, it is also of value to those who pose a threat to the commercial success of a business and to the safety of the societies we live and work in.

Good data management is about being security-minded and risk-aware. It should avoid creating unnecessary processes and costs but should have proportionate systems and procedures in place that are easy to understand and follow. The Utilities and Subsurface Mapping Panel (USMP) of the Chartered Institution of Civil Engineering Surveyors (CICES) has produced this updated best practice guidance to highlight areas that all professional surveyors should be mindful of when conducting a utility or subsurface survey and recommended steps to consider. Professional surveyors should show leadership in highlighting potential vulnerabilities to clients. Good data management is a business advantage and surveyors following this guidance should ensure they promote their adherence to best practice, demonstrating the value they place on a security-minded approach to data management.

Accreditation schemes adhered to by companies can assist in demonstrating compliance with good data management practice. For example, certifications such as Cyber Essentials, Cyber Essentials Plus and ISO27001 for information security management systems, provide proof that a company has rigorous data management systems in place, while schemes such as the PUMA PAS128 utility mapping accreditation not only demonstrate compliance with the BSI PAS128 specification but also include sections assessing a company’s maturity in terms of data management, with a section examining how a company fulfils the requirements of this guidance document.

About this guidance

The guidance has been designed to cover the role of the surveyor at each stage of the survey lifecycle. It is intended that surveyors and client organisations can refer to it at any of these stages:

- Tendering.
- Planning and risk assessment.
- Data collection.
- Data processing and handover.
- Data storage, retention and disposal.

The guidance refers to data in its widest sense, from desktop utility records searches and site reconnaissance to utility detection and verification. The term ‘data’ includes everything from historic paper records and photographs to digital geospatial and geophysical data, such as CAD drawings, electromagnetic location (EML) and ground penetrating radar (GPR) data, point clouds and 3D models for use in augmented reality applications.

While centred on utility surveys, the guidance will be applicable to other types of survey, especially those using mass-data capture methods such as 3D laser scanning, LiDAR and unmanned aerial systems (drones). The guidance is specifically aimed at surveyors working in the UK but will also be of use to international surveyors in considering the many facets of secure data management. Client organisations may also find the guidance useful when commissioning surveys.

Data and risk

Without appropriate measures in place, data can be easily copied, compromised through unauthorised changes, leaked or unintentionally disclosed. This is of particular concern where the data being collected is sensitive. There are three main areas of risk to consider:

- Physical – Where? From the location of the survey site to the office where the data is processed and archived, are there any risks you need to be aware of?
- Personnel – Who? From the individuals capturing the data on site to the processing and creating of models, to storage and exchange, are there any risks around who has access to the data?
- Technical – What? From the equipment and software being used to capture and process the data to how it is stored and disseminated, are there any risks you should be considering?

By considering these three areas at each stage of the survey, the risks to the security of sensitive data can be managed holistically, across the project lifecycle.

1. Tendering

When tendering for any survey work, the surveyor should consider the security of sensitive data at all stages and include appropriate and proportionate measures where required. The surveyor should:

01. **Site Assessment**
    Assess the site and/or asset being surveyed. If specific security measures are stipulated in the tender documents, plan the bid around these. If no, or minimal, security guidance is stipulated by the client, consider the Triage Process for the Publication or Disclosure of Information[1] from the National Protective Security Authority (NPSA) and assess the risk. Contact the client to discuss what additional measures may be needed. Sites requiring higher security measures could include utilities supplying or being adjacent to:
    - Critical national infrastructure.
    - Defence, law enforcement, national security or diplomatic buildings.
    - Commercial sites that create, trade or store significant volumes of valuable materials, currency, pharmaceuticals, chemicals, petrochemicals or gases.
    - Landmarks, nationally significant sites or crowded places.
    - Locations or routes used to host events that could have a security significance.
02. Assess the neighbouring buildings and infrastructure assets. If the survey will need to collect data on these, consider if they are sites that require additional security measures.
03. **Existing data**
    If the client is supplying existing data, appraise the management of that data, whether in print or digital formats, and consider the following:
    - Will copyright licences be needed or included?
    - Will any of the supplied data be sensitive and therefore will additional security measures be required? For example, concerning who has access to the data or if it can be downloaded and stored offline.
    - Will data be combined from various sources? Consider if the management of combined data could allow sensitive information to be deduced and require additional security due to the information that can be gathered from models and simulations.
    - Will live monitoring data be shared? Consider who would require access to the system and what knowledge they would have of the alert codes and validation.

[1] Triage Process for the Publication or Disclosure of Information: www.npsa.gov.uk/security-best-practices/build-it-secure/security-minded-approach-open-shared-data

04. **Data collection**
If tendering for a survey at a site where the data will require higher security measures, consider what employee screening is required. If working regularly on projects that require higher security, consider arranging vetting[2] for staff to demonstrate to clients that the survey company has a security-minded approach to data and to enable faster deployment.

05. **Data processing**
Make the client aware if external data processing, modelling and visualisation will be subcontracted to another company and if this company is based in the UK or overseas. If considering an overseas subcontractor, appraise what data would be sent for processing and if there could be any risk to intellectual property or to the commercial success of a business or if the location could be considered potentially hostile or a security threat to the UK.

06. **Data delivery requirements**
The client should supply clear directions for the delivery arrangements for hard and soft copy survey material, including raw survey data and what encryption is required.

07. Be aware of how the client expects to validate and verify the delivered survey data.

08. **Data retention and storage**
The client should supply clear directions about the retention of survey data for warranty or professional indemnity purposes by the surveyor.

- If the surveyor is permitted to store the data, the storage requirements should be reflected in the contract (for example, Cyber Essentials, Cyber Essentials Plus[3] or ISO 27001[4] certification).
- If the surveyor is not permitted to store the data, a 'digital fingerprint' system, for example, could be considered. This is where the client takes full responsibility for the storage of the survey data, with a verified manifest created on data delivery. If an issue or dispute arises, the client has to provide the surveyor with copies of relevant survey data, the authenticity of which can be verified using secure digital signatures generated during delivery of the original material.
- The surveyor should check what requirements its insurance company has in relation to retention of, and access to, relevant data.

09. If the data is being stored in the cloud or in a file sharing system for the surveyor, client or third party, consider if there are any access restrictions in the country that hosts the storage server. While ensuring the security of potentially sensitive data, it is important not to block access to data that can be shared under defined and agreed terms for permitted purposes.

10. **Data ownership**
The client should assert in the contract who owns the data and its permission requirements for sharing data with third parties. The surveyor could explore with the client the advantages and risks of data sharing, dependent on the project and collection method.

11. The client should state who will take ownership of excess data collected above the requirement, for example through mass data collection methods and if it is permissible for sharing or onward sale to third parties. Clients should be mindful that some survey quotes may be artificially low in order to win a competitive tender, as the loss may be compensated by onward sale of data.

[2] www.gov.uk/government/publications/government-security-classifications/government-security-classifications-policy-html
[3] www.ncsc.gov.uk/cyberessentials/overview
[4] www.bsigroup.com/en-GB/products-and-services/standards/iso-iec-27001-information-security-management-system/

2. Planning and risk assessment

At the planning and risk assessment stage, the surveyor should:

01. Assess the site, assets and/or building being surveyed and check if the contract requires higher security measures to be applied. Ensure the measures stipulated in the contract will be complied with.

02. Assess the neighbouring buildings and assets. If data could be collected on these, find out who the building occupiers are and notify them that a survey will be taking place. This step is essential if the survey site includes or is close to a site that would require additional security measures. The client should not be relied on to notify the occupiers.

03. If mass data collection methods are being used, consider if data of a building's interior could be collected, including for example, whiteboards in offices or name plaques on doors and inform the client and building occupiers, as they may want to mask these prior to data collection.

04. The survey zone should only be expanded if it is efficient to do so, for example, when mass-data collection tools are the most appropriate method of data collection for the survey. The survey zone should not be expanded for the sole reason of collecting excess data for possible onward sale without the prior permission of the client. If the survey zone is increased, assess the security risks around collecting data on all buildings and assets within the expanded zone.

05. If there is publicity surrounding the project, especially a sensitive one, this could increase the risk of the data being stolen or obtained for malicious use. Consider this extra risk when planning the timing of the survey and if extra security personnel or other measures will be needed.

06. Ensure field surveyors are conscious of the vulnerability of equipment to theft and that they are aware of any pin code protection and tracking devices available, as well as standard theft mitigation measures[5].

07. When collecting sensitive data, ensure secure wifi or data transfer methods will be available on site, or as close as possible to the site, for upload via a secure device. Do not rely on open insecure wifi networks in public places. Ensure the device/s are secure, for example access is limited to named employees, accounts are password protected and require multi-factor authentication. Consider guidance[6] from the National Cyber Security Centre (NCSC) on device security.

08. If sensitive data will be stored on a removable drive or memory card, ensure this is encrypted and password protected, and that the field surveyors are aware they need to remove the drive or card from the equipment as soon as the data collection is complete and keep it in a secure place until the data can be transferred.

09. If sensitive data is to be transferred to a cloud server or a secure data storage location from the field, ensure these are access-controlled and password protected. Consider NCSC guidance[7] on sanitisation of storage media and wipe the removable drive or memory card as soon as the data has been uploaded for processing or transferred in the field. If the data cannot be deleted from the collection tools in the field, appraise what additional protective measures will need to be in place to prevent unauthorised access.

10. Consider how survey equipment will be transported to and from the site. Caging equipment within a vehicle is considered best practice, however if the survey will require overnight stays, a secure location should be arranged so the equipment is not left in a vehicle overnight.

11. Consider if the data will be processed in-house or subcontracted. Ensure that the processors and modellers will be aware of any additional security measures. If external processors and modellers are being used, disclose this to the client if not mentioned in the contract, and consider if any confidentiality agreements need to be signed.

[5] The Survey Association's Theft Mitigation Measures: www.tsa-uk.org.uk/downloads

[6] www.ncsc.gov.uk/collection/device-security-guidance

[7] www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media

3. Data collection

At the data collection stage, the surveyor should refer to the risk assessment and should:

01. Carry out data collection in accordance with the survey plan and risk assessment. If no additional security measures were stipulated and the field surveyor/s feel the survey warrants them, they should talk to the lead surveyor about the potential vulnerabilities and risks, and if these need to be discussed with the client.

02. Adhere to theft mitigation measures. Ensure any tracking, locking mechanisms and entry pins on equipment are used. The field surveyor/s should be aware that the data could be potentially more valuable than the equipment. If the equipment and data is stolen, inform the client, the building owner, the building occupier and the police as soon as possible.

03. Ensure the lead surveyor is aware of any data collected above the contracted requirement.

04. If using a removable drive or memory card, remove the drive or card from the equipment as soon as data collection is complete and keep it in a secure place until the data can be transferred to a secure data storage location.

05. Ensure the data transfer method and device/s are appropriately secure. Do not rely on open insecure wifi networks in public places.

06. When transporting equipment to and from site, ensure it is secure (preferably caged within a vehicle). If the survey requires overnight stays, transfer the equipment from the vehicle to a secure location overnight.

4. Data processing and handover

At the data processing and transfer stage, the surveyor should refer to the contract and any related security documentation and should:

01. Clear all data from removable devices and on-board memory of the survey equipment as soon as it has been downloaded to a password protected PC or uploaded to the cloud or server.

02. If the survey collected data about neighbouring buildings and infrastructure assets, consider:

- Removing any data from any collections submitted to the client that is not required, especially if any of this information is sensitive or not already in the public domain, for example information about security sensors.
- Whether any additional security measures are required to protect data that is not publicly available and will be included in a common data environment accessible to multiple organisations or stakeholders.
- If the survey has led to aggregation or augmentation of significant amounts of data, for example the enhanced view of data used in augmented reality (AR) systems, such as AR headsets. This can increase sensitivity and should be shared in a controlled manner.
- Whether there are requirements in the contract or associated documentation for any additional security measures to protect data about utility routes and underground structures of neighbouring assets.

03. If the survey collected any sensitive data, including the interiors of buildings, provide appropriate protection to the raw data set and provide access on a strict need-to-know basis. Any redaction should be carried out during post processing and only the redacted version should be stored in any common data environment unless there are appropriate security controls in place.

04. Follow the directions for the delivery arrangements to the client for hard and soft copy survey material, including raw survey data. If additional security measures are in place, ensure systems are compliant and up to date with the stipulated requirements and that upload and download facilities are protected. If the client requested a hard copy deliverable, ensure a traceable postage method is used.

5. Data storage, retention and disposal

If storing, retaining and disposing of data, the surveyor should refer to the contract and should:

01. If the contract stipulates that the surveyor can keep a copy of the data for warranty or professional indemnity purposes, follow the storage security requirements in the contract (for example, maintaining Cyber Essentials, Cyber Essentials Plus or ISO 27001 certification). Retain the data securely for the contract period plus the length of the warranty – no longer. Once this period is reached, securely dispose of all data connected to the contract. A process should be defined for the regular review of stored data and disposal of data that is past the agreed retention period.

02. If the contract stipulates that the surveyor cannot retain a copy of the survey data, prepare a manifest of the data for the client to verify and consider using a secure digital signature to verify the manifest against data delivery.

03. Be conscious of staff changes and remain alert to any risks that new staff coming into the company could pose with open access to archived sensitive data.

04. If using an escrow holding arrangement for third party data, appraise the validity of this arrangement annually.

05. If the contract allows for any data to be shared by the surveyor with a third party, consider how this data will be managed by other users and be mindful that it can be sold onwards. Ensure all personally identifiable or potentially commercially or security sensitive data is obfuscated or removed before being received by any third party.

06. If the contract allows for the data to be used by the survey company for internal audit or training purposes, ensure all personally identifiable or potentially commercially or security sensitive data is obfuscated or removed before being used in this way.

07. Maintain a security-minded culture throughout the survey company:

    - Make the management of security risks a key part of all surveying activity and decision-making.
    - Keep abreast of legal requirements relating to privacy and data protection, and other security related laws, codes and standards.
    - Keep security procedures and processes simple and appropriate, and not inhibitive of appropriately controlled data sharing.
    - Empower employees at all levels to challenge and report potential vulnerabilities and suggest opportunities for improved security.

This guidance has been prepared by the Utilities and Subsurface Mapping Panel (USMP) of the Chartered Institution of Civil Engineering Surveyors (CICES).

Lead authors: Dr Neil Brammall CEng MIGEM CGeog (GIS) FRGS FCInstCES M.ASCE, Janos Dobsi FCInstCES MBA and Sam Roberts FGS FCInstCES with advice from NPSA.
With thanks to members of the Utilities and Subsurface Mapping Panel for their contributions.

Version 2.0
August 2026