



**CIOB**

THE CHARTERED INSTITUTE OF BUILDING

# THE ROLE OF SECURITY

IN THE CONSTRUCTION INDUSTRY



# FOREWORD

## THE SECURITY IMPERATIVE FOR THE CONSTRUCTION MANAGEMENT COMMUNITY



## INTRODUCTION

Security within the construction sector is becoming increasingly important. This is not just in terms of the physical controls and guarding, or security-minded behaviour by personnel, but also in respect of how we manage risks arising from unauthorised access to, and manipulation or sharing of, data, information and systems. The consequences of poor security should not be underestimated and could affect project financial margins, the construction programme, business reputation, the built asset itself and, worst of all, the lives of personnel.

As a result of an increasing awareness of these issues, security has become a key theme in the CIOB Digital Special Interest Group [SIG]. This guidance has been produced in order to help members [and their supply chains] understand the principles of good security planning, and to design appropriate and proportionate mitigation measures for construction projects.

Understanding the security risk profile and conducting effective planning for appropriate and holistic project security [encompassing personnel, physical and cyber security] is therefore essential and will help in enabling a safe and productive construction environment.

**David Philp** FCIQB  
Global BIM Consultancy Director AECOM, CIOB Trustee

# THE ROLE OF SECURITY IN THE CONSTRUCTION INDUSTRY

## SECURITY

Construction managers should be able demonstrate engagement with the built environment, a commitment to ethical working and promotion of a culture of continual improvement. In addition, they should be able to show that they are aware of their responsibilities to the public and other third parties by taking into consideration, at all times, the security of:



### PEOPLE

The people around them



### ASSETS

The built assets they are working on, in and/or have access to



### SERVICES

The services delivered from those built assets



### DATA

The data and information that they hold and/or have access to

A built asset is defined as a building, multiple buildings (e.g. on a site or campus), a portfolio or network of assets, built infrastructure (e.g. roads, railways, pipelines, dams, docks, etc.), or public space. It may also include associated land or water.

---

*Security can be defined as the state of relative freedom from threat or harm caused by deliberate, unwanted, hostile or malicious acts.*

---

At its highest level, security includes national security issues. For example, protection against terrorism, tackling organised crime and detecting hostile acts by nation states. However, it also encompasses preserving the value, longevity and ongoing use of an enterprise's assets, whether tangible - a built or other physical asset - or intangible - intellectual property and nationally or commercially sensitive data and information. In addition, it includes the handling of privacy issues such as the protection of personal data.



Security can be compromised by individuals through lack of knowledge, carelessness, complacency and deliberate non-compliance. Therefore, in addition to physical and technological aspects, personnel considerations are essential. Construction managers need to be aware of the potential impact of the way in which they discharge their professional duties, including the sharing data and information, both within the work environment and on social media. They should also be proactive in using processes and technology appropriate to the sensitivity of the work or activity being undertaken, as well as encouraging and supporting good security behaviours in other staff.

Further, a construction manager should appreciate that the way they undertake their role impacts not only on the security of the construction activity taking place, but on the security of the completed built asset and therefore the personnel using it and the services delivered from or by it, as well as the project and asset data and information.

Whether working towards Building Information Modelling [BIM Level 2] compliance or not, members are encouraged to follow **PAS 1192-5**, a specification for security-minded building information modelling, digital built environments and smart asset management.



Security-mindedness is defined as the understanding and routine application of appropriate and proportionate security measures in any business situation so as to deter and/or disrupt hostile, malicious, fraudulent and criminal behaviours or activities.



## CONSTRUCTION MANAGER:

### A CONSCIOUS SECURITY MINDSET

---

*A construction manager is expected to be able to demonstrate their understanding of, and ability in, identifying, assessing, implementing, managing and communicating issues about security through the six principles set out overleaf.*

---

The six principles are based on those developed by the Engineering Council tailored, where necessary, to be more relevant to the construction profession.



## PRINCIPLE ONE

ADOPT A SECURITY-MINDED APPROACH TO YOUR PROFESSIONAL AND PERSONAL LIFE

- Demonstrate an awareness of how behaviour and actions, including use of social media, can impact on their personnel security and that of others
- Identify potential threats and security vulnerabilities that exist at each stage of the construction process, suggesting potential measures to mitigate unacceptable risks
- Appreciate how exploitation of a vulnerability may result in harm to people, a built asset, services or data / information
- Understand the importance of implementing a combination of physical, personnel and technological mitigation measures to address security risks
- Demonstrate appropriate use of social media professionally and socially
- Identify and oversee the implementation of security policies and processes appropriate to the construction phase

## PRINCIPLE TWO

APPLY RESPONSIBLE JUDGEMENT AND TAKE A LEADERSHIP ROLE

- Demonstrate working with other professionals to ensure informed, proportionate, holistic judgements
- Demonstrate use of professional judgement in assessing security risks within a construction project
- Able to challenge assumptions and proposals while seeking to improve practices, and empower others to do the same
- Provide staff with the opportunity to maintain appropriate levels of security competence





## PRINCIPLE THREE

COMPLY WITH LEGISLATION AND CODES, UNDERSTAND THEIR INTENT AND BE PREPARED TO SEEK FURTHER IMPROVEMENTS

- Aware of security-related laws in countries where they operate
- Aware of, and acts in accordance with, security-related codes of practice relevant to construction activities
- Able to identify the role of existing security guidance recognising any limitations in respect of construction, and suggest improvements where reasonably practicable

## PRINCIPLE FOUR

ENSURE GOOD SECURITY-MINDED COMMUNICATIONS

- Able to identify the security policies and processes relevant to staff and other members of the supply chain, and communicate them clearly and effectively
- Able to express clearly the balance of security risks and opportunities
- Adopt an 'open reporting' approach to security risks, incidents and near-misses, coupled with a spirit of questioning and learning from others
- Selective of the material used when publishing information at conferences, workshops and seminars or when writing in professional or trade publications to avoid releasing sensitive data and information





## PRINCIPLE FIVE

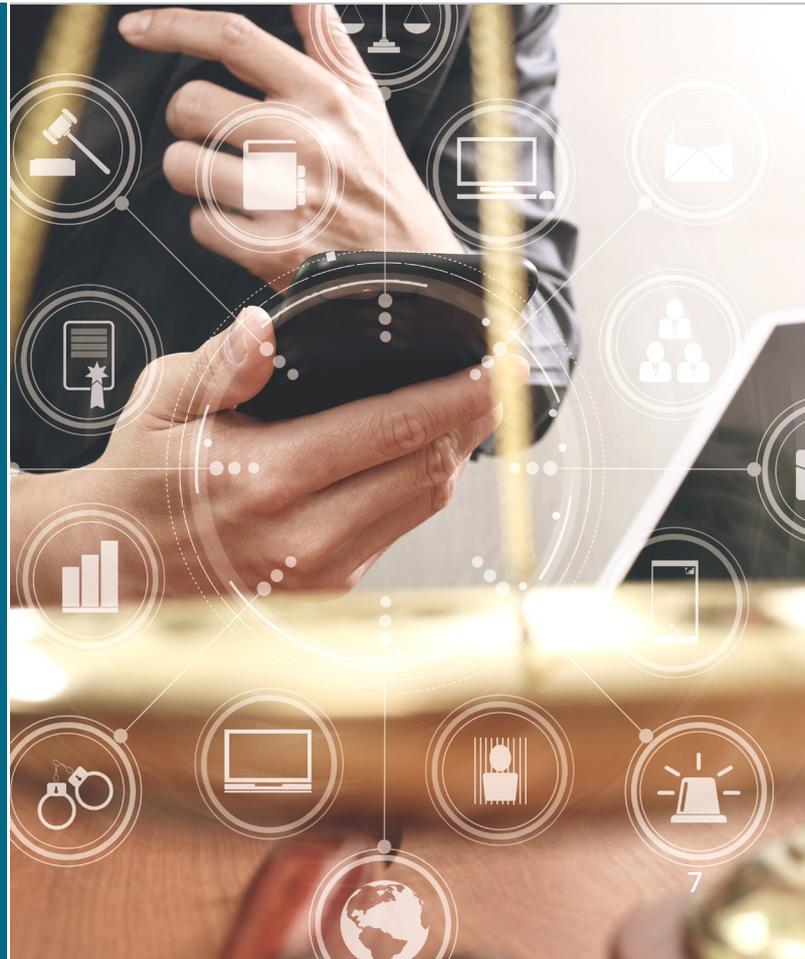
UNDERSTAND, COMPLY WITH AND SEEK TO IMPROVE LASTING SYSTEMS FOR SECURITY GOVERNANCE

- Demonstrate understanding of own role in contributing to the security of the built asset
- Contribute to the development, implementation and review of security policies and processes
- Ensure security-related roles and responsibilities are clearly assigned and understood by staff and members of the supply chain
- Improve own understanding of security risks and mitigation measures that can be applied during construction
- Contribute to the development and implementation of appropriate mechanisms for reporting and feedback on security incidents and issues
- Contribute to the scrutiny and auditing of the security culture and implementation of security policies and processes

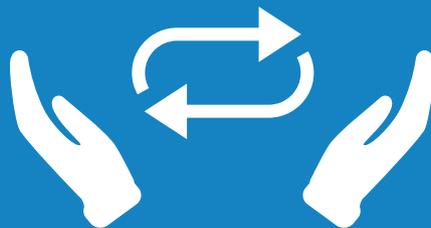
## PRINCIPLE SIX

CONTRIBUTE TO PUBLIC AND PROFESSIONAL AWARENESS OF SECURITY

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



# SECURITY COMPLIANCE



Examples  
of how you can demonstrate compliance  
with this Security Framework  
are set out in the section overleaf.



# GOVERNANCE

## Client requirements

- Make yourself familiar with any client security requirements set out in project contractual documentation
- Comply with the security requirements in place and report where any improvements could be made
- Communicate client security requirements to your staff and ensure that they also understand and comply with them
- Report any security breaches or incidents, including near-misses, as well as any issues that you feel may not be being addressed or addressed adequately. Empower your staff to do the same
- Check models, plans, images, data and information before sending them to any third party to make sure that they do not contain anything sensitive, including metadata, that should not be shared – be aware that once something has been released on the internet or otherwise made publicly available it is virtually impossible to delete, destroy, remove or secure all copies
- Consider what information and images are used in presentations, technical papers and marketing material



## Good basic security

- Familiarise yourself with any legal requirements to protect data and information in any countries where you operate
- Develop and maintain your understanding of security vulnerabilities that exist within construction activities and the methods that can be used to reduce the risks that result
- Watch out for, and report any suspicious behaviour you notice on or around company premises or your construction sites
- Include good security practices in staff inductions and training
- Ensure staff know what to do in the event of a security breach or incident, including a near-miss
- Ensure procedures for demobilisation of your staff are followed

# PERSONNEL

## ○ Your behaviour

- Social Media
  - Do not put information on social media that allows the projects you are working on to be identified
  - Do not post photographs taken on your site on social media, especially if geotagging is not turned off on your device
  - Consider what information you put onto LinkedIn or similar professional networking sites, for example, avoid putting details of systems that you work with, especially any systems relating to safety and/or security
  - Know what your digital footprint looks like and actively manage it – this includes making sure that others (such as friends and family members) know your views and what it is appropriate to publish
- Understand whether you are in a position that makes you more likely to be the target of social engineering or external influence/pressure

For more information see: [www.cpni.gov.uk/my-digital-footprint](http://www.cpni.gov.uk/my-digital-footprint)



## PHYSICAL

### ○ Client requirements

- Manage the logistics of installing sensitive assets within a built asset so that, whenever possible, these assets can be fitted late in the project when the majority of contractors no longer need access to the site
- Monitor the implementation of, and compliance with, any physical security measures in place and be prepared to challenge and/or report breaches and near-misses
- Ensure secure storage and destruction of physical plans and digital media

For more information see:  
<https://www.cpni.gov.uk/physical-security>





# TECHNOLOGICAL

## At home

### FIREWALLS

Protect your home internet connection by using a firewall

- Ensure any firewall included within your operating system is turned on
- If you are connecting several devices to the internet, check whether your router has a firewall and whether it is activated

### SETTINGS AND PASSWORDS

Increase security on your devices and the software installed on them

- Check settings when you purchase new software and devices and, where possible, alter the default settings to increase security
- Protect your router, devices and accounts with passwords – this includes changing default passwords
- Take the opportunity to use two-factor authentication on your most important accounts – for example, banking

### ACCESS TO YOUR DEVICES

Consider who has access to your devices

- Check whether different accounts have administrative privileges that would enable downloading and installation of software

### MALWARE AND VIRUSES

Protect against malware and viruses

- Install and maintain antivirus software
- Only download apps for mobile phones and tablets from manufacturer-approved stores (for example, Google Play and Apple App Store)

### KEEP DEVICES AND SOFTWARE UP-TO-DATE

- Set operating systems, software, devices and apps to automatically update

For more information, visit the Cyber Essentials page at:  
[www.ncsc.gov.uk](http://www.ncsc.gov.uk)





## TECHNOLOGICAL (Cont.)

### At work

- Do not use work devices for sending/receiving personal e-mails
- Avoid using personal devices for undertaking work and do not transfer files from a personal device to a work one
- Report phishing e-mails and do not open links and attachments contained in them or any other e-mail that you believe may not be genuine
- Do not open unknown files on removable storage media, such as a USB memory stick
- Lock devices when you leave them unattended, especially when they hold or have access to sensitive information

This document has been produced under guidance from the UK government's Centre for the Protection of National Infrastructure (CPNI). For more detailed information on security issues and mitigation measures, members are directed to [www.cpni.gov.uk](http://www.cpni.gov.uk)



# YOUR SECURITY FRAMEWORK COMPLIANCE CHECKLIST (1)



*This framework can be used to help you build a security-minded approach to your project either during the mobilisation or as a health check on a live-project.*

## GOVERNANCE

Requirement	<input checked="" type="checkbox"/>	Your Comments
Has the client set out any security requirements?	<input type="checkbox"/>	
Does your organisation have any security requirements in relation to the project?	<input type="checkbox"/>	
Are there legal requirements to protect data and information in the country in which you are working?	<input type="checkbox"/>	
If so, have staff been made aware of any additional security requirements?	<input type="checkbox"/>	
Are security inductions and training in place to communicate security requirements to staff and the supply chain?	<input type="checkbox"/>	
Is monitoring and auditing of the implementation of the security requirements scheduled and undertaken?	<input type="checkbox"/>	
Is there a process in place for the reporting of security breaches and incidents?	<input type="checkbox"/>	
Has this process been communicated to staff and the supply chain?	<input type="checkbox"/>	
Is there a process in place for checking data and information for sensitivities before it is sent to, or viewed by, third parties?	<input type="checkbox"/>	
Has this process been communicated to staff and the supply chain?	<input type="checkbox"/>	
Is there a process in place for the demobilisation of staff and organisations working on the project?	<input type="checkbox"/>	
Have checks been carried out to ensure this process is being followed?	<input type="checkbox"/>	

# YOUR SECURITY FRAMEWORK COMPLIANCE CHECKLIST (2)



*This framework can be used to help you build a security-minded approach to your project either during the mobilisation or as a health check on a live-project.*

## PERSONNEL

Requirement	<input checked="" type="checkbox"/>	Your Comments
Has a policy relating to the placing of work-related information and images on social media been developed?	<input type="checkbox"/>	
Has this policy been communicated to staff and the supply chain?	<input type="checkbox"/>	
Have checks been carried out to ensure this policy is being followed?	<input type="checkbox"/>	
Has guidance been provided to staff on actively managing their individual digital footprint?	<input type="checkbox"/>	
Have high-risk positions on the project been identified (these positions are those that are likely to be the target of social engineering or external influence/pressure)?	<input type="checkbox"/>	

## PHYSICAL

Requirement	<input checked="" type="checkbox"/>	Your Comments
Have physical security measures been implemented on site?	<input type="checkbox"/>	
Is compliance with physical security measures being monitored?	<input type="checkbox"/>	
Has a policy relating to receiving personal deliveries at work been put in place?	<input type="checkbox"/>	
Has this policy been communicated to staff?	<input type="checkbox"/>	
Have checks been carried out to ensure this policy is being followed?	<input type="checkbox"/>	

# YOUR SECURITY FRAMEWORK COMPLIANCE CHECKLIST (3)



*This framework can be used to help you build a security-minded approach to your project either during the mobilisation or as a health check on a live-project.*

TECHNOLOGICAL / CYBER		
Requirement	<input checked="" type="checkbox"/>	Your Comments
Has a policy relating to the use of work devices for sending/receiving personal e-mails been developed?	<input type="checkbox"/>	
Has this policy been communicated to staff?	<input type="checkbox"/>	
Has a policy relating to the gathering, processing and storing of work-related data and information on personal devices been developed?	<input type="checkbox"/>	
Has this policy been communicated to staff?	<input type="checkbox"/>	
Is there a policy relating to the use of removable storage media?	<input type="checkbox"/>	
Has this policy been communicated to staff?	<input type="checkbox"/>	
Is there a process for reporting and handling phishing e-mails?	<input type="checkbox"/>	
Has this process been communicated to staff?	<input type="checkbox"/>	

# MINDFUL SECURITY FOR CONSTRUCTION MANAGERS

## Be security **conscious**

- Understand your security role and responsibility
- Be aware of your security obligations to the project and its stakeholders
- Think holistically about security: personnel; physical and cyber security

## Understand the impact of your **behaviours**

- Understand the vulnerabilities and security risks relevant to your project and the impact that a security breach or incident could have
- Understand how your behaviours can increase or decrease the likelihood of security breach or incident



## Encourage and support good security behaviours

- Lead by example
- Include security in all inductions
- Carry out security briefings
- Include security in performance reviews
- Encourage reporting of potential security issues

## Be **proactive** with security

- Assess the security risks to your project
- Create appropriate and proportionate mitigation measures encompassing personnel, physical and cyber security. Develop a formal security strategy and management plan
- Implement and monitor mitigation measures
- Create a site environment that supports a security-minded culture
- Only gather, process and store data and information using approved devices and systems



# CIOB

THE CHARTERED INSTITUTE OF BUILDING

The Chartered Institute of Building,  
1 Arlington Square,  
Downshire Way,  
Bracknell,  
RG12 1WA, UK  
Tel: +44 (0) 1344 630 700

Registered Charity No. (England and Wales) 280795 and (Scotland) SC041725  
CIOB 227/0715



Copyright CIOB 2018