10 cybersecurity rules for Czech Television suppliers

1. *Caution when working in cyberspace*

• I exercise caution when using a computer, mobile device, the Internet or accessing the information and communication systems of Czech Television (CT). Threats, such as viruses, malicious code, attackers, can target to steal access data or infect devices, e.g. through fraudulent emails, SMS, phone calls or infected websites, and try to get into the CT computer network to cause damage (data theft, service disruption, ransom extortion, etc.).

2. *Human Resource Security*

- I comply with the relevant provisions of the internal governing documents of Czech Television.
- I use only approved means for storing and sharing data.
- I do not store or share data of ethically inappropriate content or content that damages the name of CT.
- I do not visit websites with inappropriate content or download illegal software

3. *Accounts & Passwords*

- I never give out passwords to anyone, nor do I try to get passwords from CT employees.
- I create unique passwords with a minimum length of 12 characters, meeting 3 of 4 conditions:
    - lower case letter,
    - upper case letter,
    - number,
    - character (#, @, &, !)
- It is forbidden to use the same passwords for private purposes and for the purpose of cooperation with Czech Television.
- I change passwords regularly and protect authentication means.

4. *E-mail*

- I take extra care with unexpected emails or unknown senders. I open attachments and links only after verifying their authenticity.
- I do not send anything that would annoy the recipient or damage CT's name.

5. *Internet*

- I don't access websites that I don't need for my business, especially not websites with inappropriate content or illegal files.

- It is forbidden to use public storage sites for CT data (e.g. Google Drive, Dropbox).

6. *Borrowed equipment (e.g. computer, notebook, mobile phone)*

- I do not interfere with the hardware or software configuration of the device and do not change security settings.
- I only install approved software from the CT Software Center.
- The use of removable media is subject to caution, and I check the media with an antivirus.

7. *Data (visual and audio materials, paper and electronic documents)*

- I protect CT data and follow the empty desk rule.
- I only save files to approved storage sites.

8. *Malware and unwanted activities*

- The computer must have up-to-date antivirus installed.

9. *Reporting security events*

- If a security incident or unusual behaviour of a computer or phone is suspected, the supplier should report it to the IT Helpdesk (+420 261 131 777, Helpdesk@ceskatelevize.cz).

10. *Personal data*

- The Supplier will ensure that all personal data processed in the performance of the contract will be protected in accordance with applicable data protection legislation, including the GDPR.