10 golden rules for cyber security

TEMplate

# Authority and review

## Document control and review

|  |  |
| --- | --- |
| **Document check** |  |
| Author |  |
| Owner |  |
| Date created |  |
| Last revised by |  |
| Last revision date |  |

.

## Version management

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date of approval** | **Approved by** | **Description of change** |
| 1.0 |  |  |  |

# 10 Golden Rules for cyber security

|  |  |
| --- | --- |
|  | **Protect your accounts with strong authentication!**  **Always use multifactor authentication (MFA) whenever possible!**   * Long passwords are more efficient because they are more difficult for cybercriminals to crack, given the many possibilities offered by the number of characters. * Strong passwords are **at least 14 characters long, are not easy to figure out and contain: uppercase, lowercase, numeric characters, special characters (&,$,%,!,=,+...).** |
|  | Use different passwords for professional and personal accounts |
|  | Store all your data in a system where backups are made regularly and centrally. |
|  | Run security updates on all your devices as soon as they become available |
|  | Never leave physical information (e.g. papers) or devices unattended at your desk |
|  | Avoid public Wi-Fi and use the organisation's Virtual Private Network (VPN) |
|  | **Avoid phishing by asking yourself the following questions**:   * Is the sender someone I know? * Was I expecting a post on the topic mentioned? * Does the message ask for information such as a username, password or bank account number? * Is it urgent? * Where does the link lead? (just hover over it, don't click) * Does the message contain a QR code? * Am I being addressed personally? * Are there any language errors in the message? * Is the message in the Spam / Junkmail folder? * Is someone trying to make me curious? * Is payment requested?   **How do you respond to a phishing email?**   * Do not reply to them, do not open any attachments or click on the links. * Never share bank details requested via SMS or e-mail. * Report the phishing attempt to **[IT department/provider]** and delete the email/text. |
|  | Observe the following measures when handling internal or confidential information:   * Lock your computer if you leave it unattended. * Do not leave computers or papers unattended on desks outside working hours. * Do not leave papers unattended in printers. * Always watch your surroundings when consulting or discussing confidential information in public places. Try to isolate yourself wherever possible to prevent anyone overhearing a conversation |
|  | Use only official websites and platforms to download applications and software. Downloading software should be avoided. Software is installed by **the IT department/provider.** |
|  | Report all information security incidents to your IT department/provider  Always contact **[IT department/provider]** when:   * you have any questions or comments on this document; * you notice anything contrary to this document; * a suspected or confirmed incident occurs.   Contact details: **[IT department/provider phone number] / [IT department/provider email].** |