CPNI
Centre for the Protection of National Infrastructure

Pandemic Security Behaviours - Update

PUBLISH DATE:
Nov 2020

CLASSIFICATION:
Official

This guidance is intended for employers (particularly IT Managers, Human Resources and Security Teams) in the national infrastructure. It aims to inform employers about the continuing personnel security vulnerabilities during COVID-19 and provide practical guidance on mitigating these risks as the pandemic extends into a second wave.

General Security

From the start of the first UK lockdown in March 2020, organisations across the UK have had to adapt their usual security practices. What began as short-term contingency security measures may now have become the 'new normal'.

The threat to security from sophisticated hostile state actors, terrorists and criminals, has not reduced during the COVID-19 pandemic. Hostiles have taken advantage of this period because organisations and their employees are understandably distracted from focussing on security.

It is therefore crucial for all staff to remain alert to the threats and for organisations to take steps to mitigate security risks even whilst continuing to deal with difficult and ongoing changes in circumstances.

Key Points

- Conduct a **risk assessment** before adjusting security policies and procedures to accommodate COVID-19 adapted working practice.
- **Communicate** any changes to security policies and procedures clearly across the whole workforce.
- Remind the workforce of the **continued security threat** during this period.
- Continue to provide **wellbeing support** and security guidance to the workforce, especially those **working remotely** over an extended period.

Further advice and guidance is available on the CPNI website: https://www.cpni.gov.uk/security-risks-throughout-covid-19-0.

General Security

1. Long term ‘remote working’ due to COVID-19

1.1. During COVID-19 there has been disruption to normal workplace operations because of restrictions on travel and the need to provide COVID- secure workplaces. Many organisations have been required to adopt a programme of ‘remote working’ for large parts of the workforce. This has required existing security policies and procedures to be adapted to meet the new arrangements.

Organisations should ensure that a personnel security risk assessment is completed by those with the right knowledge of the threat, the business needs and technology being used. These risk assessments should be regularly updated to ensure any measures adopted at the beginning of the pandemic are still fit for purpose.

1.2. Areas for consideration in the risk assessment may include:

- Large numbers of the workforce working remotely since the start of the pandemic with little direct management oversight.
- IT Security Controls – in order to increase bandwidth some organisations may have altered their security controls.
- Protective Monitoring flags may need re-adjustment to recognise unusual working patterns.
- Arrangements for the workforce continuing to use their own electronic devices remotely may require greater flexibility.
- Policies for the use of cameras and microphones for remote teleconferencing may need adjustment.
- An increased number of previously untested third-party suppliers to provide continuous operations where existing suppliers are no longer available may introduce new risks.
- Changes to the Government’s Job Support Scheme, or sadly, the need to issue staff with redundancy notices, may lead to greater financial stress and uncertainty within the workforce, which if not addressed, can lead to workplace behaviour of concern.

Organisations should ensure that the workforce are given appropriate security awareness refresher training, especially those working remotely since the start of the pandemic, as security complacency and fatigue can start to appear.

1.3. Areas for consideration in training and guidance may include:

- Clear reminders on what is allowed when working remotely regarding: printing, cameras, microphones, use of social media and accessing websites.

The information contained in this document is accurate as at the date it was created. It is intended as general guidance only and you should not rely on it. This information should be adapted for use in the specific circumstances required and you should seek specialist independent professional advice where appropriate before taking any action based on it. To the fullest extent permitted by law, CPNI accept no liability whatsoever for any loss or damage incurred or arising as a result of any error or omission in the guidance or arising from any person acting, relying upon or otherwise using the guidance. Full terms and conditions governing the use of this guidance are available on our website at www.cpni.gov.uk.

©Crown copyright

- Repeating security guidance frequently as a reminder of good practice, for example pinned to other alert messaging.

- Refreshing advice concerning SMART devices in the home such as Alexa and SmartTV.

- Reissuing clear guidance on the secure storage, transport and destruction of sensitive material and IT.

- Advice on how to communicate securely by email, on the phone and when teleconferencing.

- Changing pin codes for conference calls daily, with the new code communicated securely such as in a secure Outlook diary message.

- Repeating advice on how to work from home securely where there are others sharing the same living space.

- Refreshing security awareness training on phishing scams specific to the current situation particularly, such as on professional networking sites ahead of some of the workforce needing to find new employment.

Organisations should continue to ensure that during long periods of disruption due to COVID-19, the workforce has open lines of communication both for secure operational delivery and staff well-being.

1.4. Measures on communications can include:

- Arrangements for virtual interviews for joiners, leavers and moving roles.

- Advice on how to conduct an interview remotely for employment screening, ongoing HR matters or security investigations.

- Ensuring line managers maintain regular contact with employees via team messages and one to one contact, to ensure both operational delivery and staff wellbeing.

- Line managers should be mindful of changes in personal circumstances that might put additional stress on their employees, such as financial concerns, risk to families and ill-health and report these concerns to HR.

- The organisation should ensure that the whole workforce has continued remote access to Occupational Health and Welfare services, if required, during periods of high anxiety.

- Frequent reminders to the workforce of the importance of reporting security concerns even when working remotely, and crucially, how to do so.

General Security

Disclaimer

The information contained in this document is accurate as at the date it was created. It is intended as general guidance only and you should not rely on it. This information should be adapted for use in the specific circumstances required and you should seek specialist independent professional advice where appropriate before taking any action based on it. To the fullest extent permitted by law, CPNI accept no liability whatsoever for any loss or damage incurred or arising as a result of any error or omission in the guidance or arising from any person acting, relying upon or otherwise using the guidance. Full terms and conditions governing the use of this guidance are available on our website at www.cpni.gov.uk.

Freedom of Information Act (FOIA)

This information is supplied in confidence to the named reader and may not be disclosed further without prior approval from CPNI. This information is exempt from disclosure under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation.

©Crown copyright

2. On-Site working during COVID-19

2.1 During this phase of the COVID-19 pandemic, as the number of staff accessing sites fluctuates, most organisations have been required to adjust security policies and procedures to enable safe and secure working.

Things to consider are:

- Where it has been necessary to relax security procedures it is vital that organisations are aware of how security measures at the site have changed and ensure that they minimise any security vulnerabilities as staff numbers may need to flex up and down.

- Remind the organisation’s guard force of any changes to security policy regarding entry and exit such as the removal of sensitive material from site. In addition, the need for increased vigilance of employees who breach the rules, either by accident or deliberately.

- If fewer members of the workforce than normal are present to observe and help enforce good security behaviours, it may be necessary to have a greater reliance upon technical measures to prevent deliberate or accidental security breaches.

- Consider the implications for security on the workforce wearing face coverings, especially for your guard force, and the restrictions this brings to those assessing behaviour of concern and communication.

3. Further guidance

3.1 CPNI has a range of guidance that can support organisations during COVID-19 and this can be found at https://www.cpni.gov.uk/security-risks-throughout-covid-19-0

General Security

Disclaimer

The information contained in this document is accurate as at the date it was created. It is intended as general guidance only and you should not rely on it. This information should be adapted for use in the specific circumstances required and you should seek specialist independent professional advice where appropriate before taking any action based on it. To the fullest extent permitted by law, CPNI accept no liability whatsoever for any loss or damage incurred or arising as a result of any error or omission in the guidance or arising from any person acting, relying upon or otherwise using the guidance. Full terms and conditions governing the use of this guidance are available on our website at www.cpni.gov.uk.

Freedom of Information Act (FOIA)

This information is supplied in confidence to the named reader and may not be disclosed further without prior approval from CPNI. This information is exempt from disclosure under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation.

©Crown copyright