10 Ten Tips for Physical Security

1 LOCK DOWN DEVICES

Place tablets and phones in a locked drawer when not in use. Never leave unsecured devices unattended!

2 USE ENCRYPTION

Many devices will offer the option to encrypt a file or the whole device. Encryption means that even if someone steals the device, they can't read your files.

3 KEEP A CLEAN DESK

Notes, devices and documents can convey sensitive information. Keeping everything locked up and out of sight will help keep that information out of an intruder's hands.

4 PICK UP YOUR PRINT JOBS ASAP

Printouts often contain sensitive information. Be sure to pick up your print jobs right away.

5 DESTROY BEFORE DISCARDING

Documents and electronic files need to be destroyed before the medium itself is thrown out or recycled.

6 DON'T LET PEOPLE FOLLOW YOU IN

Entering the building is the first step for many attackers. Everyone who needs to be there has their own key card; don't let strangers persuade you to let them in!

7 BE AWARE OF SOCIAL ENGINEERING

Social engineers deceive people in order to manipulate them into giving out valuable information or making mistakes. Be aware of the common social engineering tricks, such as pretending to be a delivery person to access a building.

8 BACKUP FILES

Mistakes or accidents will happen, and something will get lost, broken or destroyed. Keeping regular backups will save you from having to redo your work.

9 KNOW GOVERNMENT AND WORKPLACE POLICIES

Your industry may fall under special government regulations for physical security. It's important to know the policies that apply to your situation, whether they were put in place by the company or the government.

10 KEEP AN EYE OUT

Be aware of your surroundings. Intruders may eavesdrop or spy on you over your shoulder! If entering a PIN on a pad, shield the pad with your hand.

©2019 Infosec, Inc. All rights reserved.