Engineering Council

GUIDANCE ON SECURITY

for engineers and technicians

May 2016

Guidance on Security for Engineering Professionals

This guidance sets out six key principles to guide engineers and technicians in identifying, assessing, managing and communicating issues about security. It also describes their associated responsibilities to society and generally being security-minded.

1. **Adopt a security-minded approach to your professional and personal life**
2. **Apply responsible judgement and take a leadership role**
3. **Comply with legislation and codes, understand their intent and seek further improvements**
4. **Ensure good security-minded communications**
5. **Understand, comply and seek to improve lasting systems for security governance**
6. **Contribute to public and professional awareness of security**

Security is referred to both explicitly and implicitly in several Engineering Council documents including the UK Standard for Professional Engineering Competence (UK-SPEC), the Information and Communications Technology Technician (ICTTech) Standard, and within the learning outcomes for accredited degrees and approved qualifications and Apprenticeships. The Engineering Council will review this guidance periodically and welcomes comments on it. Professional engineering institutions are encouraged to use it to assist them in developing guidance for their members.

Security

Security can be defined as the state of relative freedom from threat or harm caused by deliberate, unwanted, hostile or malicious acts. It operates on a number of levels ranging from national security issues to countering crime. It includes preserving the value, longevity and ongoing operation and function of an enterprise's assets, whether tangible or intangible, and the handling of privacy issues such as the protection of personally identifiable information.

The role of engineers and technicians

The behaviour of people is central to any engineering enterprise and the security of its operations, products and services. Assets can be compromised by individuals through lack of knowledge, carelessness, complacency and deliberate non-compliance. Therefore, in addition to physical, technological and process aspects, security must necessarily involve consideration of people and their potential behaviour, both in their professional duties and when sharing information including when using social media.

Appropriate and proportionate security should be an integral part of the design and operation of an asset, and encompasses its whole lifecycle. It must recognise that threats and vulnerabilities change and evolve over time.

Good security can enable business benefits and competitive advantage by protecting key assets and services, and engendering trust.

By following the six principles within this guidance, engineers and technicians should be able to:

- reduce the vulnerabilities in assets, systems or operations
- provide early warning of potential threats
- reduce opportunities for unauthorised or gratuitous access to information to plan hostile acts and/or the compromise of design and intellectual property
- explain and manage security risks in an appropriate and proportionate manner
- minimise the potential impact of security breaches or failures on their work, clients, services and the supply chain
- improve the resilience, reliability, effectiveness and trustworthiness of their product, process or service
- enable economic and societal benefits to be realised securely

Principles to guide engineers and technicians

These six principles will guide engineers and technicians when identifying, assessing, managing and communicating issues about security.

1. Adopt a security-minded approach to your professional and personal life

A security-minded approach requires engineers and technicians to:

- be aware that their behaviour, use of social media, publications and public presentations affects their own security and the security of others
- assess potential threats and vulnerabilities end to end, taking account of the potential harm to people, the asset or system, and the sensitivity of the information, which may be societal, environmental or commercial
- be aware that security risks are interdependent, adopting a holistic risk management view that is appropriate and proportionate, and is an integral part of all engineering activity and decision-making
- remember that security risk assessment is an aid to professional judgement, not a substitute for it
- be aware that overly-elaborate processes and procedures can lead to poor compliance and undermine a security culture
- identify vulnerabilities that may be used in a hostile, malicious or inadvertent manner to create security breaches or failures
- be responsive to changes in the operating environment, including the impact of changes in use of the asset or system, its wider connectivity and emerging threats and vulnerabilities

2. Apply responsible judgement and take a leadership role

When implementing a security-minded approach, engineers and technicians should demonstrate a commitment to privacy, reliability and ethical conduct by:

- leading others in improving practice
- working with other professionals to ensure informed, proportionate, holistic judgements
- empowering all those involved to identify potential security challenges and opportunities
- being prepared to challenge assumptions and proposals
- ensuring that everybody reporting to them has the opportunity to maintain competence in the area of security

3. Comply with legislation and codes, understand their intent and seek further improvements

Seeking advice where necessary, engineers and technicians should:

- be aware of, and comply with, the security-related laws in countries where they operate or where their products or services will be used
- act in accordance with relevant security-related codes of conduct
- recognise and understand the intent behind security standards and codes, as well as their limitations
- seek further improvements where reasonably practicable, thus embedding a culture of continuous security development

- be open-minded and avoid using regulations to facilitate complacency

4. Ensure good security-minded communications

Good security depends on communicating effectively and appropriately with customers, clients, suppliers, sub-contractors and non-engineering colleagues. Engineers and technicians should:

- adopt appropriate measures to protect sensitive information when it is communicated, used and stored, both within and beyond their organisation
- be able to express clearly the risks and benefits
- where appropriate, encourage an ‘open reporting’ approach to security risks, incidents and near-misses, coupled with a spirit of questioning and learning
- take a measured approach to publishing information at conferences, workshops and seminars, or in professional or trade publications, to avoid helping those intent on hostile reconnaissance
- be aware of the impact of data aggregation, both through accumulation and association, including the use of disparate sources
- recognise the persistent nature and accessibility of information published on the internet or otherwise made publicly available
- recognise that indiscriminate publication of project, technical or personal information can aid reconnaissance and enable security breaches through social media

- be aware of the use of social engineering[1] to manipulate individuals to give up confidential information
- ensure responsible use of social media use for both personal and professional purposes

5. Understand, comply and seek to improve lasting systems for security governance

Effective security requires good governance, with clear reporting lines and accountability at board or executive level. Engineers and technicians should:

- ensure that they, and those who work with them, understand the relevant security management policies, processes and procedures
- seek regular briefings on the security threats facing their organisation and understand how threat agents might exploit vulnerabilities in their customers/users and their own assets, systems or business processes
- ensure that security-related roles and responsibilities are clearly assigned and understood, irrespective of whether functions or services are outsourced
- ensure that there are appropriate mechanisms for reporting and feedback on security incidents and issues
- contribute to the development and review of relevant security management frameworks, particularly about aspects which may not be well understood

[1]Social engineering: www.cpni.gov.uk/advice/Personnel-security1/Social-engineering-Understanding-the-threat/

- scrutinise the security culture and responses to management systems, with audits encompassing processes and technical and paper systems

6. Contribute to public and professional awareness of security

Engineers and technicians have an important role in raising awareness and understanding about security risk and benefit. They should:

- be prepared to engage in debate on security risks and benefits, especially in relation to new technologies and innovative developments
- be security-minded during public discussion
- recognise the social, political and economic implications of security risks and acknowledge these through appropriate channels
- be honest and clear about uncertainties, and prepared to challenge misrepresentations and misconceptions
- contribute to public and professional awareness of security by sharing and promoting knowledge of effective solutions

The Engineering Council welcomes comments on this guidance which will be reviewed periodically.

Further information:

Engineering Council

UK-SPEC www.engc.org.uk/ukspec

ICT Technician Standard www.engc.org.uk/icttech

Guidance on:

Security www.engc.org.uk/security

Risk www.engc.org.uk/risk

Whistleblowing www.engc.org.uk/whistleblowing

Centre for the Protection of National Infrastructure (CPNI)

www.cpni.gov.uk

CPNI Passport to Good Security

www.cpni.gov.uk/advice/Passport-to-Good-Security

HM Government

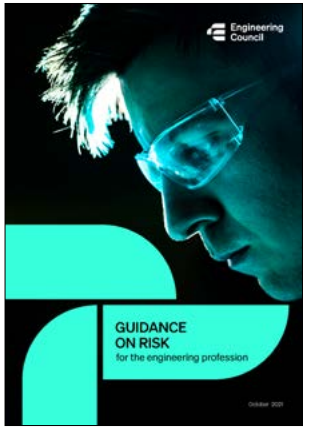
www.gov.uk/government/publications/cyber-essentials-scheme-overview

Register of Security Engineers and Specialists

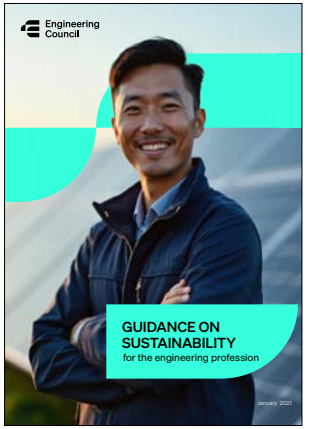
www.rses.org.uk

www.ice.org.uk/rses

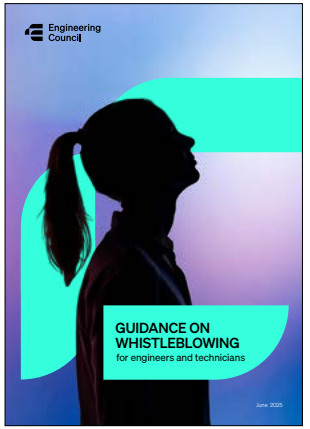
Other guidance we publish:



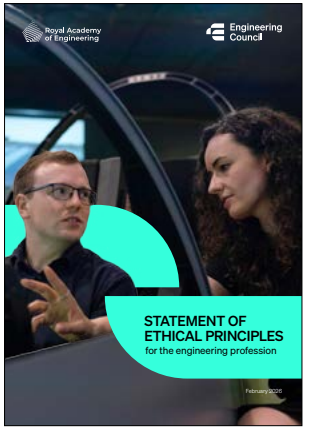
Risk



Sustainability



Whistleblowing



Ethical Principles

Engineering Council

+44 (0)20 3206 0500
info@engc.org.uk
engc.org.uk
Engineering Council
TheEngC
Engineering Council
theengineeringcouncil