CPNI
Centre for the Protection of National Infrastructure

# Pandemic Security Behaviours

PUBLISH DATE: March 2020

CLASSIFICATION: Official

Personnel Security

## The aim of this guidance

This document provides high level guidance on good personnel security practices during the impact of a national/global pandemic, such as the COVID-19 virus, where usual security practices are either suspended or changed to reflect different working patterns, either on a temporary or permanent basis.

Sadly, the threat to security from sophisticated hostile intelligence actors through to low level criminals will not dissipate during these periods. They will adapt to take best advantage at a time when both organisations and the workforce are distracted. A member of your own workforce could undertake a deliberate insider attack or unwittingly expose your organisation to security risk by making a simple mistake. It is therefore crucial that everyone is alert to the threat to security at this time and takes appropriate steps to mitigate security risks even when having to adapt to difficult and new circumstances

This guidance is intended for employers (particularly IT Managers, Human Resources and Security Teams) in the national infrastructure and aims to inform employers about the personnel security vulnerabilities during these contingency periods and provide practical guidance on mitigating these risks.

## Key Points contained in this guidance

- **Always conduct a personnel risk assessment before proportionately adjusting security policies and procedures to accommodate new working practices both for remote workers and on site.**
- **Communicate clearly any changes to security policies and procedures to the whole workforce.**
- **Provide support and guidance to the workforce, especially those working remotely, covering both technical and wellbeing issues.**
- **Remind the workforce of the continued security threat during this period.**
- **Further advice and guidance is available on both the CPNI and NCSC website.**

## 1.Remote Working due to a Pandemic

1.1 When there is disruption to normal operations because of restrictions on travel or on workforce numbers gathering in one place, organisations may be required to adopt a programme of 'remote working' for the majority of the workforce following their own business contingency plans. This may require 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, plus the business needs and technology, in order to identify new risks from changes in working practices and to mitigate these proportionately.**

1.2 New areas for consideration in the risk assessment during a Pandemic may include:

- Large numbers of the workforce working remotely, possibly using new technology for the first time and for long periods.
- IT Security Controls – in order to increase bandwidth some organisations may consider detuning their security controls.
- Protective Monitoring flags may need adjustment to recognise unusual working patterns around childcare and commuting etc.
- Arrangements for the workforce using their own electronic devices remotely may require greater flexibility.
- Policies for the use of cameras and microphones for remote teleconferencing may need adjustment.
- The use of a greater number of previously untested third- party suppliers to provide continuous operations
- Large numbers of the workforce being put on furlough leading to disgruntlement.

**Organisations should ensure that the workforce are given appropriate security awareness training, especially for those inexperienced at working remotely and using new technology.**

1.3 Areas for consideration during a Pandemic may include:

- Clear guidance on what is allowed when working remotely regarding: printing, cameras, microphones, use of social media and accessing websites.
- Repeating security guidance frequently as a reminder of good practice, for example pinned to other alert messaging.
- Providing advice concerning SMART devices in the home such as Alexa and SmartTV.
- 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.
- Advice on how to work from home securely where there are others sharing the same living space.
- Refresh security awareness training on phishing scams specific to the current situation.

**Organisations should ensure that the workforce has open lines of communication both for secure operational delivery, but also staff well-being.**

1.4 Areas for consideration during a Pandemic should be:

- 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.

- Encouraging line managers to keep in regular contact with employees both through team messages and one to one contact both for operation delivery but staff wellbeing.
- Line managers should be mindful of changes in personal circumstances that might put additional stress on their employees, such as financial concerns and ill-health and report these concerns to HR.
- The organisation should ensure that the workforce has remote access to Occ 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 how to do so.

## 2. <u>On-Site working during a Pandemic</u>

2.1 During a Pandemic, where some staff continue to access sites, there maybe adjustments required to security policies and procedures to enable continuous working while fewer staff are present. However, there may also be scenarios at a site where individuals may take advantage of relaxed security procedures or even minimal supervision for their own unauthorised purposes. It is therefore vital that organisations are aware of how existing security measures at the site have changed and what provisions have been made to minimise any vulnerabilities.

**A personnel risk assessment should be conducted before policies and procedures are amended to ensure a proportionate response to the new working practices. This should be conducted by those with knowledge of the threat as well as operational delivery and technical capabilities**

2.2 Consideration should be given to:

- Ensuring an organisation's guard force are aware of any changes to security policy regarding entry and exit, removal of sensitive material from site, and increasing vigilance to those breaching the rules either by accident or deliberately.
- If fewer members of the workforce are present to observe and enforce good security behaviours having a greater reliance upon technical measures to prevent deliberate or accidental security breaches.
- Frequent reminders to staff on both physical and technical security measures that should be adopted. These should include guidance on when and how to report security concerns.
- Recognising signs of disgruntlement from within the workforce specifically where staff are being put on furlough and receiving reduced pay or conversely from those required to continue working whilst covering for absent staff.

## 3. Further guidance

3.1 CPNI and NCSC has a range of guidance that can support organisations in these activities:

Personnel Risk Assessment - insider-risk-assessment

Remote Working - https://www.cpni.gov.uk/system/files/documents/af/05/personnel-security-in-remote-working-a-good-practice-guide.pdf.

Don't Take The Bait - https://www.cpni.gov.uk/dont-take-bait.

Its Ok To Say - https://www.cpni.gov.uk/its-ok-to-say-education-programme.

Line Manager Campaign - https://www.cpni.gov.uk/line-managers-campaign.

NCSC Working From Home guidance - https://www.cpni.gov.uk/ncsc-advice-home-working.

Remote interviewing guidance.

3.2 Please note. This guidance will be refreshed as new personnel security risks and mitigations are identified.