Office of Cyber-Security & Information Assurance

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

Guidance Document

Issue Date 6th July, 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.

5 Steps to Cyber Security: Step 4 - Backup Your Data

Backing up your data regularly, and testing restoration will reduce the impact and inconvenience of any data lost from theft, physical damage or malicious software such as ransomware.

This guidance document covers some considerations to take into account when thinking about backing up your files.

Identify the files to backup

Ideally, you should consider complete backups of systems and data but if this is not practical, decide what data your organisation needs to keep running and how often this data should be backed up.

Before backing up your data, you also need to think about where the backups will be stored, how accessible they are and the repercussions in the case of a breach, particularly if storing personal and sensitive information.

- Store backups securely, in a location where there is a low risk of physical damage and theft. This should be away from your original data.
- Encrypt the data - many external hard drives and cloud services provide this feature.
- Consider following the **'3-2-1' rule** for backing up data:
  - **3** copies of data
  - **2** different backup mediums, e.g. external hard drive, CD's, cloud
  - **1** backup stored off-site, ensuring that it is offline / disconnected from the network

Disconnect backups when not in use

Every time the process of backing up has been completed, backup devices must then be completely disconnected and isolated from the device storing the original data.

Consider using the cloud

Using a cloud backup service means your data will be **stored in a separate location** (off-site), which can be accessed and used to restore your systems whenever required.

Many different cloud storage solutions exist but when researching the right service for you, ensure that your selected solution features **backup capabilities**. Regular cloud storage solutions may be permanently connected to your network and also be affected by malware if there are no backup protections.

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.