CPNI
Centre for the Protection
of National Infrastructure

MANAGERS: ARE YOU MANAGING SECURITY?

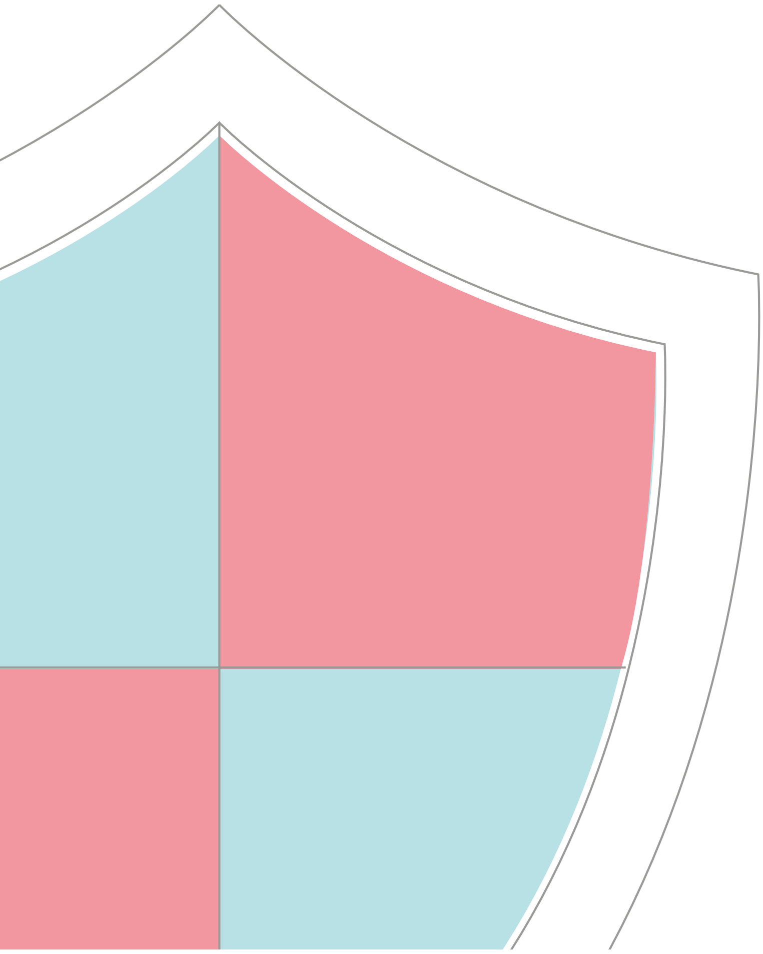
THE HOW-TO GUIDE

| CPNI SECURITY BEHAVIOUR CAMPAIGN: THE ROLE OF LINE MANAGEMENT

DISCLAIMER

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation or favour by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential, and including but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using the information contained in this document or its references. You should make your own judgment as regards use of this document and seek independent professional advice on your particular circumstances.



MANAGING SECURITY

As a line manager, do you consider organisational security to be part of your job?

What about informing your team about security matters, or keeping them updated on your organisation's security policy? Whose responsibility is that? What should you be doing?

This guide gives you practical advice on how to brief your team on being security-conscious and how to encourage them to think about security on a daily basis.

Promoting security in the workplace is important for all kinds of different reasons. From keeping sensitive organisational or product information away from the prying eyes of competitors, to maintaining your organisation's reputation by avoiding embarrassing security breaches, to keeping your workforce and/or the public protected from harm.

Potential security risks can come from several sources, for example:

A criminal | **A violent activist** | **A spy** | **A terrorist** | **A disaffected employee**

Individuals like these could cause harm to your organisation in a number of ways, such as by carrying out cyber-attacks, physical acts of theft or sabotage, or by manipulating employees to obtain information under false pretences.

This kit will help you to think about the kind of security behaviours you should expect from the people you manage, to help protect them and the organisation from security threats and risks. It also provides suggestions on how to develop a culture within your team where team members take responsibility for security, know what the correct security procedures are, and work together to keep organisational assets safe and secure.

YOUR RESPONSIBILITIES AND YOUR ROLE

AS A LINE MANAGER, THERE ARE FIVE KEY SECURITY RESPONSIBILITIES THAT WE'D ADVISE YOU TO ADOPT. THESE ARE AS FOLLOWS:

1. Understand the security threats and risks to your team

A range of organisational assets can potentially be a target for someone with malicious intent, for example, organisational materials, equipment, designs, intellectual property, intelligence, and even the workforce. What could happen if these assets fell into the wrong hands? What damage could be caused to your team, your organisation, your community or even the wider UK public? How aware are your team of the security threats and risks they face as part of their work? Could they even be a target of an attack that could result in them coming to harm?

If you're not clear yourself on what the security threats and risks are to your team and/or organisation then you'll struggle to explain to the people you manage why security matters and why it's important for them to act in a security-conscious way.

Your role

You should be familiar with the security threats to your organisation (and specifically to your team) and know these well enough to explain them clearly to your employees. You also should be absolutely clear on what security-conscious behaviour means and what you expect. Speak to IT, HR, security and anyone else in the organisation with a specific security interest to keep yourself up-to-date on the threats, and to make sure you're clear on the latest policy and procedures and why these matter.

2. Know how your team needs to behave to keep themselves and the organisation secure

Do you know what security behaviours your team should be demonstrating in order to keep themselves and the organisation safe and secure? Are you clear on your expectations of employees in relation to security?

If you could get each of your team members to change one habit, in order to keep them and the organisation more safe and secure, what would it be? Wearing their passes at all times when they are in the office? Not leaving sensitive information out on printers or photocopiers? Or perhaps it's ensuring they are being sensible in how they talk about the sensitive nature of their work online?

Your role

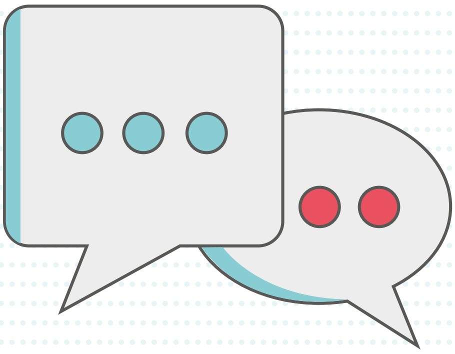
Make sure you know what your organisational security policy is and how this relates to the work of your team. This will help you to:

a. Brief your team clearly and consistently on how you expect them to behave to minimise the risk of security vulnerabilities

b. Identify areas where the team are adhering to the policy well and areas where they may be making mistakes

c. Answer any questions they may have about the security policy and procedures with confidence and credibility

Ultimately, unless you are clear on what you expect from the people you manage, they will not be clear on what they should be doing in order to behave securely.



3. Gauge current levels of awareness and security knowledge

Have you checked that your team knows your organisation's security policy? Is security policy training a standard part of your induction procedure for new starters, and is training up to scratch? Who should be in charge of carrying out that training – is it your security team, your HR department, or is it you?

Your role

Get feedback from your team about what they know and what they do not know about security policy. Find out where the knowledge gaps lie and evaluate what can be done within your team to plug them. Also, encourage staff to learn from their mistakes by being open about sharing them with you.

4. Topping up employee knowledge with the latest security policy updates

What has recently changed in your organisational security policies? Has any new guidance been released in the last few months? Make sure you keep your employees updated about the latest security policies as these can change regularly. Social media policy, for example, is likely to require regular review.

Your role

Ensure security conversations form part of your regular team meetings so your employees can raise any concerns, questions or issues they have and you can remind them about any new policies or changes in threats or procedures. Where possible, link these conversations to organisational security campaigns so your briefings are coordinated and have greater impact.

5. Keep a security-conscious culture alive

Security breaches can happen anywhere, so one of the most effective countermeasures is to have eyes everywhere. Employees should be aware of potential security risks, not just in their part of the building or site, but across the wider organisation. This includes the risks they face while travelling to and from work, and while working online.

Your role

Make sure your team is kept informed of the threats to the organisation and that they are aware of how these impact not just on their work, but on their colleagues' work too. Encourage them to maintain a security-conscious mindset in all aspects of their work – be it working at different sites, with different teams, or online.

ONE LAST THING...
Don't make it boring!

Simply listing procedures and rules, or trying to lecture people, will not engage them. To help you make security messages interesting and relevant to your staff, we have developed some materials that you can use as part of a security awareness-raising campaign.

Use these materials to help open up a dialogue within your team about security. Get them actively talking about the role they play and how they can contribute to maintaining a secure and safe workplace.

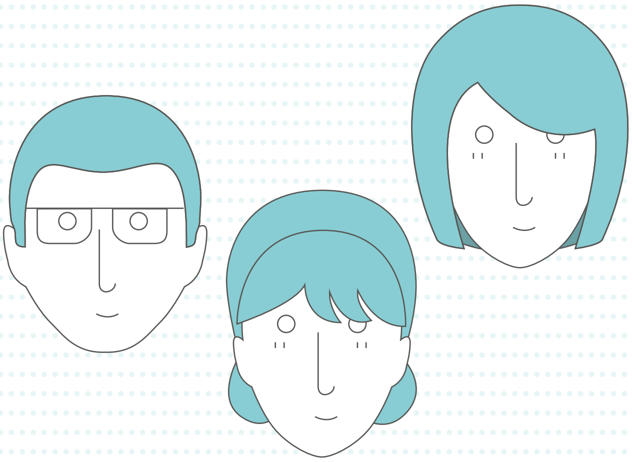
You might want to provide case studies in addition to these campaign materials to illustrate the damage that can be done, and how it directly affects everyone in the organisation. Also, look for constructive ideas from your team to help keep security messages and appropriate behaviours alive. This will ensure everyone has a security-conscious mindset as they go about their everyday work.

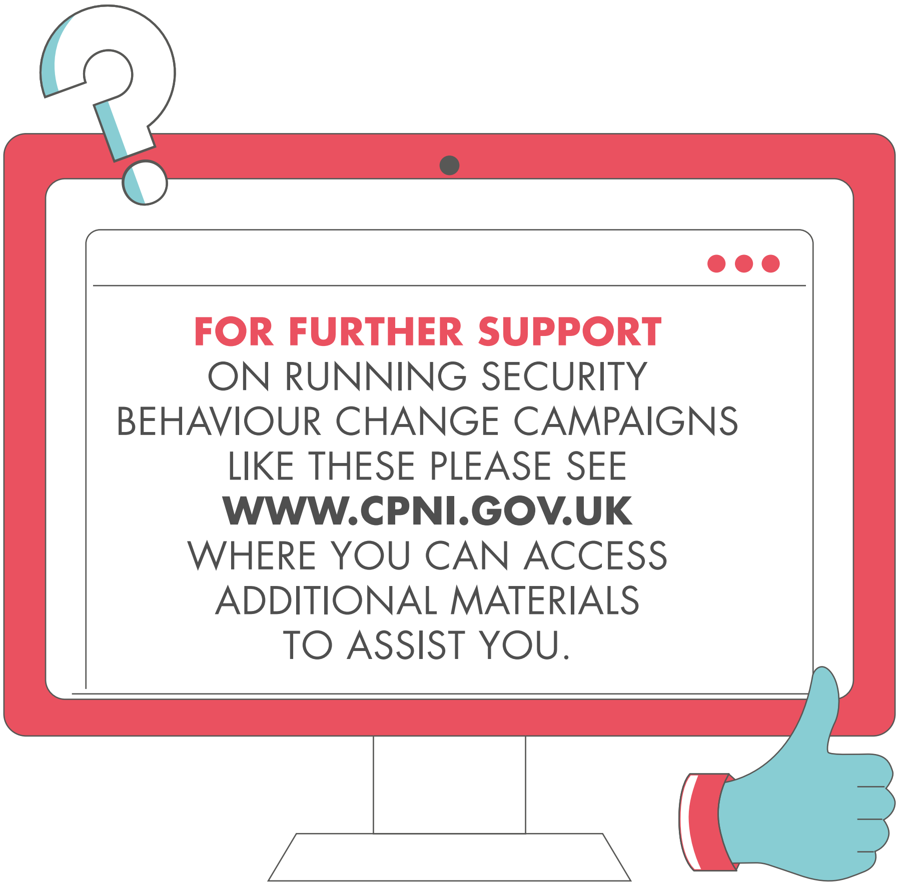
LINE MANAGERS' PACK MATERIALS

This pack includes a range of materials to help make it easier for you as line managers to understand your responsibilities in relation to staff security behaviour and to assist you with raising security awareness within your team.

- **Are you managing security?** – Managers: Are you managing securely? (this document)
- **Online video** – Animated infographic guide for you (as a manager) to watch, helping explain how security forms part of your role and responsibilities
- **Checklist poster** – Managers' quick-reference checklist on your responsibilities with regard to maintaining security awareness within your team (something you can keep by your desk or close to hand)
- **Amendable and customisable security awareness presentation slides** – MS PowerPoint slides to help you brief your staff on what the security threats and risks are and how they can help ensure sensitive organisational assets are kept safe and secure
- **Post-It-style notes selection** – To remind employees to adhere to good practice security behaviours in the workplace. Use these to help bring the security message alive but monitor how they are being received by the team as you want to avoid being patronising.

In addition to these materials, you or your organisation may like to run specific security awareness campaigns targeted at embedding certain good practice security behaviours (e.g. security in the workplace, security-conscious digital footprint management).





FOR FURTHER SUPPORT
ON RUNNING SECURITY
BEHAVIOUR CHANGE CAMPAIGNS
LIKE THESE PLEASE SEE
WWW.CPNI.GOV.UK
WHERE YOU CAN ACCESS
ADDITIONAL MATERIALS
TO ASSIST YOU.

TOGETHER, WE'VE GOT IT COVERED.

CPNI
Centre for the Protection
of National Infrastructure