A P P R O V E
JSC "Riga Aeronautical Institute"
Vice-President
_____M.Karoļs
" ____ " _____2018

A P P R O V E
JSC "Riga Aeronautical Institute"
Rector
_____A.Melnis
" ___" _____2018

RIGA AERONAUTICAL INSTITUTE INFORMATION SECURITY POLICY

Riga, 27 August 2018
Place, date

1. Definitions of terms used

Company	***JSC "Riga Aeronautical Institute" (hereinafter referred to as RAI)***, registration No. ***40003083288***, registered address ***Mežkalna iela 9, Riga, LV-1058***, ***Latvia,*** which is the employer for any employee employed on the basis of a Labour Contract.
Management/ Immediate superior	The Board and/or any other person at the Company, which are assigned management functions and authorities.
RAI representative *(in the area of information security policy)*	The Office Manager or other Employee, who has been appointed and approved as a representative by an order of the Company.
Employee	Any natural person employed by the Company.
Management	The Board and/or any other person at the Company, which are assigned management functions and authorities.
Third party	A natural person, legal person or other person, which is not linked to the Company.

2. Purpose and scope

2.1. The purpose of the RAI's information security system is to protect employees, partners and customers of RAI from illegal or harmful direct or indirect, intentional or accidental actions of persons, when processing information and data that get at the disposal of respective persons, as well as using certain equipment for the needs of performance of their job duties.

2.2. The Information Security Policy (hereinafter referred to as the Policy) regulates processing of information in any systems or on any media, which are involved in processing of data/information at RAI, regardless of whether processing of data/information is related to internal commercial operations of or external relations of RAI with any third persons.

2.3. This Policy also regulates how Employees of RAI use the equipment and tools available to them within the scope of performance of their job duties.

2.4. The Policy can be applicable jointly with any other policies, regulations, procedures and/or guidelines, internal and working regulations, the RAI Constitution, etc., which the RAI periodically takes and introduces.

2.5. All the questions about the information security system and matters of security of information/data, which are not stipulated in the Policy, should be addressed to the Management and/or the Office Manager.

2.6. RAI ensures that all research and innovation processes are implemented in a way that protects information, data, and technologies from illegal or unauthorized access, misuse, or leakage. To this end, RAI conducts risk assessments for international and internal cooperation projects, applies appropriate security measures to preserve scientific freedom and academic integrity, provides training and raises awareness among employees about research security risks, and

cooperates with other institutions, in compliance with relevant regulatory enactments and guidelines, including EU and national-level documents on research security.

3. Classification of information

3.1. Any information/data, which becomes available to Employees in the course of performance of their job duties, if such information/data are related to RAI and its operations, customers or cooperation partners, shall be deemed belonging to RAI and confidential, and therefore protected by relevant regulatory enactments on protection of confidential information, trade/commercial secrets and personal data.

Category	**Description**	**Scope of applicability (including, but not limited to)**
Public information	Information, which can be processed and distributed at and outside RAI without any negative effect on RAI, any of its partners, customers and/or related parties.	(a) Public financial statements submitted to state authorities; (b) Information, which is available in public resources or otherwise publicly known, unless it has become publicly known, because an Employee acted in violation of information/data security requirements.
Internal information	Any information, any use of which, if it happens in violation of requirements of applicable	(a) Any documents drafted and/or prepared by an Employee, structural unit of RAI;
	regulatory enactments, this Policy or any other regulation adopted by RAI, can harm interests of RAI and/or any of its Employees, partner, customers.	(b) Any catalogues (of contacts, information, WinStudent database, Accounting database, etc.) created for the purposes of commercial activity of RAI; (c) Any internal service reports, notices, statements, opinions drafted for the needs of commercial activity of RAI.
Confidential information	Any information, which is so essential for RAI, any of its customers and/or partners or related parties, unauthorised disclosure of which may negatively affect commercial activity, operations, reputation, general status of RAI, its shareholders, customers and/or cooperation partners, and serious harm can be inflicted on any such persons as a result of such disclosure.	(a) Policy, procedural, internal regulations, management decisions; (b) Information, which is labelled as a trade secret of RAI for the Employee; (c) Other financial, human resources, legal, marketing information, sales procedures, plans and operations; (d) Business, production plans; (e) Personal identification data; (f) Information protected by cooperation contracts, which RAI concluded in the course of its commercial activity.

3.2. In order to ensure proper protection of information and data, RAI shall classify internal information. Information/data shall be protected regardless of whether such information comes at the disposal of any Employee in the form of any printed materials, on any data storage devices,

as audio/video materials or in any other way.

3.3. RAI shall use the following general classification of information:

4. Systems involved in processing of data/information

4.1. Any information systems, including, but not limited to computer equipment, any software, operating systems, any storage media, network accounts, e-mail accounts, browser systems and any other technical base and tools, used in the operation of RAI, are considered property of RAI.

4.2. Any Employee shall be liable to use such technical equipment and tools with due care and attention, and only for the purposes related to commercial activity of RAI. The only exceptions are the cases, when RAI grants technical equipment to an Employee (for example, a mobile device), giving an explicit consent to its use for personal means.

5. Duties of employees

5.1. Any information/data, which get at the disposal of the Employee, when they perform their job duties, shall be deemed confidential and should be used as confidential, observing their protection according to this Policy, and shall not be disclosed to any third parties, unless the Management informs that such information has become public or was otherwise reclassified into information, which is no longer protected according to the procedure laid down in this Policy.

5.2. All the personal data and other information, using which a natural person can be identified, shall be collected and processed only, when needed and to the extent it is needed for the purposes of performance of Employee's job duties, provided that such actions are carried out within the limits of the authority granted to the Employee and according to the data protection requirements envisaged in the law (in particular, according to 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)).

5.3. Any requests of data and/or requests for processing of data, which any Employees received from data owners – natural persons in the course of performance of his/her job duties, shall be sent immediately for further review by the Board.

5.4. Any Employee shall be liable to observe this Policy, as well as fulfil the requirements of applicable local, regional or international regulatory enactments envisaging information/data processing and protection conditions. Failure to observe this Policy shall be considered a serious violation of the work procedures and may result, at the discretion of RAI, in disciplinary penalty or firing of the Employee. The Employee in violation may also be held administratively or criminally liable.

6. Access and protection management

6.1. Employees may access any devices available to Employees, if it is necessary for the needs of performance of job duties of respective Employees, within the scope of their responsibility and on a need-to-know basis. Access rights to any systems do not mean that the Employee is authorised to view or use all the information available in the respective system.

6.2. System safety passwords shall be created with due care, in such a way that they cannot be guessed, they do not include personal data and are changed on a regular basis (at least once in 3 (three) months). Any Employee is personally responsible for the compliance of his/her password with this Policy and other regulations of RAI.

6.3. The Employee shall access confidential information / data only, if such authorisations are envisaged in the Employment Contract of the respective Employee, and/or if RAI has granted such authorisation to the Employee.

7. Security measures

7.1. All the data and information collected and processed in any form (printed, electronic, etc.) are subject to the requirements of this Policy and any regulatory framework with regard to collection, processing, protection and storage of such data/information, and such documents should be stored in a safe place specified by RAI with such a period of storage as envisaged by applicable laws and/or specified by RAI.

7.2. Employees are prohibited to store any confidential information in their personal devices, with the exception of information, which is temporarily necessary for any specified job-related activity. All the necessary confidential and personally identifiable information should be stored only in the cloud storage approved by IT staff of RAI and in the intranet of RAI. Any downloading of such data to local devices should be avoided and should be done only, when it is reasonably necessary due to processing of information for working needs.

7.3. A properly authorised IT staff of RAI shall be entitled to filter and supervise access of Employees to internet and activities of Employees on the internet according to the requirements of applicable regulatory enactments.

7.4. Any mobile, portable devices (including laptops, tablets, smartphones and other palmtop devices), as well as any cloud information storages should be approved by the IT staff of RAI and properly protected to prevent any unauthorised access.

7.5. Only licensed systems and software authorised by RAI can be installed in equipment and tools used at RAI. A permission of the IT staff should be received before downloading and installation of any software in the devices owned by Employees and used for the purposes described in this Policy.

7.6. In the cases, when Employees use personal (home) devices to access corporate resources of RAI (for example, e-mail, online/cloud databases) Employees shall be liable to observe the requirements of this Policy in the same way, as if they use the equipment provided by RAI. Therefore, it is prohibited to store in the device any RAI-related data and information. Processing of any data is permissible only using the cloud and online storages used by RAI.

7.7. In any case it is strictly prohibited to use public access devices (for example, internet cafés, libraries, etc.) unless critically and urgently necessary for job purposes and the Employee's Immediate Superior has given an explicit written consent to such actions.

7.8. If the Employee is granted the right to access the file storage system of any RAI's customer or cooperation partner, the Employee should be liable to use the access tools assigned by the customer or the partner and to observe the provided instructions about secure information/data processing requirements (including the encryption system, use of passwords, data usage restrictions, use of specifically intended places, etc.).

7.9. As soon as at the RAI's discretion protected data/information are no longer necessary for RAI's operations, such data/information shall be deleted, all its copies shall be destroyed, the Employees involved in processing of respective information/data about their duty to delete/destroy and transfer back to RAI information/data, which they no longer need for the performance of their job duties, and, in particular, return to RAI, delete and destroy copies, if the legal employment relationship with the respective Employee is terminated.

7.10. No information/data specified in this policy should be sent, forwarded or submitted in any other ways to a Third party, unless it is necessary for the performance of Employee's job duties, and to the extent it is necessary for the performance of such job duties. If data are forwarded or submitted to Third parties, protection of the data must be ensured and all relevant security measures should be taken.

7.11. The Company shall audit the systems used in processing of information/data to control their constant compliance with this Policy and applicable regulatory requirements.

8. Prohibited actions

8.1. Unless specifically indicated otherwise, no equipment, systems or tools belonging to RAI, its customers or cooperation partners should ever or in any conditions be used for any purposes not related to the Employee's job duties or RAI operations.

8.2. The activities listed below are strictly forbidden without any exceptions:

(a) Infringement of rights protected by intellectual property rights of any person or RAI, including, but not limited to use, installation, copying, distribution or storage of any illegal software, online platforms, any other electronic content, for which RAI has no license, in any systems or equipment

of RAI;

(b) Unauthorised copying of may copyright-protected materials;

(c) Infringement of rights of any person excessively and unnecessarily collecting and processing personal data of the subject;

(d) Access to data, server or account for such purposes, which are not related to the RAI's commercial activity or performance of Employee's job duties;

(e) Exporting of software, technical information, decryption software or technology in violation of applicable international or national regulatory enactments and/or instructions of RAI;

(f) Exporting of any data or information, which has the value of property and/or confidential value at RAI, if such exporting is not necessary in the course of RAI's commercial activity or performance of Employee's job duties, and/or, if this violates internal rules of RAI, applicable regulatory enactments;

(g) Disclosing of password of the Employee and providing other persons access to it;

(h) Creation of fraudulent offers of products or services using the RAI account;

(i) Commitment of network communication security breaches or breaks. Such security breaches include, but are not limited to access to data, if the Employee is not their intended recipient, or login to a server or account, which the Employee was not explicitly authorised to access, unless such rights are granted to the Employee due to participation of the respective Employee in the specific project of RAI;

(j) Use of any programme/script/command or sending of any message for the purposes of disturbing or disabling a work session of any user with any means.

9. Reporting security incidents

9.1. All information/data processing security incidents or potential incidents should be immediately reported to the Management, which should respectively take all measures to prevent potential harm, eliminate consequences of the inflicted harm and restore the previously existing security status.

9.2. When applicable, the Management shall ensure further reporting of breaches of data/information security to authorities and natural persons involved as envisaged by applicable regulatory enactments and/or European Union laws.

Drafted by:
Marina Romele Office Manager
ADOPTED:
at the RAI Convent meeting
of 07 September 2018 Minutes
No.1809