

**WHY IT MATTERS**

Data is your most valuable digital asset. The pictures, documents, and files you create, use, and rely upon everyday are difficult or impossible to replace if damaged or deleted. Personal information can cause significant harm if stolen or disclosed. Protecting your data involves the ability to backup data (protect from loss), verify the integrity of the data (protection from alteration), and maintain confidentiality (protect from disclosure).

Fundamentally, you must recognize the value of your data and information, the different types of information, and how difficult it would be to replace the data if it were lost. Making copies of data provides a backup of the data and can be recovered if the original is lost or damaged.

**B**

**DATA**

**WHAT TO KNOW**

Data should be treated as if it were your most important asset. Your perception of data may be based on your comfort level. Most people are not concerned about protecting their information because they are not aware of the risk of loss or disclosure. Data is the most important aspect of your device. The operating system can be reinstalled and so can applications, but it may be difficult or impossible to recreate your original data.

What is a backup? A backup of your data is essentially maintaining an up-to-date copy of your files and data. This can be as simple as keeping a separate copy of all of the pictures you take, or saving all of the changes to your word documents. The purpose of keeping a backup is to safeguard yourself from data loss and facilitate a quick and painless recovery of data.

*“Drilling into the value of data” – Forbes*

<http://www.forbes.com/sites/howardbaldwin/2015/03/23/drilling-into-the-value-of-data/#5ab4fa042872>

*“Backing Up Your System” - MIT*

<https://ist.mit.edu/security/backup>

**WHAT TO DO**

To increase your chances of recovering lost or corrupted data, follow the 3-2-1 rule:

3 – Keep 3 copies of any important file: 1 primary and 2 backups.

2 – Keep the files on 2 different media types to protect against media failures (external storage, USB).

1 – Store 1 copy offsite (e.g., outside your home or business facility).

*“Data Backup Options” – US CERT*

[https://www.us-cert.gov/sites/default/files/publications/data\\_backup\\_options.pdf](https://www.us-cert.gov/sites/default/files/publications/data_backup_options.pdf)

**HOW TO DO IT**

**Android Backup** - You can use Android Backup Service to back up data connected to one or more of your Google Accounts. If you have to replace your device or erase its data, you can restore your data from any backed up Google Account.

<http://www.gottabemobile.com/2016/09/27/how-to-backup-android/>

**iOS Backup** - When you backup your iPhone, iPad, or iPod touch, you'll have a copy of your information to use in case your device is ever replaced, lost, or damaged. There are 2 methods for backing up your iPhone: iCloud and iTunes.

<https://support.apple.com/en-us/HT203977>

**WARNING:** Changes to device and application settings can have unintended consequences and may interfere with normal operation. Improper use of encryption and authentication can cause a loss of data and prevent access. Please do not attempt to apply any guidance that exceeds your level of knowledge and familiarity with your device or application. All guidance is provided “as-is” from referenced sources. User assumes responsibility for any changes made to their device and/or applications.

