**BB IT SECURITY Basics - 2022-12-01**

English Version

**Summary of key measures for: Confidentiality, availability and integrity of digital data.**

# Backup (data security against loss)

* Should go automated (so that it is really done regularly, and also so that it is not a productivity brake)
* Label data medium or make excel sheet: What is backed up where, because:
  + as soon as a data medium is broken, you can no longer see what was on it.
* Ideally: Store backup media in another location

# Updates (security against cyber attacks)

* Activate (automatic) updates:
  + Windows
  + Productive software

# Policy (guidelines and training)

* Basically good rules here would be e.g:
  + Do not connect USB sticks from home to the company PC
  + Beware of phishing e-mails: pay particular attention to the sender and domains of links.

# Additional measures (virus protection, etc.)

* Backup production systems as images at a time when they are running smoothly. e.g. With "Macrium Reflect".
* Activate Windows Defender incl. "Real-time protection", "Cloud-based protection" and "Tamper protection" (mostly sufficient as virus protection)

# Confidentiality of (patient) data

* Do not use public hosts for confidential data such as Google Cloud, GitHub, Windows cloud services, Dropbox, etc.
* No confidential information via email
* And if it is necessary: encrypted. Key exchange either personally, via encrypted services such as Signal or PGP (mail encryption), or use key infrastructure such as e-card (citizen card), cell phone signature.