Security Awareness

The Chartered Institution of Civil Engineering Surveyors (CICES) was established by royal charter to advance the science and art of civil engineering surveying for the benefit of the public. Members should be aware of their responsibilities to the public and other third parties by performing their work with integrity and professionalism, and by taking into account the safety and security of those around them at all times.

Security can be defined as the state of relative freedom from threat or harm caused by deliberate, unwanted, hostile or malicious acts. These include acts of espionage, extortion, fraud, sabotage and terrorism. Good security requires civil engineering surveyors to be aware of their behaviour, both professionally and socially, as well as using procedures and technology appropriate to the sensitivity of the work being undertaken.

Security minded behaviour should be adopted by members at all levels, from Student Member to Fellow. Specifically, members are expected to apply their professional judgment and consider the following actions:

- Identify vulnerabilities, taking account of potential harm to people, to data systems, and to what is being constructed or surveyed – including neighbouring assets that may be covered by the survey. Think about any increased risks from federated systems you may contribute to.
- Make the management of security risks a key part of all surveying activity and decision-making. Security risks are generally interdependent and each needs to be considered in the way it could link to others.
- Understand and comply with legal requirements relating to privacy and protection, and other security-related laws. Where relevant, follow codes and standards, and seek improvements where reasonably practicable. Keep security processes simple. Overly-elaborate procedures written in complicated or contractual language can be difficult to comply with.
- Contribute to a culture where workers at all levels are able to challenge and report potential vulnerabilities and suggest opportunities for increased security.
- Appraise security risks as new technology and equipment is brought into use. This is especially relevant for geospatial survey technologies.
- Protect sensitive information and data – whether it be societal, personal, environmental or commercial – when it is collected, communicated, used and stored. Check the security levels of your systems and the interconnections between them, as well as any cloud services. Securely delete any data held on board equipment as soon as practicable and report the theft of equipment with data still on board to the client.
- Be aware of what is in the vicinity of your project, and the security of neighbouring buildings and infrastructure. You could be capturing or holding data about them too.
- Use social media responsibly. Think about the consequences of what you are revealing about yourself, your organisation and the projects you are working on.
- Think about what you share online or in presentation materials. Remember that information and data placed on the Internet or made publicly available can still be accessible years after it is first published. It is virtually impossible to delete, destroy, remove or secure all copies of released information.
- Learn from security breaches and incidents, including near misses.
- Accept that it is impossible to completely protect everything, but do all that you reasonably can to protect people, assets, sites, infrastructure, data and information.

This document has been based on security guidance produced by the UK government's Centre for the Protection of National Infrastructure. For detailed information, members are directed to https://www.cpni.gov.uk/developing-security-mindedness-approach

Build it Secure includes the Security-Minded approach to Digital Engineering; Security-Minded approach to Information Management; and the Security Considerations Assessment https://www.cpni.gov.uk/build-it-secure-0

Members are encouraged to familiarise themselves with the *Guidance on Security for Engineers and Technicians* produced by the Engineering Council. http://www.engc.org.uk/security

Members are encouraged to follow the UK BIM Framework, particularly BS EN ISO 19650-5:2020 Security-minded approach to information management. https://www.ukbimframework.org/standards/

Guidance from the National Cyber Security Centre is at https://www.ncsc.gov.uk/section/advice-guidance/all-topics

Of particular interest may be cloud security https://www.ncsc.gov.uk/collection/cloud-security

SaaS guidance https://www.ncsc.gov.uk/collection/saas-security

Supply chain security https://www.ncsc.gov.uk/collection/supply-chain-security

Cyber security for construction businesses https://www.ncsc.gov.uk/guidance/cyber-security-for-construction-businesses

chartered ices

Version 3 March 2022