Information Technology Security Policy for Users

„Sale of storage capacity by auction" document for the library system

1. INFORMATION SECURITY PROVISIONS

1.1 PURPOSE OF THE INFORMATION TECHNOLOGY SECURITY POLICY FOR USERS

The purpose of the Information Technology Security Policy for Users (hereinafter as: the **Policy**) is to define the information technology security requirements for the document library system of the "Sale of storage capacity by auction" (hereinafter as: **document library system**) of HEXUM Földgáz Zrt. (registered office: 2151 Fót, Fehérkő u. 7., company registration number: 13-10-042153, hereinafter as: **HFÖ**),

1.2 PERSONS COVERED BY THE POLICY

This Policy applies to any person (hereinafter as: **User**) who comes into contact with the HFÖ document library system.

1.3 OPERATOR

HEXUM Future IT Kft. (hereinafter as: the **Operator**) will provide the entire IT infrastructure of the HFÖ, including also the document library system.

1.4 CLIENT SERVICE

The Operator's Customer Service (hereinafter as: **Client Service**) provides general IT support to the User and handles IT failures.

Availabilities of the Client Service:
Telephone number during working hours (weekdays 08:00-16:20): +36 30 159 1312
Email address for fault reporting: help@hexum.hu

1.5 USE OF THE DOCUMENT LIBRARY SYSTEM

The document library system may only be used by designated Users of the affiliated organisations authorised for loading documents during the registration process related to the auction sale of the HFÖ Storage Capacity.

Each User is provided with a "private" library structure for storing organisational documents. The User is responsible for any inappropriate saving to the library. The Operator disclaims any responsibility for data stored in an inappropriate library.

1.6 SAVING AND RESTORING THE DOCUMENT LIBRARY SYSTEM

The Operator makes backups of the administrative data stored in the specified directory on the server, as and with the frequency specified in the backup instruction. As a consequence, it is possible to statically restore files and spread sheets with the content corresponding to the time of the backup, excluding the scrolling forward or backward of processes. Special rescue requests must be notified to the Client Service in writing and the consultations shall be arranged on the feasibility of the implementation.

The Operator will carry out the data recovery in accordance with the User's written request sent by electronic mail.

The data recovery request shall include the following:

(a) the last known exact location and description of the data to be restored; and
(b) the date to be restored.

1.7 OBLIGATIONS OF THE USER

Information shall be protected throughout the life cycle of its creation, processing, distribution, storage and disposal.

If the User gets access to data that the User is not competent to process, the fault shall be reported to the Operator.

All IT security-related observations, comments or suspected violations shall be immediately reported to the Operator.

The User will keep confidential all user IDs, passwords, passkeys, or any other means of access to the resources of the HFÖ.

Personal identification codes and passwords shall be kept strictly confidential and shall not be disclosed by Users to each other or to the Operator.

The User will notify the Operator if it detects any deterioration or potential deterioration in the level of IT security in order to prevent IT security deficiencies and will use the experiences to prevent any further eventual problems in the future.

The User will cooperate with the Operator in reviews to investigate incidents that may threaten IT security.

The User is also prohibited from unauthorized use of other User's authorizations, network monitoring and detection, password testing or even attempting to do so, subject to accountability under criminal or civil law.

The User is responsible for:

a) ensuring compliance with the IT security rules;
b) operations performed in the document library system;
c) maintaining access to the document library system;
d) virus protection of documents stored in the document library system.

2. INFORMATION ON DATA PROCESSING

Data protection guidelines for the data processing of the document library system service:

HEXUM Future IT Ltd. (2151 Fót, Fehérkő u. 7.) hereinafter as the data controller acknowledges the it is bound by the content of the declaration, but reserves the right to amend the declaration, provided that it informs its audience about the changes in due time.

In the course of its data processing activities arising from the operation of the document library system, the data controller shall fully comply with its data protection obligations under Act CXII of 2011 on the Right to Information Self-Determination and Freedom of Information (Infotv.) and Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) in order to ensure the highest and most complete level of protection of personal data.

The data controller attaches the utmost importance to respecting the right of information self-determination of its customers. It will manage personal data confidentially and will take all measures to ensure their security.

2.1 DATA PROCESSING PRINCIPLES:

Personal data may be processed if

1. - the data subject consents (voluntarily) to this processing, or
2. - it is ordered by law or by a local government regulation based on the authorisation of the law for reasons based on the public interest (mandatory).

Personal data may be transmitted and the different processing operations may be interconnected if the data subject has given his consent or if the law so permits and if the conditions for data processing are fulfilled for each individual personal data.

Personal data may be processed only for specified purposes, in order to exercise a specified right or to fulfil a specified obligation.

Only those personal data may be processed which are indispensable for the purpose of the processing, which are suitable for the purpose, and only to the extent and for the duration

necessary for the purpose. Voluntary personal data may only be processed following a consent based on appropriate information.

The data subject shall be informed in an unambiguous, explicit and detailed manner of all the facts relating to the processing of his data, in particular the purposes and legal basis of the data processing, the identity of the person authorised to data processing and management, the duration of the data processing and the persons who may have access to the data. The information shall also cover the rights and legal remedies of the data subject in relation to the processing.

The use of unrestricted, generic and uniform personal identification code or mark is prohibited.

The processed personal data shall be:

- collected and processed fairly and lawfully;
- accurate, complete and, where necessary, timely;
- be stored in a manner ensuring that the data subject can be identified only for the time necessary for the purpose for which it is stored.

2.2 SCOPE OF THE DATA PROCESSED

Scope of the data processed: first and last name, e-mail addresses, telephone numbers, company name, date and time of logins and file management operations specified when registering with the document library system.

Deadline for deleting data: five years from the date of registration or until the consent is withdrawn.

E-mail messages sent to the Client Service in connection with the use of the service will be deleted by the Data Controller together with the name and e-mail address of the sender and other personal data voluntarily provided by the sender, after a maximum of five years from the settlement of the case.

2.3 OTHER DATA PROCESSING

Information on data processing not listed in this information notice will be provided at the time of data recording.

2.4 METHODS OF STORAGE OF PERSONAL DATA, SECURITY OF DATA PROCESSING

The data storage locations of the document library system are located at the Data Controller's headquarters.

The Data Controller will select and operate the IT tools used to process personal data during the provision of the service in such a way that:

- the processed data is accessible to the authorised persons (availability);
- authenticity and verification of the data is secured (authenticity of data processing);
- the unchanged state of the data can be verified (data integrity);
- the data are protected against unauthorised access (data confidentiality).

The Data Controller will ensure the security of data processing by technical, organisational and organisational measures that provide a level of protection appropriate to the risks associated with the data processing.

In the course of processing, the Data Controller will retain the following:

- confidentiality: it protects information so that only authorised persons can have access to it;
- integrity: protects the accuracy and completeness of the information and the method of processing;
- availability: it ensures that the authorised user has access to the required information when he needs it and that the means of access are available.

The Data Controller's IT systems and network are protected against computer fraud, espionage, sabotage, vandalism, fire and flood, computer viruses, computer hacking and attacks leading to denial of service. The operator provides security through server-level and application-level protection procedures.

Data and availability of the data controller

Company name: HEXUM Future IT Kft.
Registered seat: 2151 Fót, Fehérkő u. 7.
Tax number: 26750406-2-13
Electronic contact details: help@hexum.hu
Telephone contact details: +36 30 159 1312

2.5 LEGAL REMEDIES

The data subject may request information about the processing of his personal data and may request the correction or, except for data processing prescribed by law, the deletion of his personal data in the manner specified when the data were recorded.

At the request of the data subject, the data controller will provide information about the data processed by the data controller or by a processor appointed by the data controller, the purposes, legal basis and duration of the data processing, the name, address (registered seat) and activities of the processor in connection with the data processing, as well as the persons who receive or have received the data and the purposes for which they receive or have received the data. The data controller will provide the information in writing and in an easy-to-

understand form within the shortest possible time from the date of the request, but not later than 30 days.

The Data Controller will delete the personal data if the processing is unlawful, the data subject so requests, the purpose of the processing has been terminated, or the statutory period for storing the data has expired, or the court or the National Authority for Data Protection and Freedom of Information has so ordered.

The Data Controller will notify the data subject of the correction and deletion, as well as all those to whom the data were previously transmitted for processing. It will refrain from such notification if this does not prejudice the legitimate interests of the data subject in relation to the purposes of the data processing.

The data subject may object to the processing of his personal data if:

- the processing ('transmission') of personal data is necessary solely for the purposes of enforcing a right or legitimate interest of the data controller or of the data recipient, unless the processing is required by law;
- the personal data are used or transmitted for direct marketing, public opinion polling or scientific research purposes;
- exercising the right to object is otherwise permitted by law.

The Data Controller will -with the simultaneous suspension of the processing - investigate the objection within the shortest possible period of time from the submission of the request, but not later than 15 days, and inform the applicant in writing of the results. If the objection is justified, the data controller will terminate the data processing, including further data recording and transmission, and block the data, and notify the objection and the measures taken on the basis of the objection to all those to whom the personal data concerned by the objection were previously transmitted and who are obliged to take action to enforce the right to object.

If the data subject disagrees with the decision taken by the data controller, he may appeal against it to the courts within 30 days following the notification.

The Data Controller may not delete the data of the data subject if the data processing is prescribed by law. However, the data may not be transmitted to the data recipient if the data controller has agreed to the objection or if the court has ruled that the objection is justified.

The data subject may bring an action against the data controller in court if his rights are violated. The court will rule on the case out of turn.

The Data Controller will compensate for the damage caused to others by unlawful processing of the data subject's data or by breach of the requirements of technical data protection. The

data controller will be exempted from liability if the damage was caused by an unavoidable cause beyond the control of the data controller.

The Data Controller will not compensate the damage in so far as it was caused wilfully or through gross negligence on the part of the injured party.

Appeal for legal remedy and complaint can be lodged with the National Authority for Data Protection and Freedom of Information:

Registered seat: 1125 Budapest, Szilágyi Erzsébet fasor 22/c
Postal address: 1530 Budapest, Pf.: 5.
Telephone: +36 (1)391-1400
URL: https://naih.hu
E-mail: ugyfelszolgalat@naih.hu