National Protective Security Authority

Guidance for Security Managers

A framework for UK Critical National Infrastructure organisations on security savvy employee behaviour

Contents

Introduction

The purpose of this document is to provide a framework that outlines what **good employee security practice looks like** in UK Critical National Infrastructure organisations, where the behaviour of employees can be critical to keeping sensitive organisational assets safe and secure.

The document provides a summary of the research conducted by NPSA to identify examples of effective and ineffective security behaviour for UK Critical National Infrastructure organisations.

The aim of the framework is to assist **security professionals** within these organisations with identifying the target behaviours that they require from their employees that can be embedded in the organisation's security culture to reduce its vulnerability to terrorism, espionage and other threats. It is envisaged that the framework be used in a range of ways. For example:

- to assist an organisation with the development of personnel security policies;
- to guide the development of communications materials to help shape employee attitudes and beliefs;
- to support the development of behavioural indicators that measure personnel security performance in the workplace.

Why the framework was developed

Employee behaviour, and embedding the right behaviours, is central to the achievement of protecting UK Critical National Infrastructure from terrorism, espionage and other threats. Physical and cyber (or information) security measures can only go so far in mitigating these threats. Most of these measures rely on employees behaving in the right way in order to optimise their protective security capabilities. In addition, employees can act as a protective measure in their own right, playing a significant role in the detection, deterrence and prevention of potential security threats.

For these reasons, the development of an **appropriate security culture** within UK Critical National Infrastructure organisations, where the right security behaviours are adopted as a matter of course by the workforce, is an essential component to their protective security regime. It is also something that can be achieved at a relatively low cost in comparison to other physical and technical measures. However, building a good security culture and embedding the right security behaviours can be complex. There are a number of elements that need to be taken into account. For example:

- Understanding the level of risk facing the organisation (and its sensitive assets) from threat actors;
- Understanding the organisation's risk appetite for security in relation to its other strategic objectives (e.g. service delivery, sales, profits);
- Identifying what protective security measures are appropriate and proportionate to put in place;
- Recognising the role that human factors can play in mitigating the threat, in addition to physical and cyber (information) measures;
- Defining the behaviours that the organisation requires the workforce to adopt in order to help mitigate risk;
- Ensuring there is a culture in place that encourages and enables the demonstration of these behaviours rather than undermines or contradicts them.

This framework was developed to help address the penultimate bullet point – to assist organisations with ***defining the behaviours that the organisation requires the workforce to adopt in order to help mitigate the risk***. The framework was developed as a result of a research project conducted by NPSA with a selection of UK Critical National Infrastructure organisations. The research identified consistencies in the security behaviours these organisations would like their workforce to demonstrate to help keep them and their sensitive assets safe and secure. This document provides a summary of these behaviours to help other organisations consider whether the same behaviours are required from their employees.

Overview of the framework

The framework is designed to assist organisations with **identifying the target behaviours** that they require from their employees that can be embedded in the organisation's day-to-day working practices in order to reduce its vulnerability to terrorism, espionage and other threats. The framework is divided into the following 10 sections:

1. Understanding security
2. Entering and leaving secure sites (or when easily identifiable as a member of the organisation)
3. In and around the workplace
4. Managing visitors
5. Using corporate IT
6. Representing your organisation online
7. Handling queries from customers, suppliers, partners or the public
8. Living life outside of work
9. Being a security advocate as a line manager [for management only – in addition to the above behaviours]
10. Being a security advocate as a senior manager [for senior managers only – in addition to the above behaviours]

How to use the framework

A key component in developing a strong organisational security culture is ensuring the target security behaviours expected from the workforce are clearly **defined and articulated.** Without this, employees may be unclear about precisely what it is they are meant to be doing in order to keep the organisational assets safe and secure.

Traditionally, good security practice has tended to be associated with employees demonstrating security savvy behaviours within the workplace (e.g. clear desk policy, escorting visitors in sensitive work areas, shredding of sensitive information, locking computer terminals when away from desks). However, in today's society, as a result of changes in working practices and technology, good security practice has become much broader than this. It now includes how employees behave when working remotely (e.g. travelling between destinations or working from home) as well as what they do when using digital devices, social media sites and the internet that link them to their place of work. Without adopting some common-sense, effective security behaviours, employees may be inadvertently making themselves, their colleagues and their organisation more vulnerable to security threats and risks.

This framework serves as a **guide to organisations** to help define what good security behaviour looks like today. In using the framework, there are two key points to bear in mind:

1. **It is not a definitive or exhaustive list.** Whilst it aims to be a reliable and valid framework, based on a cross section of views and perspectives from a range of employees across CNI organisations, there may be additional behaviours that are relevant. In addition, over time new or amended behaviours may be required as working practices, technology and threats change.
2. **Different organisations may require different target behaviours to those listed here.** This will depend on the assets that need protecting, the security threats facing the organisation, and other strategic requirements that demand employees' time and attention. It is also possible that different teams, departments and/or sites within organisations will require different security behaviours (e.g. one team may require visitors to be escorted at all times due to the nature of their work whereas another team may be comfortable for visitors to move around the work area freely).

It is important for organisations to consider this framework in light of their own needs and requirements and to develop their target behaviours accordingly. This framework has been developed to support organisations with this process and should be used as a helpful guide rather than a best practice list.

Finally, please bear in mind that defining and communicating the security behaviours expected of employees alone will not result in employees automatically demonstrating these. Human behaviour is a complex phenomenon influenced by a number of factors. Some of these factors are linked to the beliefs and attitudes held by employees about security (Ajzen, 2005)[1]. Others are linked to environmental

[1]Ajzen, I (2005). Attitudes, personality, and behaviour (2nd edition). Milton-Keynes, England: Open University Press / McGraw-Hill.
[2]CAS Management Model (2008). Culture Management in the UK Rail Industry. Safety System International 2008 Conference.

factors such as perceived social pressure to perform the behaviour (e.g. senior management endorsement) and perceived ease of performing the behaviour (e.g. having the time, resources, and confidence to do so)[2].

Therefore, the **wider context and security culture within which employees operate** will also need to be taken into account, such as the extent to which the organisational processes, system and practices help employees to demonstrate the target security behaviours.

Security behaviours framework for employees

1. Understanding security

Example effective behavioural indicators:	Example ineffective behavioural indicators:
✓ Can identify the types of sensitive assets that the organisation holds that need to be protected (e.g. data, people, equipment, chemicals, materials, internal systems or processes, designs, research, money, intellectual property, intelligence, information about staff members)	× Cannot differentiate sensitive assets from those that are not sensitive
✓ Can describe a range of ways in which sensitive assets can be compromised either deliberately or accidentally (e.g. theft, sabotage, cyber-attack, information leaks, accidental loss of items, or social engineering / manipulation of staff by either internal staff members or external attackers)	× Can highlight few ways in which sensitive assets can be compromised or is naïve to some of the more sophisticated threats such as social engineering of cyber-attack through malware
✓ Can articulate the potential consequences that could occur to employees, organisations, and/or the public should sensitive assets be compromised, such as by organised criminals, protest groups, terrorists, or state actors	× Cannot articulate many consequences that could occur should an asset be compromised, struggling to appreciate the broader implications to others or wider wellbeing or security issues

2. Entering and leaving secure sites (or when easily identifiable as a member of the organisation)

Example effective behavioural indicators:	Example ineffective behavioural indicators:
✓ Looks alert and vigilant when entering or leaving sites, or when out and about and clearly identifiable as a member of their organisation such as in uniform	× Looks distracted or unaware of their surroundings at the entry and exit points of a site such as by using a mobile phone or other digital device, reading papers, or wearing headphones
✓ Reports anything unusual or suspicious immediately to the security department following the correct procedures (e.g. reporting hotlines, informing a security guard)	× Ignores or misses suspicious activity near their workplace or does not use the correct reporting procedures
✓ Moves swiftly through entry and exit points and takes steps not to make their links to a site obvious (e.g. varies times with which they use entry and exit points or orders taxis to a nearby location rather than the site itself)	× Draws unnecessary attention to themselves and their place of work (e.g. smokes or loiters near site entry and exit points)
✓ Follows the correct entry and exit procedures for passing through site gates, vehicle barriers, doors and so forth (e.g. swiping in and out)	× Ignores or disregards the correct entry and exit procedures (e.g. does not swipe in or out, or facilitates tailgating)

3. In and around the workplace

Example effective behavioural indicators:	Example ineffective behavioural indicators:
✓ Wears their correct security pass in the workplace, ensuring it is clearly visible	× Obscures or hides their pass while onsite (e.g. in a pocket or behind a jacket)
✓ Reminds others to wear the correct pass as appropriate and acknowledges those who do the same for them	× Overlooks, or feels embarrassed to remind or nudge, those who are not following the correct pass procedure, or takes offence if others remind them
✓ Discusses sensitive projects or information in the appropriate location, such as a meeting room, with only those who need to be present	× Discusses sensitive projects or displays sensitive information in insecure areas (e.g. corridors, lifts, coffee areas, or when escorting visitors to / from reception)
✓ Disposes of sensitive information appropriately (e.g. uses a shredder for paper documents)	× Throws away sensitive documents carelessly without shredding
✓ Ensures their desk and printer(s) are clear of any sensitive information at the end of the working day, where necessary locking it away	× Leaves sensitive papers or information out on their desk or on printers at the end of the working day
✓ Allocates sufficient time to adhere to security policy when transferring sensitive information electronically or physically	× Bypasses the security policy in place when transferring information electronically or physically to meet a deadline or achieve an outcome
✓ Reports any lost organisational items immediately, such as laptops, phones or papers	× Delays on reporting a lost item, hoping it will turn up or thinking that it won't matter if a report is delayed by a few days
✓ Raises any concerning or unauthorised security behaviour they witness in the workplace through an appropriate mechanism, such as a confidential hotline or to their line manager	× Ignores any concerning or unauthorised security behaviour they see in the workplace, hoping it isn't a serious issue or that others will take the lead instead of them
✓ Shares sensitive information with others in line with organisational policy	× Makes assumptions about what information can and can't be shared with others without checking the policy or with the information owner
✓ Conducts work offsite in line with good security practice, such as when travelling to or from a site or when working from home	× Disregards the security practices when working offsite such as when in public places or working from home
✓ Leads by example, demonstrating good security practice in front of colleagues, visitors and the public	× Ignores good security practice or carries it out to the minimum standard required, giving the impression they, and the organisation, have a relaxed approach to security

4. Managing visitors

Example effective behavioural indicators:	Example ineffective behavioural indicators:
✓ Follows the visitor sign-in and sign-out process so reception staff know who to expect and when, in line with organisational policy	× Bypasses the visitor sign-in process or assumes reception don't need to know who is arriving and when
✓ Verifies who their visitors are and ensures any relevant identity and clearance checks are made in advance of sensitive meetings or discussions	× Allows visitors that have not received a precautionary identity or clearance check into sensitive meetings or discussions
✓ Checks visitors are wearing the appropriate pass when on site and ensures they return these when they leave	× Allows their visitors onsite without an appropriate pass or lets them take their passes with them when they leave, rather than returning these to security or reception
✓ Briefs visitors on any relevant security procedures as a matter of courtesy (e.g. policy on escorting visitors and bringing in their own electronic devices)	× Forgets or ignores the need to prepare or adequately brief their visitors on any relevant security procedures
✓ Shows consideration for colleagues when hosting visitors, keeping them away from sensitive work areas	× Takes short-cuts with visitors through unauthorised or sensitive work areas which can make colleagues feel uncomfortable
✓ Takes accountability for the security behaviour and conduct of their visitors when on site	× Assumes the security behaviour of their visitors is the responsibility of others such as the security guards or other colleagues

5. Using corporate IT

Example effective behavioural indicators:	Example ineffective behavioural indicators:
✓ Locks their devices or computer terminal when leaving them unattended	× Leaves their devices and terminals unlocked when they are unattended for long periods of time
✓ Waits until requested by Information (or IT) Services to upgrade their devices or install new software	× Installs applications onto work devices without the prior consent of Information (or IT) Services
✓ Keeps passwords separate from the devices themselves (e.g. keeps them in a coded form in a separate location)	× Stores passwords with an associated device, making it easy for unauthorised others to access these
✓ Connects only sanctioned devices and media to corporate IT systems such as authorised laptops, USB sticks, CDs and phones	× Connects unauthorised IT devices and media, such as personal USB sticks or mobile phones, to the corporate systems without going through the proper channels
✓ Keeps a record of the organisational devices, phones and media in their possession and where they are	× Mislays or loses track of what organisational devices, phones and media they have been authorised to use and where these are
✓ Stores only the essential information that is needed on portable devices and mobile phones, routinely deleting redundant data in case it is mislaid or stolen	× Keeps or transfers unnecessary information on portable devices or mobile phones, forgetting to routinely delete redundant data
✓ Uses work devices and email addresses only for work related reasons	× Uses work devices and email addresses for personal use, failing to appreciate the security risks this may pose to them, their contacts and the organisation
✓ Adheres to good information management practice and policy by ensuring all work related documents are stored appropriately on the corporate IT system	× Develops their own personal information management system or forgets to store work related documents on the corporate system so there is no audit trail for others to follow
✓ Uses IT systems and devices appropriately and in line with organisational policy (e.g. internet searches, social media sites)	× Misunderstands or ignores how to use different IT systems and devices in line with policy (e.g. uses social media sites on a corporate system that they are not permitted to use)
✓ Avoids using public Wi-Fi on corporate IT devices whenever possible	× Connects corporate devices to public Wi-Fi as a matter of routine

6. Representing your organisation online

Example effective behavioural indicators:	Example ineffective behavioural indicators:
✓ Gains organisational approval before blogging or publishing information online as a representative of the organisation	× Starts blogging or publishing information online as a representative of the organisation without their formal consent
✓ Involves the security department in reviewing potentially sensitive information being made publically available online (e.g. websites, blogs, social media) to ensure appropriate security actions and mitigations have been taken	× Publishes articles, adverts, blogs or social media comments that may reveal sensitive information about the organisation without running it past security (or other key stakeholders) first
✓ Gives the organisational position or response when making comments online rather than their personal view or response	× Gets drawn into giving their personal view on an issue or shares an opinion that has been not been sanctioned by the organisation
✓ Adheres to the same values and codes of practice online that apply offline (e.g. respect for others; organisational codes of conduct; justice and fairness)	× Deviates outside the boundaries of what is deemed acceptable behaviour when online (e.g. is rude or disrespectful to others; ignores organisational codes of conduct)
✓ Demonstrates maturity in terms of what they publish online, limiting the information to things where there are minimal (or no) security risks or the information is already in the public domain	× Shows naivety about the security risks online, publishing information without due consideration to the security implications (e.g. assumes that information shared online will remain just with the intended recipients)
✓ Considers the security implications associated with increasing their online work profile, and takes appropriate mitigating actions in relation to their personal profile (e.g. diminishes their personal digital footprint such as by tightening security settings on personal social media sites or removing personal details online)	× Takes a passive stance in relation to their own digital profile when raising their online work profile, failing to consider the security implications this might have for them or their family (e.g. continues to have extensive personal details online about themselves that are easy for anyone to see)

7. Handling queries from customers, suppliers, partners or the public

Example effective behavioural indicators:	Example ineffective behavioural indicators:
✓ Verifies the identity of customers, suppliers and partners before sharing information or undertaking work with them (e.g. requests photographic ID; seeks written confirmation on new contacts to external projects; double checks who unfamiliar faces are with trusted contacts)	× Takes customers, suppliers and partners at face value without checking their legitimacy or credentials
✓ Shares sensitive information only with external contacts who are authorised to receive this	× Passes on sensitive information to external contacts who are not authorised to receive the information or trained in how to handle it appropriately
✓ Refrains from sharing unnecessary or sensitive information with others, such as industry partners, suppliers, customers and the public, where they do not need to know it or are not authorised to receive it (e.g. full staff names, details about sensitive projects)	× Assumes any information can be shared with trusted contacts rather than checking first what is appropriate to share, or is overly helpful to others without realising the information they are giving could jeopardise the security of an employee or piece of work
✓ Identifies what the social engineering threat could be in relation to their work and is vigilant to what a potential approach might look like (e.g. phishing emails, bogus telephone calls, approaches by individuals with an unusual interest in their work)	× Gets complacent or is naïve about the social engineering threat or ways in which they could be manipulated to share certain information with those with malicious intent
✓ Develops tactics to handle queries from external contacts politely without revealing sensitive information (e.g. provides generic descriptions such as “we have offices all over the country” rather than detailing specifics or “Tell me more about your query and I’ll ask the relevant person to get back to you” rather than sharing employee names)	× Gives away too much information when requested by an external party (e.g. “Chris Smith doesn’t work in Finance but Greg Smith does - shall I put you through to him?”)
✓ Takes the time to double check whether certain information can or can’t be shared with others if they are unsure (e.g. offers to take someone’s details and to call them back in order that they can seek advice)	× Feels pressured to respond to a question immediately when “put on the spot”, rather than politely offering to get back to them with an answer

8. Living life outside of work

Example effective behavioural indicators:	Example ineffective behavioural indicators:
✓ Stays alert to the potential of a security threat relating to their work taking place in their personal life (e.g. in social situations and/or online)	× Assumes they won't be targeted by those with malicious intent in their personal life or takes the view "it wouldn't happen to me"
✓ Reveals minimal or no detail about sensitive aspects of their work in social situations or online (e.g. avoids blogging about work related activities)	× Draws attention to sensitive aspects of their work (e.g. references sensitive projects in social situations or on social media sites; joins online groups that identify them as having SC or DV clearances; openly links themselves to the work of sensitive organisations)
✓ Uses social media sites responsibly and shares information that does not compromise the reputation or security of the organisation	× Posts inappropriate information online that risks causing reputational or security related damage to their organisation (e.g. photographs of a work event or location data when conducting sensitive work)
✓ Sets their security settings on personal devices and social media sites high so as to reduce their vulnerability to threats (e.g. turns off geolocation on applications; only allows known contacts to view their posts)	× Assumes the default settings on their personal devices and social media sites will keep them secure. Fails to check the terms and conditions regarding data sharing on applications and social media sites
✓ Encourages friends and family not to share information about them or their work online that could make them or their organisation vulnerable	× Assumes others will know their preferences regarding what they are comfortable with being shared online, failing to let them know if they don't want certain information discussed openly
✓ Monitors and reviews their online digital footprint regularly to ensure they maintain a profile (and exposure) that they and their organisation feel comfortable with given the security threats they might face	× Adopts a passive approach to their digital footprint rather than actively managing and monitoring it
✓ Seeks advice on how best to describe careers in sensitive roles, such as on a CV, job application or social media profile, to promote their skills but not compromise security	× Gives detailed accounts of sensitive aspects of their work without seeking advice, such as when detailing their career history online, on CV's, on job application forms or to recruitment agencies
✓ Reports any suspicious or unusual incidents that occur outside of work, that make them feel uncomfortable, to their workplace	× Does not trust their instincts over suspicious or unusual incidents outside of work, failing to report these to their place of work

9. Being a security advocate as a line manager

Example effective behavioural indicators:	Example ineffective behavioural indicators:
✓ Recognises that ensuring staff (and contractors) adhere to good security practice is part of their line management responsibilities, alongside health and safety, welfare, and staff performance	× Views security as an 'add-on' to their line management responsibilities, only to be done when they have time rather than a duty of care
✓ Ensures staff (and contractors) are briefed on the potential security threats and risks they may face (e.g. invites security and other guest speakers to give briefings at team meetings to help with security education)	× Assumes staff know everything they need to about security; does little to help them to understand the value of the assets held by the organisation and the potential harm that could be caused if they got into the wrong hands
✓ Explains the security rules and guidelines to staff (and contractors) and checks everyone understands these correctly	× Leaves security briefings to the training team or the security department; fails to check that staff are clear on the security expectations of them
✓ Personalises security messages to make them meaningful for staff (and contractors) with tangible examples	× Briefs their employees on the security rules and procedures in an unengaging way
✓ Assesses the security knowledge levels of staff (and contractors) and provides additional training where required (e.g. on new security policy or when staff are provided access to new IT systems)	× Waits for staff to come to them with gaps in their security knowledge rather than proactively gauging and monitoring this themselves
✓ Encourages two-way conversations with staff (and contractors) about security, such as providing feedback and inviting discussion regarding practices and areas for improvement	× Gives minimal or no feedback to staff on the security aspects of their role or tells staff how to do security rather than involving them in discussions about how best to implement the practices
✓ Follows the appropriate procedures and protocols, should there be a security incident	× Follows their own advice rather than corporate advice regarding what to do should a security incident occur or a concern be raised with them
✓ Advises staff (and contractors) to be open with them about security errors or mistakes so they can address these together and for others to learn	× Expects their staff to be able to get security right all of the time rather than acknowledging that mistakes will happen
✓ Keeps note of the access rights of their staff (and contractors) for certain systems, sites and devices, closing down that access as they move roles	× Forgets which team members have access to which sites, systems or devices or allows staff (and contractors) to leave roles with continued access to privileged information that is no longer needed
✓ Evaluates the security risks appropriately when making decisions	× Ignores the security implications when making business decisions or has poor judgement regarding when to prioritise security over delivery
✓ Develops an environment where staff (and contractors) see good security practice as being part of their responsibilities	× Carries full responsibility for the security performance of their team, rather than encouraging personal ownership and responsibility
✓ Role models the standards of security behaviour they expect from their staff (and contractors)	× Trivialises or belittles security in front of their staff, giving the impression it is not important

10. Being a security advocate as a senior manager

Example effective behavioural indicators:	Example ineffective behavioural indicators:
✓ Keeps up-to-date on the security threats that face the organisation and wider industry (e.g. shares relevant security data with other leaders; reads current threat rProveports and updates)	× Assumes they are up-to-date on the current security threats and risks facing the organisation or does not see this as part of their senior management responsibilities
✓ Ensures there is accountability for personnel security at a senior level such as by nominating a senior risk owner	× Presumes security is the responsibility of others in the organisation and not senior management, failing to appreciate the impact this will have on the organisation's wider security culture
✓ Develops partnerships with security functions within the organisation to keep abreast of issues and updates and encourage collaborative working (e.g. National Security Vetting, IT security, physical security)	× Places little value on building good working relationships with the security functions within the organisation
✓ Keeps security in mind when making strategic decisions (e.g. asks questions on the security implications alongside questions on costs, timescales and deliverables)	× Overlooks the security implications when making strategic decisions; takes account of security as an afterthought
✓ Develops organisational systems, processes, structures and work spaces that support staff with demonstrating security behaviours and are proportionate to the threat (e.g. zone accessed areas for sensitive projects; not allowing staff to access personal social media sites on the corporate network)	× Develops organisational systems, processes, structures and work spaces that make security behaviours counterintuitive for employees to achieve, or are over engineered meaning that unnecessary security restrictions are in place that block effective delivery
✓ Monitors what sensitive organisational information and assets are stored by third parties, such as suppliers, and checks these are in line with required security standards (e.g. builds security KPIs into supplier contracts)	× Loses track of what sensitive organisational data is held by third parties and where; assumes third parties will have the appropriate secure systems and procedures in place
✓ Measures the security performance of the organisation regularly and ensures proportionate protective security mitigations are in place	× Assumes security in the organisation is up to standard without drawing on reliable, objective measures of performance
✓ Provides the strategic direction and leadership needed to instil a strong security culture in the organisation and develop a security savvy workforce	× Trusts that the right security culture already exists or will develop organically in time, rather than providing the direction required from the top