Checklist to consider when setting up a teleworking arrangement

- ❒ Are there polices and guidelines regarding the use of office equipment such as laptops, blackberries, etc. for teleworkers? Have they been communicated to the teleworker?

- ❒ Are there appropriate user access / limits for applications, e.g. administrator rights and access for installing and removing software and applications?

- ❒ Have you installed / updated the anti-virus software?

- ❒ Is a desktop firewall enabled to prevent the spread of Trojans, viruses or other malicious code rises, e.g. when uploading documents onto the corporate network?

- ❒ Is your computer set to automatically check for software and security updates?

- ❒ Have you set your privacy and security settings?

- ❒ Do you have a back-up system for data stored in the computer used for teleworking?

- ❒ Do you have encryption-enabled WiFi/VPN connection at the teleworking location?

More tips for a secured teleworking arrangement

1. Is there sensitive information that needs to be encrypted before communicating via email / phone / fax?
2. When in doubt, throw it out: links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.
3. Setup session locks so that devices are password protected at all times.
4. When using email, turn off the option to automatically download attachments
5. Save and scan any attachments before opening them.
6. Pay attention to website URLs – malicious websites sometimes use a variation in common spelling or a different domain (for example, .com instead of .net) to deceive unsuspecting computer users.