9 KEYS TO KEEP YOUR INFORMATION SECURE

Guideline for keeping information secure by EXIN

KEY 1

There is no security without you. Everyone is responsible for safeguarding the security of valuable information. Everybody needs to take steps to protect required information, the company's identity, and the access to information.

KEY 2

Company information is valuable. Always protect sensitive content with a password to prevent someone from accessing it. Of course, you should never leave sensitive data lying around or in shared conference facilities. Another preventive measure is the clean desk policy. When handling personal data, always collect, use and share personal details of customers if this is required in the process. You can always secure your printing as well, make sure you only print, copy, and scan information if necessary. Don't forget to collect the documents from the printer's output-tray.

Use the Secure Printing option for confidential documents. Dispose documents with sensitive information and/or marked confidential in the special container or the shredder. An example of sensitive information is any document with a name of an individual on it. Don't store any documents on the local drive of your laptop. Sometimes you may also have to travel for your work and you will be working from a remote place, in such cases you should always protect yourself against shoulder surfing.

KEY 3

Handle email and internet with care. Don't open unknown e-mails and attachments from untrusted parties. It's always tempting to click on hyperlinks in suspicious e-mails, but not wise! In case you need to forward a message, do it only if it's appropriate and consider deleting the history of the message. A safe way to share documents is by saving them in PDF format to ensure that the files can't easily be changed. Surfing the internet is an every day thing, however, always be careful with what you share. Never share sensitive information about the company on social networking sites. A wise move is to avoid participation in blogs in which your views and opinions may be interpreted as those of the company. And don't forget: don't access, download, store or send any illegal or offensive material.

KEY 4

Use strong passwords. Your computer's password is the key to access all information you have stored on there and on online accounts. So, overall, it is highly recommended to use a strong password to protect this information. The best way to create your strong password is by following these tips: use at least eight characters, combine letters (capital and lowercase), numbers and symbols. The greater variety of characters that you have in your password, the harder it is to guess. Don't use personal information - names, birthdates, etc. - that someone might already know or easily obtain and try to avoid common words. Change your password regularly. Keep your passwords secret. If you believe your system has been compromised, change the passwords immediately. Your password is unique and must not be shared with anybody. Have a strategy to memorize your passwords. If you do have to write them down, be careful where you store them. Use different passwords for each online account. If you use the same passwords on multiple accounts, an attacker who gains the access to one account will be able to access all of your accounts.

EXIN

KEY 5

Guard the access to your computer.

Always lock your screen when you leave your desk for any reason. Do not allow other people to plug their USB drive into your computer, especially personal non-secure drives. Don't install or use illegal and/or unauthorized software. Unknown external programs can open security vulnerabilities in the company's network. Don't connect your personal laptop to the company's network as it may contain viruses or malware, use the guest account.

KEY 6

Handle corporate devices with care.

Laptop

Don't install or use illegal and/or unauthorized software. You can double check if your wireless connections are switched off when you don't need them. To keep your laptop safe, you can connect the company's laptop to the company's network on a regular basis to update your security checks. And, of course: don't leave your laptop unattended.

USB Drives

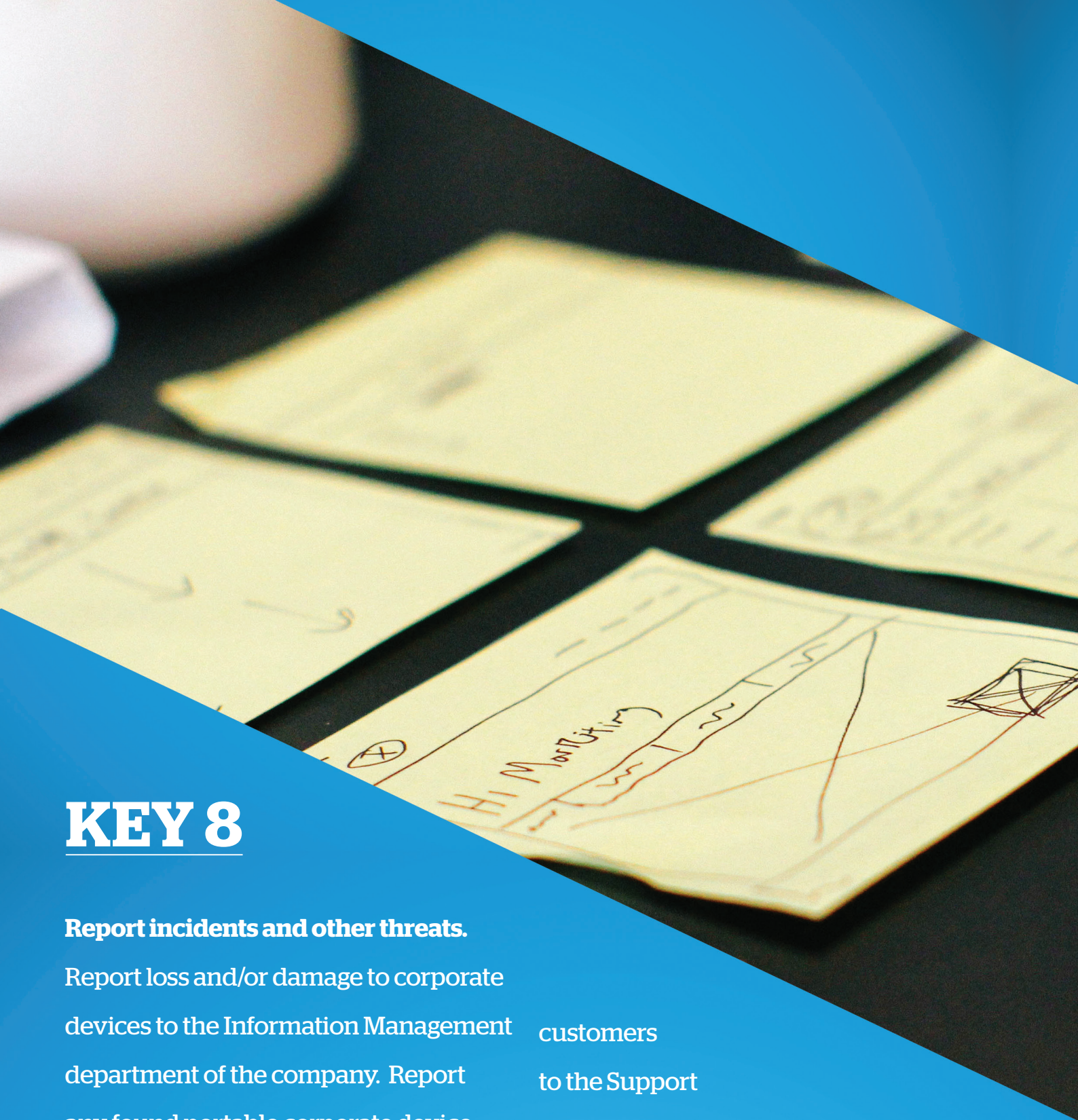
Use an encrypted USB drive (stick). Limit the amount of corporate data which you store on your USB drive, especially on personal non-secure drives. To prevent loss of the USB stick, you can attach it to a key chain or lanyard. Furthermore, the higher the storage capacity the higher the potential amount of data at risk for unauthorized access. The number of incidents has increased recently as USB drive get lost, misplaced, borrowed without permission or stolen. There are multiple ways to prevent virus transmission on the USB stick: Put the USB flash drive in read-only mode using the physical switch. You can also scan the USB flash drive after copying files from an untrusted and/or unauthorized machine. Before plugging your USB drive into someone else's computer, delete all files which are not relevant for the purpose of that action. Every now and then create a backup of your information: you'll be able to recover your data quickly that was on the USB drive.

Smartphone / iPad

Switch off wireless connections when you aren't using them (i.e. Bluetooth and WLAN). Never leave your smartphone or iPad unattended and put a password on your devices.

KEY 7

Register your visitors. All visitors should be registered at the reception and signed in when they arrive and out when they depart. All visitors should be provided with a visitor identity badge that needs to be worn at all times while they are visiting the corporate building. It's important to escort visitors around the corporate building at all times. If you see someone who is not wearing an identity badge, ask if you can help them.



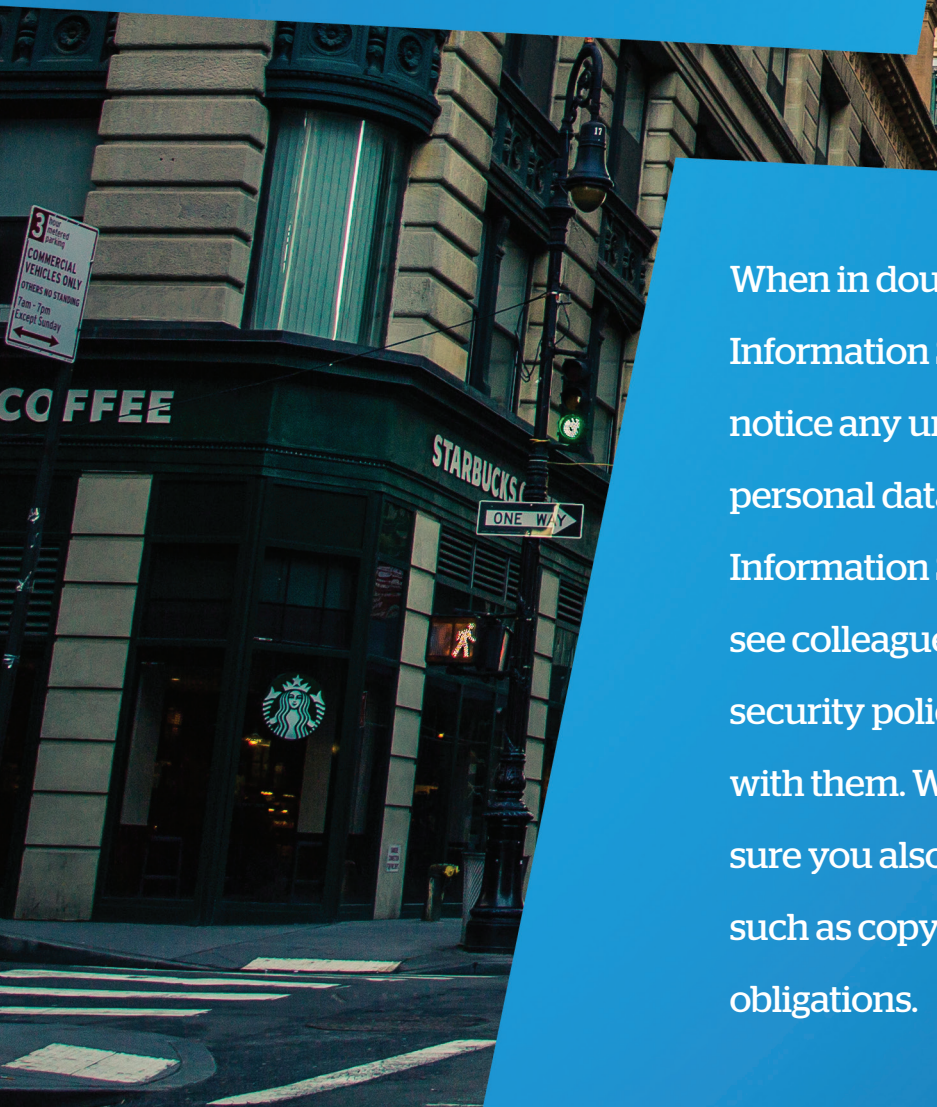
KEY 8

Report incidents and other threats.

Report loss and/or damage to corporate devices to the Information Management department of the company. Report any found portable corporate device to the Information Management department of the company. Report any suspicious activities on your workstation and unexpected unavailability of an application. Report any security breaches by and/or incidents at customers to the Support Center. If you are in doubt or when it is urgent, contact the Information Security Officer directly. Report any security breaches and/or incidents within the company to the Information Security Officer.

KEY 9

Protect personal data and comply with legislation and company policies. Your company has its own security policies and procedures, and it is your task as an employee to comply with these regulations. Ensure the confidentiality and accuracy of personal data. A high priority in your job should be to handle information concerning customers/colleagues with great care; always act in line with the privacy policy of your company. Only share personal information of individuals with third parties when you are sure that there are sufficient grounds to do so.



When in doubt, ask your manager and/or Information Security Officer for advice. If you notice any unauthorized use of or access to personal data notify your manager and/or the Information Security Officer immediately. If you see colleagues acting in breach of corporate security policies and procedures, discuss this with them. When exchanging information, make sure you also respect other legal requirements such as copyright restrictions and confidentiality obligations.

EXIN

SOURCE

Based on: ENISA (European Network and Information Security Agency). The growing requirement for information security awareness (2009).

Published and designed by EXIN. EXIN is the global independent certification institute for professionals in the ICT domain. With 30 years of experience in certifying the competences of almost two million professionals worldwide, EXIN is the leading and trusted authority in the ICT market. With over 1000 accredited partners EXIN facilitates exams in more than 125 countries and 20 languages.. For more information about information security and our certifications, please visit www.exin.com/infosecurity