

**Decree 23/2005 (XI. 23.) MNB
of the Governor of the Magyar Nemzeti Bank**

**on the material, technical, security and business continuity requirements related
to carrying out clearing transactions**

Pursuant to the authorisation defined under Article 60 (1) hd) of Act LVIII of 2001 on the Magyar Nemzeti Bank, I hereby decree the following:

General Provisions

Article 1

- (1) The scope of this Decree shall apply to organisations carrying out clearing transactions specified under Article 3 (2) b) of Act CXII of 1996 on Credit Institutions and Financial Enterprises (hereinafter called: 'clearing houses for credit institutions') on the territory of the Republic of Hungary.
- (2) Accordingly, the rules of this Decree relevant to clearing houses for credit institutions shall also apply to the Magyar Nemzeti Bank (hereinafter called: 'the MNB'), as an organisation operating a national payment and settlement system.
- (3) Meeting the requirements laid down in this Decree shall be a precondition of performing clearing activity. Meeting the requirements laid down in this Decree shall be supervised by the MNB within the framework of its oversight and central bank inspection activity.

Article 2

For the purposes of this Decree :

- a) *action plan*: a regularly updated plan, containing the conditions of preparing for crisis situations, countermeasures to crisis situations, alternative and/or restoration and control processes;
- b) *security*: the undisturbed state of operation of a clearing house for credit institutions, when clearing activity can be performed continuously, without any limitations;
- c) *security risk*: the risk of damages deriving from extraordinary events (its magnitude depends on the probability of extraordinary events' taking place and on the size of damages expected to be caused by such events);
- d) *security activity*: institutional provision for those planning, organisational, managerial, executive and controlling conditions, which serve for the protection of the assets owned by a clearing house for credit institutions and the protection of its other important valuables and interests, employees' own personal properties and safety, and the prevention and averting of extraordinary events and crisis situations in the area of the clearing house for credit institutions;

- e) *security policy*: those principles, requirements and expectations together, the enforcement of which is considered to be necessary by the clearing house for credit institutions in order to maintain security;
- f) *electronic protection*: all electronic property security systems together, which support the performance of security activity;
- g) *electronic property security system*: electronic alarm or visual monitoring system and/or other electronic equipment and technical solutions together which allow the transmission of signals and pictures, give light and/or audible signals and provide for automatic handling of rights of entry;
- h) *crisis situation*: a situation emerging after an extraordinary event's taking place and requiring immediate action, different from the regular, daily activity;
- i) *mechanical/physical protection*: architectural and technical requirements and means which serve the increased protection against unauthorised entry into the building (or part of the building) where the clearing house for credit institutions is located and into premises to be protected and which serve the safe storage of valuables to be protected;
- j) *extraordinary event*: all kinds of human conduct and events of natural or technical origin, which jeopardise or may jeopardise the security of the clearing house for credit institutions by causing the malfunctioning of or damages to or termination of the operation of the important resources or systems of the clearing house for credit institutions, carry the risk of threatening people's life, corporeal integrity or health or the possibility of causing material damages, or which result in death, damages to corporeal integrity or health or in material damages;
- k) *business continuity plan*: the system of action plans to handle crisis situations;
- l) *premises to be protected*: all premises of a clearing house for credit institutions where the informatics system carrying out clearing transactions operates and all premises classified by the clearing house for credit institutions as important from the aspect of secrecy, where documents and data carriers containing business or bank secrets and/or personal data are stored, or data classified as business or bank secrets and personal data are processed or handled.

Material and Technical Conditions of Carrying out Clearing Transactions

Article 3

- (1) A clearing house for credit institutions shall only be located in a building, or in a part of a building, which is
 - a) owned by the clearing house for credit institutions, or
 - b) rented by the clearing house for credit institutions based on a contract concluded for an indefinite period of time with an at least one-year notice period obliging the lessor.

- (2) In order to provide for the continuous power supply of the informatics systems carrying out the clearing transactions and of other means which serve the undisturbed performance of clearing transactions, the clearing house for credit institutions shall be equipped with reserve power source.
- (3) In order to allow the continuous forwarding of messages required to carry out the clearing transactions, the clearing house for credit institutions shall provide for:
 - a) the availability of at least two independent communication channels, if it is the clearing house for credit institutions that has a contractual legal relationship with the telecommunications service providers,
 - b) at least two independent connection possibilities, if the availability of the telecommunication service is provided for by the counterparties of the clearing house for credit institutions.

Security Conditions of Carrying out Clearing Transactions

1. Personal Security Conditions

Article 4

- (1) The clearing house for credit institutions – with the exception specified under Paragraph (2) – shall operate a security organisation or employ a person responsible for security.
- (2) The clearing house for credit institutions shall not be obliged to operate a security organisation or employ a person responsible for security, if it commissions a business association or private entrepreneur falling under the scope of Act IV of 1998 on Regulations on Security and Private Investigation Services Provided by Business Enterprises, and on the Trade Association of Security Guards and Private Investigators to perform the complete scope of security activity.
- (3) The head of the security organisation or the person responsible for security shall
 - a) be employed by the clearing house for credit institutions,
 - b) have a degree from police or military college or university or other university or college degree and higher-grade security qualifications, and
 - c) have at least three years of managerial experience in the field of security and guarding.
- (4) The head of the security organisation shall be responsible for the professional management of the security organisation. Tasks of the security organisation or the person responsible for security shall be as follows:
 - a) to perform the tasks within the scope of security activity,
 - b) to train employees and/or to organise and superintend their training regarding the proper behaviour in case of an attack or other emergency,
 - c) to prepare analyses and give proposals for adequate defensive measures and for rules related to security,
 - d) to be responsible for the professional contents and updating of the security policy and the security rules,
 - e) to control the observance of security regulations.

- (5) The head of the security organisation or the person responsible for security shall perform its activity under the direct leadership of the chief executive of the clearing house for credit institutions.

2. Material Security Conditions

Article 5

- (1) The clearing house for credit institutions shall provide for the material conditions of security on the basis of assessment of security risks related to its activity, proportionately to such risks and taking account of property insurance requirements.
- (2) The clearing house for credit institutions shall treat all information, facts, solutions and data related to security as business secret, including material and technical conditions created for the purpose of security and their technical documentation as well.

Article 6

- (1) Based on its security rules, the clearing house for credit institutions shall – taking into account the contents of Paragraphs (2) and (3) – provide for the mechanical/physical protection of the building (or part of the building) where it is located and the premises to be protected.
- (2) Irrespective of whether the building is exclusively used by the clearing house for credit institutions, the outer perimeter surfaces of the building (or part of the building) where the clearing house for credit institutions is located shall meet the requirements of partial mechanical/physical protection described in detail in the recommendation published by the Association of Hungarian Insurance Companies (hereinafter called: ‘MABISZ’) and titled ‘Technical conditions of insurance against burglary and robbery’.
- (3) The quality of the perimeter surfaces of the premises to be protected shall meet the requirements of complete mechanical/physical protection specified in the recommendation mentioned in Paragraph (2).

Article 7

- (1) In addition to the mechanical/physical protection, the premises to be protected shall be equipped with electronic protection as well.
- (2) Electronic property security systems shall only be
 - a) installed on the basis of a plan approved by the head of the security organisation, the person responsible for security or the person defined in the organisational and operational regulation of the clearing house for credit institutions,
 - b) designed, installed and maintained by persons who have passed the special examination required by the relevant legal provision.

- (3) The codes necessary for programming the electronic property security systems and for issuing operator's authorisation shall be available at the head of the security organisation, the person responsible for security or the person authorised by them in writing and/or the person determined in the organisational and operational regulation of the clearing house for credit institutions, along with regulating safe keeping and access authorisation.
- (4) The clearing house for credit institutions shall provide for the installation and continuous operation of a connection capable of transmitting automatic remote signals between the centre of the electronic property security systems and the receiving centre of a security company providing remote monitoring services.

Article 8

- (1) The mechanical/physical and electronic protection shall only comprise appliances with adequacy certificates issued by a quality control institute approved in the European Union or by MABISZ.
- (2) The mechanical/physical and electronic protection of the premises to be protected in the building or part of building exclusively used by the clearing house for credit institutions shall be integrated with the security system of the whole building or part of building.

Article 9

- (1) The clearing house for credit institutions shall
 - a) store the documents and data carriers which allow its operation and are not needed for performing the daily tasks (backup copy of computer programmes, archived data, backup saves etc.) in a separate lockable room with at least 30-minute fire resistance,
 - b) keep another copy of documents and data carriers in another separate lockable room, different from the one mentioned under Point a), with at least 30-minute fire resistance.
- (2) The clearing house for credit institutions shall define in document management rules the scope of those documents and data carriers which it has to store and protect in accordance with Paragraph (1).

Article 10

- (1) The clearing house for credit institutions shall provide for 24-hour guarding in the building or part of building classified as strategically important from the aspect of operation.
- (2) The place of work of the person working as the guard shall be determined on the basis of local conditions and the security policy of the clearing house for credit institutions. The guard shall be enabled to contact the fire brigade by remote signal or through a telecommunication line and the police through a telecommunication line without delay in an emergency.

- (3) No additional guarding shall be required, if the part of building classified as strategically important by the clearing house for credit institutions is located in a building where the owner or operator of the building provides for guarding of the whole building as specified in the relevant decree.

Business Continuity

Article 11

- (1) The clearing house for credit institutions shall have a tested business continuity plan based on the assessment and analysis of possible security risks which materialise in extraordinary events that jeopardise security. The plan shall contain detailed action plans, including the names of persons in charge authorised to take measures, for the restoration of security as fast as possible after an extraordinary event's taking place, and for the continuation of clearing activity even in crisis situation by providing for continuous operation.
- (2) The business continuity plan shall define the testing environment and frequency of testing all or a part of the resources and systems that provide for the continuation of clearing activity and the action plans which serve for business continuity in a crisis situation, and how the regular and regulated updating of the action plans shall be ensured.

Security Policy, Security Rules

Article 12

- (1) For the safe performance of clearing activity, the clearing house for credit institutions shall define its security policy and the principles relative to security conditions.
- (2) Based on its security policy, the clearing house for credit institutions shall have security rules compiled taking into account security risks and their changes, and containing detailed defensive measures.
- (3) The security rules shall contain:
- a) the tasks and scope of authority of the security organisation or the person responsible for security,
 - b) the materials, tools, equipment, procedures, techniques required for having the material conditions of security in place, indicating the technical specifications to be applied (recommendation, standard and/or technical licence) and in a breakdown according to forms of protection,
 - c) the building (parts of building) classified as strategically important,
 - d) the premises to be protected,
 - e) the general and specific rules of handling extraordinary events,
 - f) the general and special order of employees' responsibility for security,
 - g) the measures for employees' personal safety, emphasising the protection of jobs (persons) exposed to increased danger,
 - h) the order of employees' security training.

Closing Provisions

Article 13

- (1) This Decree shall enter into force on 1 January 2006.
- (2) Simultaneously with the entering into force of this Decree, Article 54 of Decree 9/2001 (MK 147.) of the MNB on Payment Transactions, Clearing and Settlement Transactions, and on the Rules of Money Processing Operations shall be repealed.
- (3) Clearing houses for credit institutions already carrying out clearing transaction on the territory of the Republic of Hungary when this Decree enters into force shall meet the requirements specified in this Decree not later than within 6 months following the entering of this Decree into force.