THE CYBER RESILIENCE CENTRE FOR LONDON

OUT WITH THE OLD, IN WITH THE NEW

Strong resilience is needed throughout the lifecycle of any device you own for business.

Here are 10 tips to protect you and your organisation when replacing an electronic device:

>>>OLD

- ✓ Before disposing of your device, make sure all information is wiped so that anyone who uses it in the future cannot recover anything previously stored on it. Deleting your files is simply not enough, these files can always be recovered. To do this, **reset the device to the factory default settings**.
- ✓ Now the device is reset, **do not reconnect to your Wi-Fi** as you will have deleted any security software and settings you once had installed.
- ✓ Where possible, **physically destroy the device**. This is the safest way of preventing anyone in the future being able to access information that was once stored. Companies specialising in data destruction typically break equipment into pieces no larger than 6mm.
- ✓ If you choose to have your device destroyed professionally, **make sure the company meets recognised industry standards** such as those published by the Asset Disposal and Information Security Alliance (ADISA). Your data still needs to be wiped before handing the device over to an external company.
- ✓ If your device has a SIM card, memory card, hard drive or other data storage, don't forget to **remove it before you dispose** of, exchange or sell the device.

THE CYBER RESILIENCE CENTRE FOR LONDON

<<<NEW

- ✓ When buying a new device, make sure you **buy new tech from reputable sellers**. If you are buying a used device, ask them what steps they have taken to remove any information previously stored on it.
- ✓ If the device is dispatched via courier, ask the seller of the checks carried out to **confirm the delivery process is secure**. Always ask for tracked delivery and make sure it can only be signed for by a named individual.
- ✓ **Create an On-Boarding Policy for new devices**, for a consistent configuration that meets your security requirements. Never assign a new device to a user or connect it to your Wi-Fi until this process is complete.
- ✓ Prevent tampering of equipment by **restricting the number of people allowed to configure the initial set-up of the device**. For example, a nominated administrator within your organisation who has additional rights of access to your system.
- ✓ **Keep manuals for all of the devices** you use so that you can follow the manufacturers guidance when looking to dispose of them.

Don't forget to sign up for our FREE emails!

@London_CRC Cyber Resilience Centre for London @CRCforLondon londoncrc.co.uk info@londoncrc.co.uk