Teleworking and personal data protection

Governed in the Principality by Law no. 1.429 of July 4, 2016 on teleworking, «*Teleworking is a form of work organization and execution using information technologies within the framework of an employment contract governed by Law no. 729 of March 16, 1963, as amended, and in which work, which could also have been carried out on the employer's premises, is carried out partly away from those premises on a regular basis* ».

Its implementation presupposes that two cumulative conditions are met:

- the employee’s agreement,
- the provision by the employer of the technical and material resources required for such an exercice.

In view of the widespread use of teleworking in the Principality, the APDP felt it necessary to issue a reminder of the best practices to be adopted by both employers and employees to ensure the security of information systems, the protection of personal data and respect for employees' privacy.

Working from home is often not as secure as working within the company, which is a godsend for hackers, always ready to take advantage of the slightest security flaw.

Working remotely, usually from home, must not lead to constant and inappropriate surveillance of employees' work or working hours, nor infringe on the need to respect their private life and that of their family and friends.

Recommendations for employers

It is important to take both information and awareness-raising measures for employees and technical measures to secure the information system.

➢ Measures to inform and raise awareness among employees

Raise your employees' awareness. Whatever technological solutions you adopt, you need to make your employees aware of the security issues involved in teleworking from the outset, by training them in best practice and making them aware of the risks that their actions (or lack of action) can have on the security of the information system (for example, not updating an antivirus or using an unsecured Wi-Fi connection).

Control usage, for example by means of an IT charter or any other document clearly detailing the best practices to be adopted, the restrictions imposed and the procedures to be followed.

Provide responsive support to your teleworking employees by giving the technical department (or any other dedicated department) the means to respond quickly and effectively to questions asked and/or technical problems encountered by said employees. This will prevent them from trying to resolve problems themselves, often to the detriment of the company's IT security.

- **Technical measures to secure the information system**

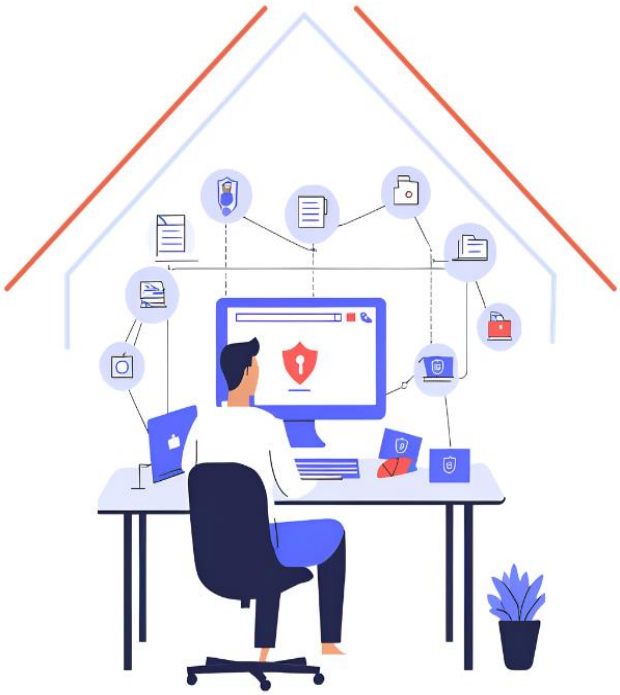
Categorize data and analyze risks for greater IT security. To do this, you need to clearly identify the risks that your company may be exposed to, in particular by classifying data according to their sensitivity, so that you can consider prohibiting remote access to some of them, or putting in place enhanced security mechanisms for others.

You must provide your employees with the equipment they need (PC, telephone, tablet, etc.) for their work. This will ensure that the equipment is secure and under the company's control.

Set up a two-level authentication system to limit the risks of intrusion. It is essential to identify each employee with certainty. For example, when an employee connects to the company network, they should first be asked to enter a user name and password, followed by a one-time code generated by an application or a « *key ring* ».

Equip all employee workstations with at least a firewall, antivirus software and a tool for blocking access to malicious sites. The antivirus solutions used should be professional versions to protect the company from most known viral attacks. In addition, security updates should be deployed as soon as they become available, as cybercriminals are quick to exploit vulnerabilities once they become aware of them.

Secure your external access by setting up a VPN (Virtual Private Network) to avoid direct exposure of your Internet access. Opt for VPN authentication, preferably two-factor authentication, to guard against impersonation. As well as encrypting your external connections, this system also strengthens the security of your remote access by limiting it to authenticated equipment and people.



Reinforce your password management policy for teleworking users and IT support staff by ensuring that passwords are long enough, complex enough and unique enough (a combination of upper- and lower-case letters, numbers and special characters) for each piece of equipment or service used. At the slightest doubt, or even as a precaution, change them and activate dual authentication whenever possible.

Use protocols that guarantee confidentiality and authentication of the recipient server, and make sure you have the most recent versions of these protocols.

Systematically log the activity of all your infrastructure equipment (servers, firewalls, proxies, etc.) and regularly check access logs to remotely accessible services to detect any suspicious behaviour. You should also allow a sufficiently long retention period for all the accesses and activities of your infrastructure equipment, and even workstations. This logging and access consultation will enable you to detect any abnormal activity that could be the sign of a cyber-attack, such as a suspicious connection from an unknown user, or from a known user outside their usual working hours, or an unusual volume of information being downloaded. They will also enable you to understand how a cyber-attack may have occurred, so that you can take remedial action.

Do not make unsecured server interfaces directly accessible. Generally speaking, limit the number of services made available to the strict minimum to reduce the risk of attacks.

Toughen the back-ups of your data and activities. These must be carried out and tested regularly to ensure that they are working. Similarly, it's important to check the level of backup for your external hosting (cloud, company website, email service, etc.) to ensure that the service you subscribe to is in line with the risks incurred by your company.

Set up automatic standby systems. The equipment supplied to your employees should automatically go into standby mode after a short period without activity, to prevent any unauthorized person from accessing the information accessible from your information system.

If you have provided your employees with « *webcams* »: in order to protect the privacy of employees and those around them, the cameras must not be permanently activated, but only in specific circumstances (participation in certain work meetings by videoconference, for example). However, your employees must be able to refuse to use the camera, unless there is good reason to do so. Otherwise, the use of a telephone conference is an appropriate way of participating in work meetings.

Videoconferences or telephone conferences must not be recorded, unless there is a specific justification, for example for evidential purposes. In such cases, participants must be informed in advance.

Recommendations for employees

Scrupulously follow your employer's safety instructions, in particular by respecting the company charter if such a document has been put in place. If you have any problems applying the prescribed measures, you should inform the company immediately, as only they will be able to remedy the situation.

Use the equipment and tools provided by your company (computer, telephone, VPN, etc.) for teleworking.

Secure your internet connection. Wi-Fi can be a very fragile access point to your computer for hackers. However, many people have installed their Internet box without necessarily changing the default passwords or blocking certain accesses. You therefore need to make sure that you have activated the protections on your Internet box, particularly in terms of Wi-Fi (WPA2 or WPA3 encryption) and the built-in firewall. You should also remember to update your box regularly, either by rebooting it or from its administration interface.

Strengthen your passwords. As the majority of computer attacks are due to passwords that are too simple, it is important to use passwords that are sufficiently long, complex and different, mixing upper and lower case letters, numbers and special characters, on all the equipment and services you access, whether personal or professional. At the slightest doubt, or even as a precaution, change them and activate dual authentication whenever possible.

Separate your business use from your personal use. Professional activity should be carried out on your professional equipment and only on your professional equipment, and personal activity should be carried out only on your personal equipment. You should therefore create separate accounts for the websites and software you use. Similarly, the VPN provided by the company should only be used for teleworking and not for surfing video streaming sites!

Apply security updates to all your connected equipment (PCs, tablets, phones, etc.) as soon as they are made available to you in order to correct any security loopholes that could be used by hackers to gain access and use them to attack your company's network via your access points.

Don't do anything at home that you wouldn't do at work. This means, in particular, not visiting suspicious sites and installing applications on your work equipment only with the agreement of your company's IT department. In addition, you should limit recreational use (e.g. social networking) on your work equipment as much as possible.

Be wary of messages (email, SMS, etc.) containing a dubious request or unexpected content. It could be a phishing attack designed to steal your confidential information (login details, passwords), the sending of a virus as an attachment or a link that would take you to a booby-trapped site, or even an attempt to scam you out of your money. Never click on attachments/links in messages, always ask the sender for confirmation by another means, and if in doubt, contact your company's IT department.

Communicate securely by using your company's internal communication channels.

Regularly back up your work, if possible on the company network, or using the resources provided by the company for this purpose (encrypted external media that you disconnect once the back-up has been made).