Pursuant to Articles 39, 40 and third paragraph of Article 183 of the Companies Act (Official Gazette of the Republic of Slovenia, nos. 42/2006, 60/2006 – amend., 26/2007 – 68/2008, 42/2009, 33/2011 and 91/2011), Article 36 of the Employment Relationship Act and second paragraph of Article 21 of the Articles of Association of the company Luka Koper, d.d., the management board hereby adopts the following

RULES ON PROTECTION OF BUSINESS SECRET

SECTION 1
GENERAL PROVISIONS

Article 1

These Rules provide the common basis and a uniform system to be applied for identification, protection and access to business data representing the business secret of the company Luka Koper, d.d. (hereinafter referred to as "Company").

As Company's business secret shall be deemed any and all data, documents and information which constitute the Company's competitive advantage, are related to the Company's business operation and their disclosure to an unauthorised person or to the public might lead to adverse consequences for the Company. In the following text, the term of business secret can also be referred as secrecy, confidentiality, etc.

Article 2

As business secret shall be considered in particular, but not exclusively, the data referring to:

- Company's business operation,
- its business- and technological processes,
- security system and
- critical infrastructure.

Article 3

The obligation to protect the Company's business secret applies to:

- all Company's employees,
- all legal and natural persons to whom data are submitted due to the nature of their work and business cooperation with the Company.

Each person to whom the data classified as business secret is entrusted, or who has become acquainted with the content of such data shall be obliged to protect it and to preserve its confidentiality.

Article 4

The terms used in this Rules shall have the following meaning:

1. **Business secret** shall mean any and all data, documents and information which constitute a competitive advantage of the Company, are related to the Company's business operation and whose disclosure to an unauthorised person or to the public might cause adverse consequences for the Company.

Business secret is a fact or a means from the Company's field of work referring to the Company's business operation, its business- and technological processes, security system and critical infrastructure which, due to the reasons stated herein, shall be protected from unauthorised disclosure, is classified herein as business secret and whose disclosure might cause adverse consequences to the Company.

2. **Document** is each written, drawn, printed, copied, filmed, photographed, optical or any other record of content which has the characteristics of business secret.

3. **Media** is any means which contains a business secret.

4. **Identification of business secret** is an operation or process during which data is identified as business secret in line with these Rules, and its level of confidentiality and duration of confidentiality are determined.

5. **Persons authorised to deal with a business secret** shall be the members of the management board in their capacity as Company's management body, as well as the heads of organisational units (hereinafter referred to as "Heads of OU") for the field of work performed in their unit and other employees of Luka Koper, d.d. based on written authorization of the Company's management board or Head of OU granted in line with the provisions of these Rules.

6. **Termination of confidentiality** of a business secret shall mean the declassification of a confidential data into a publicly accessible data pursuant to the general rules regulating the Company's business operation.

7. **Treatment of business secret** shall mean the identification, designation, accessing, application, recording, reproduction, transmission, transfer, destruction of business secret carriers, storage, archiving and other measures and processes which grant the security and confidentiality of business secrets.

Article 5

Pursuant to the provisions of these Rules, a determined level of business secret confidentiality shall be attributed to a data (hereinafter referred to as "confidential data") whose content is so important that its disclosure to an unauthorized person would cause or might cause clear adverse consequences to the Company, to its economic interests and competitive advantages.

Article 6

A data which has been designated as business secret in order to conceal a committed criminal offence, for the purpose of misuse and arrogation of powers or to hide any other illegal act or unlawful activity, is not confidential.

Equally, as business secret shall not be considered any information that according to the law is designated as public.

Article 7

A person who fills a determined position or is employed within the Company shall be obliged to protect the business secret, irrespective of how the business secret came to his/her knowledge.

The obligation to protect the business secret shall not cease even when the person from the paragraph above ceases to fill a determined position or terminates his/her employment with the Company. The

person's obligation to protect the business secret shall last until a competent authorized person declassifies the information as confidential or makes it available to the public.

All employees shall be obliged to assess the sensitivity of information within the framework of their tasks and competences by proposing to authorized persons to identify determined information as confidential, if this is considered necessary.

SECTION II
IDENTIFICATION OF BUSINESS SECRET

Article 8

The level of confidentiality of a business secret shall be determined by an authorized person based on conditions and in the manner defined herein.

Article 9

The authorized person shall determine the level of confidentiality of a data on its occurrence or at the beginning of implementation of a task resulting in confidential data.

Article 10

The authorized person shall identify as confidential also the data resulting from the merging or linking of data which originally are not confidential but once merged or linked represent a data or a document which needs to be protected due to reasons stated herein.

When confidential data is contained only in a minor part of a document or in an individual document, this has to be excluded from the rest and treated as required by the attributed level of confidentiality. If exclusion is not possible, the level of confidentiality shall apply to the entire document.

Article 11

The relevant criteria for the assessment of adverse consequences and confidentiality level are defined precisely in DN 68 – Protection of business secret.

Article 12

While assessing the level of confidentiality, the authorized person shall define the lowest level which still guarantees the data security that is required for the protection of Company's interests and its security.

The document which is formed of data already classified as confidential shall be attributed at least the same level of confidentiality and duration of confidentiality as applies to the data with the highest level and duration of confidentiality contained in the same document.

Article 13

The level of confidentiality can only be modified by the authorized person who determined the level of confidentiality.

The grounds leading to the modification of confidentiality level must be given in writing. The authorized person shall modify the confidentiality level of the data as soon as the conditions for attribution of

individual confidentiality levels stated herein are changed. The information concerning the changed confidentiality level shall be circulated to all person who received or have access to the data.

Article 14

Each confidential data and each document containing confidential data shall be marked with the confidentiality level and organisational unit details.

The designations stated above shall be applied in a manner that is appropriate for the type of media and its characteristics.

Article 15

The confidentiality of data shall cease:

- on the date stated in the document, if stated,
- on the occurrence of a determined event,
- on revocation of confidentiality.

When the termination of confidentiality cannot be defined as stated in the paragraph above because of the nature or content of the data, the confidentiality shall cease on the expiration of the time limit stated in the regulation applying to archival documents and archives in general.

Article 16

The eligible user of confidential data who received the data in legitimate manner may propose to the authorized person the revocation or declassification of confidentiality level if in his/her opinion the confidentiality of data is not justified or appropriately attributed.

The authorized person is obliged to consider the proposal from the previous paragraph and inform the submitting party about his/her decision.

SECTION IV
ACCESS TO CONFIDENTIAL DATA AND THEIR PROTECTION

Article 17

The right to access confidential data is only held by individuals who must be acquainted with confidential data due to the filling of their position, or because of their implementation of tasks or due to their business cooperation with the Company.

Article 18

While taking over their position or prior to the beginning of their business cooperation with the Company, the individuals from the previous article shall sign a 'Statement on protection of business secret' in which they confirm their acquaintance with these Rules and other provisions regulating the protection of Company's business secrets emerging during their filling of position or cooperation with the Company, and declare their commitment to treat these data in line with this Rules.

Article 19

A person who during the implementation of his/her work becomes acquainted with the data designated as business secret is not allowed to use these data for any other purposes than for the implementation of his/her working duties or filling of position.

Article 20

The authorised person from the organisational unit shall provide that an accurate record and control of all confidential data distributed outside the organisational unit is established. From the record should emerge when and to whom were the confidential data transmitted, and when and by whom were they accepted. The record can be kept either in electronic form or in paper.

Article 21

On the level of the organisational unit, the confidential data shall be kept in such a way as to allow access only to authorized personnel and to those who need them for the implementation of their duties.

Article 22

Confidential data can be sent outside the premises exclusively based on prescribed security measures and proceedings which must guarantee that confidential data are accepted by authorized person or individuals who are entitled to deal with them.

Any transmission or forwarding of confidential data via unprotected information-communication tools is forbidden.

Article 27
COMPETENCES AND RESPONSIBILITIES

Those responsible for a direct implementation of proceedings and measures related to the protection of business secrets are:

- All employees of Luka Koper d.d.;

- Heads of organisational units of Luka Koper d.d. for:

1. adequate treatment of data classified as business secrets;
2. attribution of confidentiality levels;
3. establishing and keeping of records of documents representing business secret and access to them;
4. issuing of authorizations in case of substitution of Head of OU or issuing of authorizations for determined operations stated herein, required to protect the business secret;
5. protection and storage of data classified as business secret;
6. training and education of employees concerning business secret protection;
7. supervision over the treatment of business secrets;
8. providing information and taking of measures in case of loss or disclosure of business secrets;

- Authorised persons, responsible for Security and Safety, and IT:

1. for supervision and reporting to the Company's management board on deficiencies, by proposing solutions for efficient implementation of these Rules and instructions.
2. for the elaboration of a 'Plan for protection of business secret', to be approved by the management board. The Plan for protection shall be attributed the level BUSINESS SECRET – CONFIDENTIAL.
3. for the implementation of measures in cases where there is a suspicion of business secret being disclosed to unauthorized persons.

- Company's management board, by providing conditions that are required for the implementation of these Rules and related instructions.

Article 23
PROCEDURE IN CASE OF BUSINESS SECRET LOSS OR DISCLOSURE

Any employee from Luka Koper d.d. who discovers that confidential data were lost or disclosed to unauthorized persons shall immediately notify the head of organisational unit in which he/she is employed.

Persons on determined positions or persons doing business with Luka Koper d.d. who discover that confidential data were lost or disclosed to unauthorized person shall immediately notify the employee from Luka Koper d.d. with whom they do business or the head of organisational unit in charge of security (i.e. Port Security).

The head of organisational unit in which a disclosure of confidential data took place shall cooperate with authorized persons from Luka Koper d.d. who are in charge of Security & Safety and IT, and they shall immediately take all further measures necessary to investigate the circumstances in which confidential data were lost or disclosed to an unauthorised person, in order to prevent adverse consequences and further loss or unauthorized disclosure of confidential data.

SECTION V
CONTROL

Article 24

Those in charge of internal control over the implementation of these Rules and regulations that were adopted on their basis, are:

- authorized persons within their organisational units, and
- authorised persons in charge of Safety & Security, and IT on the level of Luka Koper d.d.

SECTION VI
VIOLATION OF PROVISIONS OF THESE RULES

Article 25

Any violation of the provisions stated herein and any violation of regulations that were adopted on their basis, represents a breach of national legislation as well as infringement of labour law and employment contract.

A person who violates the legal provisions stated above shall be liable to disciplinary action, payment of compensation and shall be held criminally responsible.

TRANSITIONAL AND FINAL PROVISIONS
Article 26

The area responsible for the protection of business secret shall precisely define in the working instructions

- the manners and forms of classification of data / documents' confidentiality,
- the procedures and measures for treatment of confidential data,

- the manner of keeping a record of documents classified as business secrets with a determined confidentiality level, and access to records,
- the way of implementation and content of internal control exercised over the implementation of these Rules and other regulations adopted on their basis.

Article 28

The measures for physical and technical protection and the measures for the treatment of business secrets shall be implemented within six (6) months of the date of adoption of the Plan for protection of business secret.

Article 29

These Rules shall become effective on 7 March 2017 and shall remain in force until revocation.

On the day of adoption of these Rules, the Rules on business secret adopted on 1 January 2014 shall expire.

President of the Management Board:	Member of the Management Board:	Member of the Management Board resp. for Finance and Accounting:	Member of the Management Board – Workers' Director:
Dragomir Matić /signature/	Andraž Novak /signature/	Irena Vincek /signature/	Stojan Čepar /signature/

/Seal: Luka Koper, d.d./

/Transl. note: Left corner of the last page was initialled by two signatories. /