Extract from the Regulation on Information Security

1. Introductory Provisions

1.1 The purpose of this document is to summarize those information security requirements that are applicable to external parties that are in contractual relationship with HungaroControl Pte. Ltd. Co. (hereinafter: the Company).

This extract is prepared based on the Organizational Instruction issued by the technology director on Information Security.

1.2 The **personal scope** of this document extends to natural or legal persons not employed by the Company that come into contact with the Company's IT systems or have access to data and information owned or managed by the Company (hereinafter: external parties).

1.3 The **material scope** of this document extends to

a. all IT system components used by the Company (including all info-communication technology elements in ATM and ATM-R system environments) and all IT services provided by the Company's IT systems that store, manage, process, monitor, control, and transmit data and information owned or managed by the Company;

b. all properties, premises, and building services engineering equipment used to ensure the proper operation of the IT system components, regardless of the legal basis for use.

1.4 Relevant legislation and other references, requirements:

a. this document has been developed taking into consideration the industrial standards and recommendations, the provisions of all relevant internal regulations of the Company, the contents of ISO/IEC 27001:2013 Information technology – Security techniques – Code of practice for information security controls, and the relevant provisions of the laws listed in clause 1.4. b. of this document;

b. relevant regulatory obligations:

i. Act LXXVI of 1999 on Copyright.
ii. Commission Regulation (EC) No 1032/2006 of 6 July 2006 laying down requirements for automatic systems for the exchange of flight data for the purpose of notification, coordination and transfer of flights between air traffic control units.
iii. Commission Regulation (EC) No 633/2007 of 7 June 2007 laying down requirements for the application of a flight message transfer protocol used for the purpose of notification, coordination and transfer of flights between air traffic control units.
iv. Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002.
v. Commission Regulation (EC) No 29/2009 of 16 January 2009 laying down requirements on data link services for the single European sky.
vi. Act CLV of 2009 on Protection of Classified Information.
vii. Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.
viii. Act I of 2012 on the Labour Code.

ix. Act C of 2012 on the Criminal Code.

x. Act CLXVI of 2012 on the identification, designation and protection of essential systems and facilities.

xi. Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies.

xii. Government Decree 65/2013. (III. 8.) on the implementation of Act CLVI of 2012 on identification, designation and protection of essential systems and facilities.

xiii. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

xiv. Commission Implementing Regulation (EU) No 1029/2014 of 26 September 2014 amending Regulation (EU) No 73/2010 laying down requirements on the quality of aeronautical data and aeronautical information for the single European sky.

xv. Act CCXXII on the General Rules of Electronic Administration and Trust Services.

xvi. Decree of the Ministry of Interior 41/2015. (VII. 15.) on the requirements for technological security and secure information devices, products, and security classification and security level specified in Act L of 2013 on Electronic Information Security of State and Local Government Bodies.

xvii. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

xviii. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

xix. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

xx. Government Decree 271/2018. (XII. 20.) on the roles and responsibilities of computer emergency response team, and the rules for security incident handling, (technical) analysis and conducting vulnerability assessment.

xxi. Commission Implementing Regulation (EU) 2017/373 of 1 March 2017 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011, (EU) No 1035/2011 and (EU) 2016/1377 and amending Regulation (EU) No 677/2011.

xxii. Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises.

xxiii. Government Decree 161/2019. (VII. 4.) on the identification, designation and protection of essential transportation systems and facilities.

xxiv. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

2. Interpretative Provisions

2.1 **Information Security:** ensuring and maintaining the confidentiality, integrity and availability of data and information.

2.2 **Confidentiality:** ensuring that data and information are accessible only to those authorized to do so.

2.3 **Integrity:** ensuring accuracy and completeness of data, information and processing methods.

2.4 **Availability:** ensuring that data, information and the IT systems that provide them are accessible and usable to authorized persons as required.

2.5 **Cyber Security and Cyber Defence:** protection against unauthorized use of data and information and protection against other cybercrimes; and the necessary measures necessary to achieve such protection.

2.6 **Info-Communication Technology** (**hereinafter: IT):** a general term used for (primarily computer and telecommunication) systems and methods that store, manage, process and transmit data and information; under this instruction, the term is used for the Company's corporate, ATM and ATM-R information technology, telecommunication and mobile communication systems.

2.7 **External party:** natural or legal persons that come into contact with the IT systems of the Company or have access to the data or information owned or managed by the Company but are not employed by the Company.

2.8 **User:** collectively the employees of the Company and all those natural or legal persons that come into contact with the IT systems of the Company or have access to the data or information owned or managed by the Company, but are not employed by the Company.

2.9 **Information Security Incident:** unwanted or unexpected individual or serial events that may jeopardize the operation of the Company.

2.10 **Data:** the appearance of facts, concepts, briefings that are suitable for interpretation or processing by human or automatic means.

2.11 **Information:** the meaning attributed to the data; fact that carries new knowledge for the recipient and thus reduces his uncertainty.

2.12 **IT Help Desk:** the function provided by Info-communication Services Department at the Company (hereinafter: the ICTS), the task of which is to handle user requests and inquiries – also including information security shortcomings and incidents - in standardized manner.

2.13 **User ID (or User Account):** a unique string (sequence of characters) clearly relatable to the user and which is used by the user for user identification and to sign-in to and access applications and IT systems.

2.14 **Removable media:** any portable data storage device that can be connected by the user without the support of Info-Communication Services Department (hereinafter: the ICTS) (e.g. floppy disk, CD/DVD/Blue Ray disk, USB drive, external HDD, memory card, other info-communication device, etc.).

3. Information Security Risk Management

3.1 Tasks related to Information Security Risk Management

This chapter does not contain requirements for external parties.

4. Conflict of Interest

This chapter does not contain requirements for external parties.

5. Information Security related Roles and Responsibilities

This chapter does not contain requirements for external parties.

6. Information Security Measures relating to Human Resources

This chapter does not contain requirements for external parties.

7. Management of the Company's Information Assets

7.1 Information Security Classification According to Act L of 2013 (Information Security Act)

This chapter does not contain requirements for external parties.**Information Asset Inventory, Ownership, Classification and Protection**

It is the duty and responsibility of external parties to apply all security measures to all data and information provided under the contract according to the information security classification.

The requirements regarding the management of data classified by laws and regulations are included in the Company's "*Security Regulation on the Protection of Classified Data*".

8. Rules of Acceptable Usage of Information Assets

It is the responsibility of external parties that no IT and mobile communication device (typically tokens and removable media; hereinafter: devices) that was possibly received for the purpose of performing the contract is left unattended, that devices that are not being used are locked away and that the risks of using the devices in public places (e.g. increased risk of spying out user identification and authentication data) are considered.

It is prohibited to allow unauthorized persons to use the devices received for the purpose of performing a contract.

External parties are obliged to demonstrate law-abiding conduct during the use of the devices received and of the IT services provided by the Company.

For information security purposes, usage of the IT services provided by the Company (including the e-mail and internet services) is logged and - in order to detect malware, malicious codes and activities - it is (content) filtered, (virus) checked and in case of need (e.g.

in case of possible so-called zero-day attacks) it might be blocked automatically, without human intervention.

It is prohibited for external parties to browse undesired or potentially harmful web content or publicly accessible services such as:

a. websites related to illegal activities , downloads and drugs;
b. contents related to violence and abuse;
c. cyber and internet crime related sites;
d. pornography;
e. weapons and weapon making;
f. peer-to-peer file exchanger services;
g. gambling and betting;
h. racism, hate speech and
i. any content, website or service that poses a potential risk to the Company.

For information security reasons, the Company both prohibits and restricts access to the above contents.

It is prohibited to share data and files that are required for the fulfilment of contracts via cloud services. Only the Company provided services (e.g. SharePoint, WebShare) may be used for such purpose, applying the security measures relevant to the data class of the given data and information.

External parties must comply with all requirements related to user password complexity and management.

9. Access Control and Entitlement Management

9.1 Business Requirements of Access Control

This chapter does not contain requirements for external parties.

9.2 User Access Management

This chapter does not contain requirements for external parties.

9.3 Users' Information Security Responsibilities

External parties are obliged to contribute to maintaining the information security of all IT systems and applications and to the prevention of unauthorized access attempts to all data and information owned or managed by the Company by complying with all requirements related to the acceptable use of information assets and the requirements stipulated in this document.

External parties are responsible for all activities and actions performed with their own user IDs (accounts) within the Company's IT systems and applications. Therefore, it is the responsibility of external parties:

a. that the passwords that are protecting their accounts are carefully chosen, i.e.:

   i. the password should be easy to remember but hard to guess,
   ii. the password must be at least 8 characters long,
   iii. the password must contain a numeric or special character in addition to upper case and lower case letters,
   iv. it is prohibited to use as password the user's ID or any personal information that could be obviously related to the user (e.g. birthdate, name of the user, family member or of pet, etc.) ,

v. it is prohibited to use as password a word or expression that can be subject of dictionary-based attack (i.e. which is identical to the form found in a dictionary,
vi. it is prohibited to use as password sequential or repeated characters,
vii. passwords used in the Company's IT environments should not be identical to passwords used outside the Company, especially considering publicly available internet services;

b. that proper password secrecy and management is ensured, i.e.

i. it is prohibited to disclose, reveal or make accessible the password to anyone,
ii. it is prohibited both to write down or to store or transmit the password electronically without encryption;
iii. the initial passwords provided by the operator of the given system must be changed during the first log-in,
iv. all passwords may be valid for at least 1 day and maximum70 days and they should be changed before their expiration.

External party must immediately notify his/her contact person or the Company's IT Help Desk after experiencing any suspicious event that may result in the misuse of his/her user ID (account) (e.g. abandoned, lost device, any suspicious phenomenon related to the user ID, abnormal operation and/or functionality, etc.).

9.4 Network, System and Application Access Control

External parties are allowed to access only those network connections and services that they have been explicitly authorized to.

10. Cryptographic Controls

This chapter does not contain requirements for external parties.

11. Physical and Environmental Security Requirements

11.1 Physical Security Requirements

External parties are obliged to comply with all physical security requirements of the Company according to the Company's physical Security Policy (so called 'In-House Rules Extract').

11.2 Environmental Security of IT Devices and Server Equipment

This chapter does not contain requirements for external parties.

11.3 Security of Mobile Devices and Removable Media

It is the responsibility of external parties to comply with all relevant requirements when using any device received for the fulfilment of the contract.

It is the responsibility of the external party to apply all security requirements according to the information security class of the data stored on the removable media to ensure the protection of such data during the use of the removable media. If a removable media contains data belonging to different information security classes, the applied security measures should meet with the requirements of the highest information security class of contained data.

In the Company's IT environment, removable media should only be used for work and/or for the purpose of performing a contract, and only after virus scanning performed with the

antivirus solution applied at the Company. It is prohibited to connect or use removable media from untrusted sources (e.g. abandoned or found ones), which are probably not virus-free.

It is the responsibility of the external party to use cryptographic measures according to the information security class of data stored on the removable media outside the Company's facilities to ensure the proper protection of stored data.

Data stored on removable media is not managed centrally by the Company consequently the external party is responsible for any data losses, damages, and data recovery costs.

Removable media should only transport outside the Company's premises once proper encryption is applied for all stored data. The used encryption method must meet at least 256-bit AES (or equivalent) encryption algorithm.

12. Information Security Aspects of the Operation

This chapter does not contain requirements for external parties.

13. Electronic Communications Security

13.1 Network Security Requirements

This chapter does not contain requirements for external parties.

13.2 Security Requirements for Data and Information Transfer

External parties are obligated to comply with all data and information transfer related obligations and requirements stipulated in the contract.

14. Information Security Aspects of IT System Acquisition, Development and of IT Projects

14.1 Determining Information Security Requirements

This chapter does not contain requirements for external parties.

14.2 Functional and Security Testing, Protection of Test Data

Personal data may only be used for testing purposes in an anonymized form.

15. Information Security Aspects of Contact with External, Contracting Parties

External parties are obliged to comply with all information security related obligations and requirements stipulated in the contract.

16. Information Security Incident Management

All external parties are obliged to report immediately to his/her contact person or to the IT Help Desk all information security weaknesses and potential incidents that he/she has experienced.

Among others, the following events may suggest the existence of an information security weakness and (potential) incident, which must be reported:

a. ineffective or inadequate (information security) regulation;
b. possible breach of confidentiality, integrity, availability of information assets (data, information, applications, IT services, etc.), especially concerning personal data;
c. accidental (human) error;

d. violation of laws, regulations, or the Company's internal regulations;
e. changes without control or approval;
f. hardware or software failure, malfunction, or undesired functionality;
g. violation of access controls or related obligations.

17. Information Security Aspects of Managing Extraordinary Situations

This chapter does not contain requirements for external parties.

18. Protection of Personal Data

18.1 General Data Protection Requirements

This chapter does not contain requirements for external parties.

18.2 Personal Data Processed by the TCHI

The TCHI processes users' personal data solely in connection with the work processes arising from its activity as operator and from the activity of creating protecting a secure IT environment at the Company.

Detailed information on the processing of personal data by the TCHI is included in Annex 1.

18.3 Personal Data Related to Private Usage

This chapter does not contain requirements for external parties.

19. Information Security Reviews

This chapter does not contain requirements for external parties.

Annexes:

Annex 1: Data Processing Policy for Personal Data Processed by TCHI

Annex 1: Data Processing Policy for Personal Data Processed by TCHI

1. In order to ensure the security of the Company's IT systems and that security is maintained at a high-level, the processing of personal data present in the user and technical data generated during the system-use is necessary - with respect to the principle of data minimisation - as follows:

1.1. Scope of processed data:

a. technical details indirectly connected to the person of the user (unique network ID of client devices, i.e. their IP address, unique ID of client device network interface card, i.e. their MAC address),

b. logged technical data recorded during the use of network services (network traffic and internet usage data),

c. user access and entitlement management data (user's name, user ID, number, (entitlement) group memberships) and data related to Company's administration (workplace landline and mobile phone number, office, position, workplace email address),

d. backups saved during operational activities,

1.2. legal basis for data processing: reacting to IT emergencies, network security incident handling, operating electronic telecommunication networks and offering electronic telecommunication services, as well as data management for the purpose of the cybersecurity and information security of the Company to the extent absolutely necessary for and proportional with ensuring network and IT security, in other words, the defence capabilities (at a given level of confidentiality) of the given network and IT system against random incidents and illegal or malicious activities threatening the data stored or transmitted on these networks or systems or the access, authenticity, integrity and confidential nature of services offered by or accessible through such networks and systems, as a legitimate interest of the Company based on a legitimate interest assessment.

1.3. the individuals carrying out the data processing: ICTS and THCS staff;

1.4. data subjects of the data processing:

a. Company employees,

b. representatives of external parties using the Company's IT system components and the services provided by them, or communicating with Company's employees via such IT devices;

1.5. sources of data:

a. devices logging and monitoring the Company's IT network and server infrastructure, including the traffic flow,

b. system components containing backups,

c. Active Directory;

1.6. purpose of data processing:

a. performing operation tasks,

b. ensuring high-level availability of the systems,

c. identifying, preventing, analysing and eliminating cyber-, IT-, information security incidents,

d. managing user access rights;

1.7. duration of data processing:

a. daily backups including data defined in Annex 1 1.1.a-c. are stored for one week,

b. weekly backups including data defined in Annex 1 1.1. a-c. are stored for one year,

c. data defined in Annex 1 1.1. a-c. are stored for five years following the termination of employee's employment;

1.8. method of data processing:

the data manager, that is ICTS and HTCS, has the right to:

a. record and store data listed in Annex 1 1.1. c.,
b. collect, sort and store data under Annex 1 1.1. a-c.,
c. request and get, analyse and connect data for IT security purposes in case of Annex 1 1.1. a-c.,
d. in order to filter out suspicious, harmful and malicious programs, codes and activities - by using automatic methods, not requiring human interaction - to run (virus) scans on, to filter (content) and, if necessary, (for example in case of possible zero-day attacks) to block data in case of Annex 1 1.1. a-b.,
e. request, get and analyse data based on approved user request in case of Annex 1 1.1. a-d.,
f. connect different data included in Annex 1 1.1. a-d.,
g. modify data upon approved user request for data included in Annex 1 1.1. a. and c.,
h. restore data upon approved user request for data included in Annex 1 1.1. a., c. and d.,
i. transfer data in case of request from any authority for data included in Annex 1 1.1. a-d.,
j. delete data in case of user request or if the duration of data processing has expired for data included in Annex 1 1.1. a-d.;

1.9. rights, legal remedies:

user has the right in relation to his personal data

a. to request and get (right of access) data included in Annex 1 1.1. a. and c-d.,
b. to request a review (right of access) data included in Annex 1 1.1. a. and c-d.,
c. to request modification (right of rectification) of data included in Annex 1 1.1. a. and c-d.,
d. to request deletion, except for the cases of mandatory data processing, (right of erasure);

2. The user has the right to turn to the National Data Protection Agency, the Data Protection Officer of the Company or to courts; the rules of exercising rights and using available legal remedies are laid out in

a. the Data Protection Regulation of the Company and
b. in Sections 14-23 of Act CXII of 2011 on Informational Self-Determination and Freedom of Information.