TECHNICAL CONDITIONS AND SECURITY RECOMMENDATIONS FOR THE OPERATION OF THE AGENT'S OFFICE

Article 1
Installation Conditions

(1) The agent must conclude with the CNB an agreement on access via the CNB's communication gateway. The operator provides information on contact persons in the CNB.

(2) The workstation (Article 2) must have LAN connectivity to a router designed for connection with the CNB.

(3) The workstation must be provided with an exclusive registered IP address from the segment of IP addresses stated in the agreement on access via the CNB's communication gateway.

(4) The agent's office (hereinafter only the "office") may be located in a normal office environment.

(5) The agent shall ensure connection to the CNB at his own expense.

Article 2
Hardware and Software

(1) The hardware and software of the office consists of the following facilities:

a) Technical facilities:
- A workstation of the PC type with parameters enabling smooth operation of software in a configuration described in b)
- LAN card min. 10 Mb/s.

b) Software:
- MS Windows operating system: supported and updated Windows 8 or 10,
- Browser MS Internet Explorer 11 (the application also works with older versions compatible with the used JRE)
- Sun Java Plug-in Version 1.8

c) Data connection:
- minimum 512 kb/s per workstation

(2) The agent may, upon agreement with the CNB, use other hardware with compatible parameters.

Article 3
Cyber security occurrences and cyber security incidents

(1) When detecting cyber security incidents, agents shall detect these incidents adequately with regard to the importance of assets within terminal stations, mobile devices, servers, data storage products and removable data carriers etc.[1]

(2) Should a cyber security incident emerge or the SKD information system behave suspiciously, agents shall be obliged to immediately notify the SKD operator[2].

[1] Article 23(2) of Decree No. 82/2018 Coll., on security measures, cyber security incidents, reactive measures, elements of submissions in cyber security and the disposal of data (Decree on cyber security)
[2] Article 8(6) of Act No.181/2014 Coll., on Cyber Security

(3) Important documents shall be records of communication with clients, e.g. files with e-mails, brief records of important phone calls and other information which the agent deems important. All records must contain a date and at least an approximate time when the described incident occurred. Possible documents which relate to the suspected incident, shall be an extract from the log records or an extract of the suspicious behaviour of the application.

(4) Agents shall submit the documents relating to the cyber incident immediately to the CNB or other authorities. After the cyber occurrence or incident are examined or resolved, the documents shall be removed, overwritten or physically disposed of in compliance with Appendix No. 4 to Decree No. 82/2018[3].

Article 4
Security Recommendations

(1) The office may be operated only by the persons recorded in the SKD as the agent's employees (Rules of the SKD, Article 6, paragraph (1)).

(2) If the agent connects the workstations to his local computer network or to any other system, or if the agent carries out the installation of further software products on these workstations, he shall be liable for any errors in the operation of the software.

(3) The agent's obligations

a) prevent access of third persons to the private keys of SKD user certificates,

b) ensure an appropriate level of security of the client computers of SKD employees, especially by using firewalls, anti-virus software and anti-spam software, by systematically seeking out known vulnerabilities, by updating the operating system and installed applications, as well as by restricting access of client stations to Internet addresses with harmful content,

c) ensure systemic and physical protection of the private keys of SKD employees, e.g. by acquiring tokens or chip cards with a secure storage for private keys and certificates.

(4) Obligations of the Agent's employees

a) consistently protect the private key of the certificate for creating the electronic signature from access of persons other than the person to whom it was issued by the certification authority,

b) ensure systemic and physical protection of the private key of the certificate for creating the electronic signature, ideally using technical devices (token, chip card) on a "need-to-have" and "need-to-know" basis, or at least by setting a high level of security, i.e. access only via strong passwords, where the keys are located in secure software storage on the client station and in non-exportable format,

c) protect the workstation with anti-virus safeguards, firewalls and other means of protection from malicious software, especially viruses, Trojans, spam, spyware etc.

d) ensure regular updates and maintenance of software, in particular the operating system, web browser and other installed applications,

e) ensure employee login to the operating system using a standard user account without administrator rights and using a sufficiently complex password, or using a different mechanism with a corresponding or higher level of security,

f) prevent unauthorised persons from using the computer and above all the SKD application using appropriate methods, e.g. by logging out or at least locking the computer when the user is absent,

[3] Appendix No. 4 – Disposal of data – Decree No. 82/2018 Coll., on security measures, cyber security incidents, reactive measures, elements of submissions in cyber security and the disposal of data (Decree on cyber security)

g) not respond to requests by third persons to provide login details (spam, phishing); the login details are only meant for the given user and the operator never requests them from users under any circumstances,

h) in the event of suspicion that a certificate has been abused, ensure immediate revocation of validity of the electronic signature certificate with the relevant certification authority, immediately invalidate the registration of the signature certificate in the SKD system, and immediately notify the Cash and Payment Systems Department of the operator. Contact: petra.korbasova@cnb.cz, tel.:+420 224 412 058.

Article 5
Service Conditions

Maintenance of the technical equipment of the office shall be ensured by the agent or by its service firm.

Article 6
Expansion of the Office

Multiple workstations may be used simultaneously at the agent's office, upon condition that each workstation has its own registered IP address.