Office of Cyber-Security & Information Assurance

Office of Cyber-Security
& Information Assurance
Oik son Shickyrys Lectraneagh as Saoghys Fysseree

Advisory Notice

Issue Date 17th March, 2020

TLP: WHITE

Information in this report has been given a Traffic Light Protocol (TLP) of WHITE

WHITE **Public** - May be distributed freely, without restriction.

Working Securely From Home

Overview

As measures are put into place for remotely working from home in response to the spread of Coronavirus COVID-19, it is important that we all maintain a secure working environment wherever we may be.

Those in self-isolation may be working from home, and in some cases may be using personally-owned devices to connect to the organisation's network. Regardless of where you are working and what devices are being used, everyone is responsible for keeping company information, systems and devices secure.

The following recommendations will help to protect company information whilst working away from the office.

Recommended Action

- Only use your company's approved methods for communicating and sharing files. Do not use personal email accounts to send or receive company information.
- Ensure that you are using a strong password for your Internet router, using at least WPA2 for network encryption – check the instruction manual if you are unsure. Links to further information can be found at the end of this document.
- Just as you would in the office, keep documents and devices securely locked away when not in use.
- When disposing of documents, ensure you follow company guidance and at a minimum ensure that documents are shredded appropriately or placed in an approved confidential waste bin if accessible.

- Ensure your computer and devices are protected with a passphrase or other security measure and shut down your laptop or company mobile phone when you have finished using them. This helps keep information safe if the devices are lost or stolen.

- Do not open emails from unknown sources, download attachments or click on links unless you are sure that they are genuine.

- Be aware of your surroundings and what people will be able to see whilst you are working. Consider using a privacy screen for your laptop and make phone or video calls from a private room.

- Lock your computer screen whenever you are away from it for any length of time.

- Follow the company's agreed procedure for reporting any risks or incidents involving company information, e.g. lost/stolen device.

You will find more general guidance on a number of related cyber security topics on our website, www.gov.im. Visit our OCSIA Knowledge Base for guidance documents and other resources, or our OCSIA Advisory Notices webpage for guidance and recommendations such as protecting yourself from ransomware and basic cyber-hygiene.

Further advice and guidance from the UK National Cyber Security Centre (NCSC) can be found at the following links:

Advice and guidance for businesses

- Mobile device guidance
- Home and mobile working

Advice and guidance for individuals

- Top tips for staying secure online
- Three Random Words (Password Security)
- Advice for individuals and families

If you have any concerns, or have been affected by a cyber-related issue, report it to the Office of Cyber-Security & Information Assurance (OCSIA) by submitting a Cyber Concerns Online Reporting Form at www.gov.im/ocsia.

TLP: WHITE