Πανεπιστήμιο Δυτικής Αττικής

Σχολή Μηχανικών

Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών

Πρόγραμμα Μεταπτυχιακών Σπουδών: ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

«GDPR, FROM THEORY TO PRACTICE»

Development of a Minimum Basic Data Protection System for Public and Private Sector Entities

Christos Vlachakis

A.M.: CSCYB21005

MSc Diploma Thesis

Supervising: Dr. Panagiotis Giannakopoulos

Aigaleo, MAY 2023

The approval of the thesis by the University of Western Attica does not indicate acceptance of the author's opinions.

Πανεπιστήμιο Δυτικής Αττικής

Σχολή Μηχανικών

Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών

Πρόγραμμα Μεταπτυχιακών Σπουδών: ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

«GDPR, FROM THEORY TO PRACTICE»

Development of a Minimum Basic Data Protection System for Public and Private Sector Entities

Μέλη Εξεταστικής Επιτροπής συμπεριλαμβανομένου και του Εισηγητή

Η μεταπτυχιακή διπλωματική εργασία εξετάστηκε επιτυχώς από την κάτωθι Εξεταστική Επιτροπή:

Α/Α	ΟΝΟΜΑ ΕΠΩΝΥΜΟ	ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ
1	Παναγιώτης Γιαννακόπουλος	Panagiotis Giannakopoulos Digitally signed by Panagiotis Giannakopoulos Date: 2023.08.23 16:38:58 +03'00'
2	Στέφανος Γκρίτζαλης	STEFANOS GKRITZALIS 25/08/2023 14:56
3	Μαυρομμάτης Κωνσταντίνος	Konstantinos Mavrommatis Digitally signed by Konstantinos Mavrommatis Date: 2023.08.24 15:51:44 +03'00'

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος **Χρήστος Βλαχάκης** του **Ανδρέα**, με αριθμό μητρώου **cscyb21005** φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών «**ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ**» του Τμήματος **Μηχανικών Πληροφορικής και Υπολογιστών** της Σχολής **Μηχανικών** του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Είμαι συγγραφέας αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο Δηλών

Outline

«GDPR, From Theory to Practice»

Development of a Minimum Basic Data Protection System for Public and Private Sector Entities

Introduction

Strong enterprise or organization privacy practices are critical in a rapidly evolving privacy regulatory landscape in Europe (ISACA, 2023). Privacy violations decrease customer trust and increasingly result in reputation damage and significant fines. Enterprise and organization privacy programs that aim to protect data subjects and gain their trust set those entities apart from competitors. Establishing compliance and maintaining it, is not an easy task for enterprises and organizations. Competent personnel both at technical and legal fields of privacy are needed. In that sense it is crucial that data holders understand data protection principles and the rights and freedoms of data subjects and implement appropriate measures and the necessary safeguards to reinforce these principles and to enable the exercise of these rights.

Having a system, a helper, to assist businesses or organizations is becoming essential given the complexity of the requirements that legislation requires.

The Regulation Scope

The General Data Protection Regulation (GDPR) (European Union and The Council, 2016) is a lengthy text comprising of 99 articles and 173 recitals. It was approved by the European Union (EU) parliament and the council on the 27th of April 2016, came into force on 4th of May 2016 and its effective date is the 25th of May 2018, as stated in its article 99, the last article of the Regulation. The GDPR is divided in eleven chapters. Chapter I contains four articles and is titled General provisions, establishing the scope of the regulation and most importantly containing twenty-six definitions some of which are essential for the rest of this paper and will be introduced shortly, in following paragraphs.

It is important at the beginning to know the purpose of the regulation. The GDPR[1] *lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data*, according to article one.

Definitions

It is essential to know few definitions in order to be able to understand under which circumstances the regulation applies. Chapter's I, Article four (4) provides that information.

According to article four *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online*

[1] 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), OJ L 119 4.5.2016, p. 1-88, http://data.europa.eu/eli/reg/2016/679/oj.

identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Within the definition of personal data of article four, also lies the definition of "identified or identifiable natural person" which is essential for the establishment of an understanding what is to be protected in regard to the processing of personal data belonging to a natural person.

So when are these personal data are being processed? The regulation is clear about that giving another definition again in article four. Once article four is already mentioned twice, it is worthy to establish that this article contains various definitions pertaining to the regulation. According to article four *'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*.

Combining those two definitions together, especially the phrase "any information" for the personal data and the phrase "any operation" for the processing, we easily conclude that the regulation applies always in the context that a piece of personal information is about to be manipulated by someone in any way. The exceptions to the above statement are provided in article two, paragraph two.

Exceptions

Few exceptions are laid down in paragraph two of article two of GDPR where the regulation does not apply and that is mainly when data is processed for purely personal or household activity and when data is processed by authorities for the purposes of prevention, detection or investigation with acts of criminal activities.

Territorial Application

Two other aspects of the regulation in regard with its application is the territorial and the citizenship issue. Again according to article three (3) we easily conclude that application of the regulation should concern all entities within the European Union borders but also entities outside those borders if they are to process data of people within the borders of European Union. Namely the above mentioned people are European citizens being within the European borders and any person of any citizenship being within the borders of European Union at the time of processing.

So what will be the case for example for an Egyptian citizen who traveled to Greece and his or her personal data are processed by an entity based in India? Does the regulation apply to that Indian company? The answer is yes. It should. Even though a European regulation it does apply to entities which want to practice business within European Union space.

Conformity Requirements

Basic Principles

The definitions provided by the regulation are of essential importance in the aspect of establishing by who, where and when a processing takes place and what is to be protected. Of essential interest is also to establish what is expected from processors of personal data to do in order to be in line with the regulation's requirements. A major reference for the required conformity is article five (5) where the basic principles of personal data protection are laid down. According to the article there are nine principles relating to the processing and must be adhered to. Those are, lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality and accountability.

The meaning of those requirements is explained in certain recitals of the regulation. Recital 39 of the regulation states that "*Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should* *be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing."* providing the general idea for the principles to be followed. Further explanations are provided in recitals 40 through 47 where all legal basis for processing are explained, in recital 58 where the principle of transparency is analyzed and in recital 60 explaining the terms of fairness and transparency.

According to the above recitals the objectives of data processing are not that straight forward and some interpretations of the thesis of the lawmaker must be made. We need the interpretations to be taken into account since we will try to code every requirement of the regulation in such a way that a software developer would effortless use our “coding technique” to produce an automated way through which someone inexperienced with the regulation can protect not only the data subjects from illegal processing of their personal data but also a business from the fines each EU country's local data protection authority can impose in the case of that illegal processing.

Table I, is our first attempt to code the requirements, as they are the core obligations of any personal data controller or processor.

Num	Rationales	Requirement	Fulfillment
1	Lawfulness	Consent	Records of processing activities
		Contract	
		Legal obligation	
		Vital Interests	
		Public interest	
		Legitimate interests	
2	Fairness	Information	Privacy Policy
3	Transparency	Easy to understand information provided	Privacy Policy
4	Purpose limitation	Why processed	Records of processing activities

5	Data minimization	What data is processed	Records of processing activities
6	Accuracy	Data is correct	
7	Storage limitation	How long	Records of processing activities
8	Integrity and confidentiality	Safety and access control	Security Policy
9	Accountability	Policies - Procedures	All of the above

TABLE 1. Conformity Requirements

Data Subjects Rights

A new element in the protection of data subjects introduced with the GDPR is the rights which lawfully have all data subjects concerning the processing of their personal data. There may be instance where these rights cannot be exercised or to be more precise can't be fulfilled from the part of the data processor, but they do exist. Data subjects' rights is another keystone area where the conformity with GDPR can produce negative impact for a data controller. Once a right is exercised from the part of a data subject, the controller is obliged to respond. There are only two exceptions to this rule as it is stated in article twelve, paragraph five where GDPR foresees the case where the requests are manifestly unfounded or excessive, in which case the controller can either charge administrative costs or refuse to act on the request. In any case the burden of demonstrating the manifestly unfounded or excessive character of the request lays with the controller.

Accountability

The accountability of the data processor is explained in article's five second paragraph and refers as the responsibility of the controller to demonstrate its compliance with the basic principles of personal data processing.

A word that is essential to the obligations of a data processor and is very often used in the regulation articles and recitals is "demonstrate". According to the regulation there are quite a lot of things that a processor or a controller must demonstrate. Actually there are nineteen appearances of the word in the regulation, as shown in the following table and most of them are part of the accountability of controllers and processors which is required by GDPR.

Num	Recital / Article	Clause
1	R42	the controller should be able to demonstrate that the data subject has given consent to the processing operation
2	R69	It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject

3	R74	the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation
4	R78	In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default
5	R81	The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller
6	R82	In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility
7	R84	The outcome of the assessment should be considered when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation
8	R85	the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons

9	A5	The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’)
10	A7	Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data
11	A11	the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly
12	A24,1	Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation
13	A24,3	Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller
14	A25	An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article

15	A28,3	(the processor) … makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article
16	A28,5	Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article
17	A32	Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article
18	A35	the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned
19	A49	the transfer is made …... by any person who can demonstrate a legitimate interest

TABLE 2. List of demonstrations

According to tables 1 and 2, at a minimum, what we do need in order to ensure the conformity with the regulation are three critical elements. A record of processing activities, a privacy policy and a security policy. Using some variables within those documents we will ensure the needed conformity with the regulation together with the usability from many different entities.

From personal experience gained at the field of conformity and in line with Table 2 demonstrations, there are two more documents needed on top of the three above mentioned, to address most of the conformity issues implied by the GDPR. These will be the transfer to third parties record and the handling of data subjects request records. For the later documents it should be stated that no automation could be used, since data entered is very variable. Any type of document can be used for the above mentioned need of recording information as long as the corresponding records are kept.

As far as the processing records document there are already some examples developed by the national data protection authorities and we will use one of these. For the privacy policy we can produce a general document fit for this purpose and for our security policy we can use a document produced according to the ISO/IEC 27000:2018 family standards[2] and especially to the existed ISO/IEC 27001:2013 standard. In regard to the standard 27001, once mentioned, is good to know and utilize the ISO/IEC 27701:2019 standard which according to ISO site *"This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization"*. This standard extends or includes and specializes within the protected information the personal data.

Conformity Tools

Now that we have established what is needed as far as documentation goes, we will present those documents and we can embed the needed variables.

Record of processing activities

An MS Excel format file would be helpful to include all the appropriate information, derived from the GDPR. As stated before there is a prototype published by the Greek Data Protection Authority which includes 29 columns to be filled with information on each processing. In order for the information to be complete at least 12 of those columns need to be filled. The 12 mandatory fields are in line with the minimum requirements of various articles of the GDPR.

[2] ISO/IEC 27000:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary

Column Identifier	Title	Mandatory
A	Number	YES
B	Business Process Area	YES
C	Purpose of the Processing	YES
D	Link to contract "Joint Controllers"	NO
E	Data subjects' categories	YES
F	Personal data categories	YES
G	Source of data	YES
H	Recipients of data	YES
I	Data retention period (wherever is possible)	NO
J	Data processor (if exists)	NO
K	Link to contract file with data processor	NO
L	Data transfer to third countries (if exists)	NO
M	Legal, basis for transfer (according to articles 45-49 of GDPR)	NO
N	Proof of warranties for international data transfers (if transfer made per art. 49 para. 1 b')	NO
O	Place or system data is stored	YES
P	General description of security measures (wherever is possible)	NO
Q	Link to security policy file	YES
R	Legal basis for processing, according to article 6 of GDPR	YES
S	Overriding legitimate interests for the processing (if the basis for legality is Art. 6 Par. 1, f')	NO
T	Legal basis for special categories of personal data, according to article 9 of GDPR	NO
U	Means for proof of consent (if legal basis is consent)	NO
V	Rights of data subjects	YES
W	Automated processing, including profiling (if applicable)	NO
X	Is Data protection impact assessment required (DPIA) ?	YES
Y	Stage of DPIA (when it is required)	NO
Z	Was Prior Consultation needed ?	NO
AA	Link to DPIA file	NO
AB	Has ever a personal data breach incident occurred ?	NO
AC	Link to Data Breach Incident file	NO

TABLE 3. Columns of Data Processing Activities File

Privacy Policy

A document for providing information to the data subjects can be the Privacy Policy, (ENISA, 2022) sometimes also called Data Policy, Privacy Notice, Data Protection Statement or alike. Since already 2004 Data Protection Working Party from the article29 made recommendations for a multi-layered approach (ARTICLE 29 Data Protection Working Party,2004). In 2017 the same Article 29 Party published new guidelines in accordance with the new requirements in the GDPR and especially those laid in article 12, paragraph 1 where it is stated that *"The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child."* (ARTICLE 29 Data Protection Working Party,2018)

In regard to the recommendations to the multi-layered approach proposed, there is also a discussion among the academic community for breaking down even more the layers of information providing; starting with icons for the first layer of information to data subjects. (L. Edwards and W. Abel, 2014)

For the second layer of information to data subjects a simple written statement is the best approach. Providing accurate data protection information through this written statement is not an easy task, because simplification is necessary so that an average person can understand the information according to the basic principle of transparency, but that simplification must not produce any misunderstandings in regard to the intended processes of his / her personal data.

For the third layer a statement with all details of a particular processing could be used. We may guess that the regulation promotes this kind of layered information if we think that it provides the right to be informed to the data subjects. It would have been an overwhelming task for every data processor, particularly for big organizations, either from the private or the public sector, to produce statements for each one of the processes they are undertake and it will not have been that helpful for the data subjects if they have to read endless pages for information purposes only.

An MS Word file format will be used, running some MACROS, to easily adapt it to different needs of various entities could be used as a privacy policy of the second layer; assuming the first level is information through set of icons, should be of the following format, containing just enough and necessary information. A proposed Privacy Policy follows. The contents themselves of the privacy policy show the effort to comply with the articles of the GDPR in regard with the information to be provided from a data controller to the subjects of the processing's, especially articles 13 and 14 and of course the data subjects' rights in articles 15 to 22.

PRIVACY POLICY CONTENTS

1. Processor Identification

2. Data sources

3. Purpose of Processing

4.Transfers outside of the European Economic Area

5. Lawful basis for processing

6. Data Retention Period

7. Secure Storage and Retention of Data

8. Disclosure of Information

9. What are your rights

    Right of Access

    Right to rectification

    Right to erasure

    Right to restriction of processing

    Right to data portability

    Right of objection

    Right to non-automated individual decision-making including profiling.

10. Our legitimate interests

11. Your interests

12. Submit a Complaint to the DPO

13. Security Policy

14. How you can update your information

15. How you can access your personal information

16. Changes to this Privacy Policy

PRIVACY POLICY TEXT

The COMPANY [FIELD] recognizes and respects the importance of the personal data it processes in its activities and has therefore fully adopted this privacy policy in accordance with the requirements of the General Personal Data Protection Regulation (hereinafter GDPR) 2016/679/EU.

With this statement, the COMPANY wishes to inform persons for whom processes data (data subjects) in what capacity, for what purpose and on what lawful basis it processes information relating to them. This statement will describe the specific personal data, the data categories, and the sources of the data (when the data are not provided by the data subject).

It will further set out:

• the criteria for determining the period of storage of the data subject personal data;

• the ability of the data subject to exercise, the rights of accessibility and rectification and, where appropriate, the rights of erasure;

• restriction and object to the processing and processing by means of automated decision-making process, including profiling;

• the eventual transmission of personal data to a third country or an international organization; and

• the ability of individuals to fill a complaint about any violation of their personal data rights with the Data Protection Authority, as well as the adherence of relevant privacy policies and safeguards by the COMPANY.

To this end, before interacting with the COMPANY website or completing any data collection forms, you are advised to read the following information to learn more about the COMPANY Privacy Policy and how the COMPANY may collect and use your information.

If you have any questions or concerns, if you wish to receive a copy of this statement or wish to exercise any of the following rights pertaining to your personal data, please contact COMPANY Data Protection Officer:

COMPANY

Address: .: [FIELD]

Email: .: [FIELD]

Telephone: .: [FIELD]

1. Processor Identification

COMPANY has its registered office in the above address. COMPANY in the course of its activities processes the personal data of data subjects and is a data controller regulated by the national authority for Personal Data Protection. Our website is hosted with a third party located in .[FIELD], but your information may be stored elsewhere within the EEA depending on the location of the third party's storage facilities. By accessing the COMPANY's website or data collection processes or otherwise engaging with COMPANY, its Officers, employees or designated third parties, you are agreeing to these terms of engagement.

2. Data sources

We collect your personal data from various sources, including:

- Personal data you give us directly

- Personal data which are produced from the execution of our contractual relationship

- Personal data which are produced during the compliance with our legal obligations.

We collect personal information about you when you:

- Contact us for advice or information via the website or telephone

- Make an application to receive a service or product

- Use our website

- Enquire about a job opportunity

- Work for or with the COMPANY

- Exchange business cards or contact details with an employee or Officer of the COMPANY

- Attend one of our informational or consultation events

- Provided by third parties in the course of discharging their legal requirements to us or in the course of an investigation

We do not collect personal data from other sources without your previous notice.

We may collect data about licensees, prospective licensees, job applicants, our current and former employees, suppliers, service providers and expert consultants.

We do not collect any personal data from your accessing the website, except for information that you submit via the various forms accessible on our website. The information collected may include but may not be limited to the following personal information: name, title/position, email address, organization/COMPANY name, business address, business telephone, mobile number, credit card details and billing information, screen name or passwords, opt-in selections, work history, and details of any convictions.

In the future, we may offer users the opportunity to sign up for an email news bulletin, in which case we would collect data from you for that purpose. We will collect information via certain third parties such as Google Analytics in order to enhance and focus improvements on our website for visitors. This will include the downloading of certain forms or documents residing on the COMPANY's website server, and information shared between your computer, Internet Service Provider, browser or other data, with our server.

We will collect any information about the individuals contained in any email, website contact forms or telephone calls between the individuals and the COMPANY.

We collect information from prospective or current licensees that may include employment history, COMPANY director and ownership information, financial information, criminal records, information about reputation and associations, and records of compliance in other jurisdictions.

In the future, we may collect information about you from third parties that we work with for the purposes of providing or delivering licensee benefits, communication and services or general communications. For example, we may wish to send email updates about licensing changes or upcoming deadlines using a third party who is able to deliver 'bulk' emails. Similarly, in the future we may engage a third party to help provide online application systems to process credit card payments and other forms of payment systems. Such third parties would collect information directly from you on our behalf.

These third parties may or may not be located within the European Economic Area (EEA) boundary.

3. Purpose of Processing

We may use your data for the following purposes:

- to provide you with information or advice that you have requested from us
- for general administrative, accounting and licensee registration operations
- for analytical purposes to enable us to develop our website and identify relevant content
- to keep you informed about our services and information that may be of interest to you
- to invite you one of our informational events or consultations
- to process a service or product request
- to process job applications
- to fulfil our obligations as an employer
- to adhere to National and EU law and regulations
- to process payments and collections relating to services or products

- for investigations of issues and complaints

4.Transfers outside of the European Economic Area

Your personal information in the European Economic Area (EEA) is protected by data protection laws, other countries do not necessarily protect your personal information in the same way. The EEA covers all countries in the EU plus Norway, Liechtenstein and Iceland. Under various agreements with regulators outside the EEA, we may transfer personal data of licensees or applicants for licenses outside the EEA. Such transfers may be made on the basis of your consent or as a condition to the service.

5. Lawful basis for processing

In particular, the lawful basis for processing data subject's data are as follows:

- Article 6 par. 1b GDPR permits processing where it is necessary for the performance of a contract to the data subject, are counterparty or in order to take steps at the request of the data subject prior to entering into a contract;

On this basis we rely, for example, for processing personal data during applications or negotiations of any kind of procurement procedure, contract, or commercial agreements for provision of goods or services to the COMPANY by holding and processing the information internally and/or disclosing your data when required by a third party recipient, bank and insurance organization through which we can fulfill our contractual obligations to you.

- Article 6 par. 1c GDPR permits processing where it is necessary for compliance with a legal obligation to which the controller is subject.

This applies to our statutory obligations such as for tax or insurance requirements, and to process license applications and issue licenses for individuals or legal or supply of goods and services related thereto.

- Article 9 par. 2b GDPR permits processing necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorized by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

On this basis we rely, for example, for processing your data in relation to processing of employment applications and holding of COMPANY employee personal information.

6. Data Retention Period

COMPANY retains your personal data for as long as the processing purpose persists, and after its expiration, we lawfully maintain your personal data when it is necessary to comply with a legal obligation under EU or national law (for example, Labor, Tax

Insurance and Administrative Law) as well as in the case where the maintenance is necessary for the foundation, exercise or support of the legal claims of COMPANY.

7. Secure Storage and Retention of Data

• We retain personal data both online in secure servers and offline in paper files. Our website hosting service monitors and maintains updated technology and security protocols for its website to protect data. Data held in paper files or archived offline for general administrative operations is secured and/or destroyed.

• When you give us personal information, we take steps to ensure that it's treated securely and strive to protect it on our internal systems. Our secure server systems encrypt your information. We use Transport Layer Security (TLS) to encrypt and protect email traffic in line with government standards. If you email service does not support TLS, you should be aware that any email we send or receive may not be protected during transit.

• We will also monitor any emails sent to us, including file attachments, for viruses or malicious software. Please be aware that you have a responsibility to ensure that any email you send is within the bounds of the law.

• However, we cannot guarantee that unauthorized third parties such as 'hackers' will never access your information after breaching security measures.

• We will retain your information for as long as is necessary to provide a licensing and regulatory service and for as long as is required for legal (including tax and accounting) purposes.

8. Disclosure of Information

• We will disclose your information to our employees, service providers and expert consultants as necessary to perform their duties and tasks for COMPANY. However, we only disclose the personal information necessary to deliver that service and have a contract in place that requires them to keep your information secure and not to use it for other purposes.

• We will disclose your data or information if required by law, for example by a court order or for the prevention of fraud or another crime. We may send information about you to the police and other parties in the justice system in order for them to investigate, prosecute or otherwise perform their functions.

• Our IT systems support provider acts as a data processor on our behalf. They do not routinely access the data on our systems but may have to provide maintenance and upgrade services which gives them access to the data.

9. What are your rights

Right of Access

You have the right to receive a) confirmation regarding the processing of your data, and b) a copy of your personal data.

Right to rectification

You have the right to obtain from the COMPANY the rectification of inaccurate personal data concerning you, or ask to have incomplete personal data completed, when they are inaccurate.

Right to erasure

You have the right to obtain from the COMPANY the erasure of personal data concerning you, if you no longer wish to have such data processed and if there is no legitimate reason for the COMPANY to retain it as a controller.

In particular, this right shall be exercised:

• when the lawful basis for processing is your consent and you withdraw it, so the data should be deleted if there is no other lawful basis for processing.

• when your personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed or unlawfully processed or if you object to the processing and there are no compelling and legitimate reasons for processing.

It should be noted, however, that this is not an absolute right, as the further retention of personal data by the COMPANY is lawful when necessary for reasons such as compliance with a legal obligation of the COMPANY or the foundation, exercise or support of legal claims.

Right to restriction of processing

As an alternative to the right to erasure and the right to object, you have the right to request that the COMPANY processes your data only in specific cases.

When do you have this right?

When:

- you correctly bring to the attention of the COMPANY the inaccuracy of all or part of your data, and the COMPANY as Controller examines and confirms the inaccuracy

- the processing is unlawful, or

- the data is no longer necessary for the purpose of processing, but you ask the COMPANY to retain it for the exercise and defense of your legal claims,

- You have exercised the right to objection and the COMPANY as a controller is examining the existence of an overriding legal interest therein.

The exercise of this right may be combined with the right to rectification and the right to object.

Specifically,

a) If you request the rectification of your inaccurate data, you may request a restriction of processing for as long as the COMPANY examines the rectification request,

b) If you request the right to objection, you may request at the same time the limitation of the processing for as long as the COMPANY examines the claim.

Right to data portability

You have the right to receive your personal data that has been processed by the COMPANY as a controller in a structured, commonly used and machine-readable format (for example XML, JSON, CSV, etc.). You also have the right to ask the COMPANY to transmit this data to another processor without any objection.

The right to portability can only be exercised by you when all of the following conditions are fulfilled:

• personal data are processed by automated means (printed forms are excluded)

• the lawful basis for processing is either your consent or the performance of a contract to which you are a party (Article 6 (1) (c) of the GDPR);

• It is your own personal data as the data subject that are processed and has been provided by you.

• the exercise of the right does not adversely affect the rights and freedoms of others.

Right of objection

You have the right to oppose, at any time and for reasons related to your particular situation, to the processing of personal data concerning you when the processing is based either on a task performed in the public interest or on where the COMPANY has a legitimate interest, including profiling.

The COMPANY will be required to stop such processing unless it demonstrates imperative and lawful reasons for processing that override your interests, rights and freedoms, or for the foundation, exercise or support of legal claims.

Right to non-automated individual decision-making including profiling.

If the COMPANY needs to make a decision that produces legal effects for you based solely on automated processing the following apply:

• The COMPANY as a controller may lawfully make such a decision only if you have given us your explicit consent or when the decision is necessary for the conclusion or performance of a contract between us or if such a decision is permitted by EU or national law, which provides for appropriate measures to protect the rights of the subject.

• If this decision is made as necessary for the conclusion or performance of a contract between us, namely the COMPANY as a controller and you as the data subject or upon your explicit consent, you have the right to challenge this decision, so that the COMPANY will be obliged to apply measures to protect your rights, ensure human interference in decision-making, or the right to express an opinion and challenge your decision as a subject of the data.

• If the COMPANY intends to perform automated data processing, including profiling, it will provide you, upon receipt of your data (when collected by you) or in a reasonable time (when taken from another source) and the following additional information:

• whether and to what extent automated decision-making takes place, including profiling,

• on the logic followed,

• on the importance and predicted consequences of the processing,

• information on the subject's right to object, which is clearly and separately described from any other information.

• in any case of profiling, you are entitled to limit the processing at any stage,

• The COMPANY will be required to delete the relevant personal data if the basis for profiling is your consent and it is revoked or if you exercise the right to delete its data and if there is no other legal basis for processing in accordance with the provisions of the GDPR Regulation.

10. Our legitimate interests

We believe that all of the purposes we process data are justified on the basis of our legitimate interests in operating the COMPANY, our legal requirements under National and EU law, and our obligations as a responsible employer.

11. Your interests

When we process your personal information for or legitimate interests, we will consider and balance any potential impact on you and your rights under data protection and any other relevant law. Our legitimate interests do not automatically override your interests- we will not use your personal activities for activities where our interests are overridden by the impact on you (unless we have your consent or otherwise required or permitted to by law.)

12. Submit a Complaint to the DPO

If you find that your personal data is being processed unlawfully or your personal data has been violated, provided that you have previously contacted the COMPANY for the matter and you have exercised your rights towards the COMPANY, and you either did not receive a reply within one month either you believe that the answer you received from the COMPANY is inadequate and your issue is not resolved, you can contact the Office of the COMPANY for Personal Data Protection.

13. Security Policy

The COMPANY shall implement appropriate technical and organizational measures according to our Security Policy, to ensure an adequate level of protection of personal data in order to prevent the destruction, loss, alteration during any unauthorized access, disclosure or transmission to a non-entitled person or entity in any way.

In addition to this, the COMPANY has reviewed the contracts it holds with processors to require them to respect your personal data under the GDPR by taking and enforcing measures to secure them from risks of destruction of loss of altered, of unauthorized access to disclosure or transmission to a non-entitled person or entity in any way and by requiring a confidentiality clause.

14. How you can update your information

The accuracy of your information is important to us. If you change your contact details or if you want to update any of the information, we hold on to you, please contact us.

15. How you can access your personal information

You have the right to ask for a copy of the personal information the COMPANY hold relating to you, subject to any contrary provisions of other National or EU law. To do this please contact us by email.

16. Changes to this Privacy Policy

We will keep our Privacy Policy under review and will update it as necessary.

This Privacy Policy was last updated on Wednesday, July 26, 2023

Security Policy

Again an MS Word file will be utilized. This file will be modular since the level of protection is tightly bounded with the processing activities and this is clearly stated on article 32, paragraph 1 of GDPR. *" . . . . . the controller and the processor shall implement* ***appropriate technical and organisational measures to ensure a level of security appropriate to the risk*** *. . . . . .. "*. The "Security Policy" file existence is also mentioned in paragraph 13 of our previous data protection policy.

We already stated that this document should be modular exactly because of the aforementioned article 32 in order to facilitate the term “appropriate” of the article. The Regulation couldn’t be more specific on that considering that the same regulation applies to very small private businesses that they process a minimum amount of personal data like for example an internet store without even a physical establishment, but also to very big public entities that they process tremendous amounts of special categories of personal data as is the case for example of a general public hospital. For this attempt the standards ISO27001 and ISO27002 will be our guides. The following table demonstrates the relevance of our policy with the ISO requirements.

Paragraph Number	Title	ISO Mapping
1	Introduction	Para 4,5,6,7
2	Governance - roles & responsibilities	Para 5,6
3	Human resource security	Para 7
4	Asset management	Para 8
5	Acceptable use of Information Systems	Para 8
6	Operating systems and application security	Para12
7	Network and communication security	Para13
8	Antimalware - Protection from malicious software	Para12
9	Access control	Para 9
10	Third parties security management	Para15
11	Password management	Para 9
12	Operational audit security controls	Para12
13	Physical and environmental security	Para11
14	Information security Incidents and Events Management	Para16
15	Business Continuity Management (BCM)	Para17
16	Supply, Development and Maintenance of Information Systems	Para14
17	Change and configuration management	Para16
18	Compliance and deviations from policy	Para18
19	Cryptography	Para10

TABLE 4. Security Policy Paragraphs to ISO Mapping

The security policy will be constructed following the structure of the standards mentioned and then the data controller will have the option to include or exclude certain paragraphs of the policy which they may or may not apply to its business processes. In order to assist the interested parties we can provide a matrix to help them choose the needed paragraphs for the creation of their custom security policy.

The proposed matrix contains all the paragraphs included in a complete security policy and the categorization of the business unit. For the categorization five different types of businesses are included and coded with VSB (Very Small Business) which they process personal data of mostly only their personnel, SB (Small Business) which they process personal data of mostly their personnel, very few of their customers and perhaps very few of special category, MB (Medium Business) which they process personal data of mostly their personnel, some of their customers and perhaps some of special category, BB (Big Business) which they process personal data of their personnel, and of their customers and many of them are of special category and SBB (Special Big Business) which they process many personal data of special category.

Paragraph Number	Security Policy Paragraphs Titles	Risk Surface				
		VSB Only Personnel	**SB** Mostly Personnel, Very Few Customers, Very few special	**MB** Mostly Personnel, Few Customers, few special	**BB** Personnel, Customers, Special	**SBB** Mostly special categories
1	Introduction	√	√	√	√	√
2	Governance - roles & responsibilities		√	√	√	√
3	Human resource security			√	√	√
4	Asset management	√	√	√	√	√
5	Acceptable use of Information Systems	√	√	√	√	√
6	Operating systems and application security		√	√	√	√
7	Network and communication security	√	√	√	√	√
8	Antimalware - Protection from malicious software	√	√	√	√	√
9	Access control	√	√	√	√	√

10	Third parties security management			√	√	√
11	Password management	√	√	√	√	√
12	Operational audit security controls				√	√
13	Physical and environmental security		√	√	√	√
14	Information security Incidents and Events Management		√	√	√	√
15	Business Continuity Management (BCM)			√	√	√
16	Supply, Development and Maintenance of Information Systems					√
17	Change and configuration management			√	√	√
18	Compliance and deviations from policy	√	√	√	√	√
19	Cryptography			√	√	√
	Total Paragraphs to be Utilized	**8**	**12**	**17**	**18**	**19**

TABLE 5. Matrix for Security Policy Paragraphs

Now we will produce our security policy, starting with its contents, followed with the policy wording.

SECURITY POLICY CONTENTS

Contents

SECURITY POLICY TEXT

1. Introduction - Document Purpose

This document is the official Information Security Policy of the Company which is based on best information security practices and serves as a single security guide for proper use of information, data and information systems. Effort is made to align the policy with the International Standard of Information Technology – Information Security Techniques

(ISO/IEC 27001:2013).

Its aim is to define the purpose, direction, principles, processes and basic rules for information security management and define the necessary security requirements, measures and controls in order to ensure the confidentiality, integrity and availability of the information, data and operational resources of the Company.

Users of this document are all Company employees, as well as relevant external parties.

The establishment of a security system is influenced by the Company's strategic objectives and priorities, the security requirements, the organizational processes used, the organizational structure - factors which are expected to change over time as well as the legal compliance requirements.

It is expected that the establishment and implementation of the security system will be:

- scaled in accordance with the needs of the organization,
- tightly integrated with the Company's process landscape and its organizational structure and,
- continually improved.

The information security policy is a very important factor in the ability of the Company to work seamlessly and support its operational activities. In addition, the development and implementation of the information security policy contributes to compliance with the specific requirements of Company independence, transparency and confidentiality arising from the regulatory and legal framework governing the Company's operation.

The development and maintenance of this information security policy aims to:

- Serve as a point of reference for all matters directly or indirectly related to information and data security.
- Provide guidance in the selection and implementation of security measures and countermeasures.
- Strengthen the "channels of communication" between the parties.
- Secure and manage resources.
- Consolidate the importance of security of Information and Information Systems.
- Assist in growing a "security and privacy culture and philosophy" on the human factor.
- Ensure the confidentiality, integrity and availability of commercially sensitive information and private data in the Company's systems, and in systems that manage such information.
- Ensure commitment to continual improvement of the security system.

The information security policy identifies the roles, responsibilities and competencies of members of the Company directly related to its implementation, and must be applied to all departments at Company, all users of Information Systems, employees, permanent and temporary staff. In addition, it is applicable to all equipment, systems and information located on the property of or used by the Company. Every division or department head of the Company is responsible for the application of the ISMS and this policy within his/her division / department.

2. Governance - roles & responsibilities

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated. Specifically, top management shall assign the responsibility and authority to Company staff for:

- ensuring that the requirements outlined in this policy are met.
- reporting on the performance of this policy

The Company at regular intervals and no later than annually or in cases of significant changes will review and revise the information security policy, so as to ensure the following:

- Alignment with Company's strategy.
- The adequacy of the protective measures foreseen in relation to the risks facing computer and information systems.
- Compliance with regulatory requirements

During the review all elements that contribute to the formation of an integrated picture of the operational environment and information systems of the Company during the current period will be considered.

Specific elements to be considered are:

- The current situation and the level of preventive and remedial security measures.
- The results of previous security checks made by the administration or by independent bodies.
- The recommendations regarding the proper implementation of the compliance program of Company information security policy, to remain aligned with the regulatory requirements.
- Logging of changes made since the previous review of the policy (changes in business processes, legislative and supervisory framework, in technical equipment and staff).
- The analysis of possible risks.
- The evaluation of modern methods of attack in information systems for the integrated approach to security threats and vulnerabilities.
- Reports about incidents of a security breach of Information Systems.

2.1. Organizational structure

The existence and operation of a specific organizational structure for integrated and successful treatment of all systems and information security issues, is essential. The organizational structure and its general functioning should be based on specific roles and security responsibilities.

This section outlines general principles and rules relating to the organizational structure and management organizational matters related to the security of information systems. It is underlined that the following roles do not represent positions of administrative responsibility at Company organization, but broader organizational roles and responsibilities assigned to employees and executives of Company. The main roles that are related to data security and information systems, are described in the following sections.

2.1.1. Information security officer

A Company employee whose main responsibilities are:

- Management of the information security framework.
- Provide recommendations for the improvement of the information security policy and ensure the enforcement of any changes.

- Determination of information security requirements, in cooperation with relevant departments of the Company.
- Review the information security policy and submit proposals on information systems security.
- Contribution in addressing information security-related events and ensure that all issues are resolved in an acceptable period of time, in compliance with the information security requirements.
- Contribution to the implementation of appropriate security measures and monitor these for timely and immediate handling of any incidents.
- Contribution to security checks, including risk assessments and Vulnerability Assessments in collaboration with their respective managers, responsible for continuous monitoring and improvement of the security policy and the overall level of security of Company.
- Update and staff training regarding the security of information and information systems.
- Presentation of specific and comprehensive proposals for resolving shortcomings or risk reduction proposals.
- Information from the information owners on the flow of confidential information and check that confidential information is handled as specified by the information security policy and the Classification Information policy of the Company.

At regular intervals or in cases of significant changes, the Information Security Officer and the Company, will review and revise the information security policy so as to ensure the following:

- Its alignment with the business needs and the business strategy.
- The adequacy of the protective measures foreseen in relation to the risks facing computers and information systems, in collaboration with those responsible for critical infrastructure.
- Compliance with the requirements of the regulatory framework that governs the Company, in collaboration with the Legal Department.
- Compliance with the requirements arising from the above- mentioned regulatory framework, through the implementation of appropriate measures and controls laid down by the information security policy.

The Information Security Officer is also responsible for:

- The implementation and maintenance of the information security policy.
- Communicating this policy to users of information systems of the Company to raise their awareness. In addition, the security policy should be communicated to all partners, who have a permanent and stable relationship/cooperation with the Company.
- Ensuring, through the Company and other units, that the information systems and their use shall provide sufficient security control mechanisms considering the functionality of the systems and the risks facing them. Specifically, ensure that appropriate measures have been taken to protect information from risks such as unauthorized access or modification, alteration, destruction, disclosure to third parties, etc.

2.1.2. Information owner

The information owner is the Company member of staff that creates or initiates the creation of information and bears overall responsibility for the management and control of information as described in the Classification Information Policy of the Company.

Responsible Owner of information is the senior executive level in the hierarchy of each department/function/unit. The responsibilities of information owners are:

- Detect and fix hazards/risks and characteristics of individual information (data, documents) managed by the unit and information classification based on the established principles and rules of the Classification Information Policy.
- Specification of requirements and standards for security, access, retention and disposal of information arising from this policy, for the information managed by each unit.
- Cooperation with the respective departments on the design, development and review policies regarding the security of information systems, as defined in this policy.
- Care for the unit's compliance with the Classification Information Policy as applicable.
- Helps to facilitate controls on the application of the policy carried out in accordance with the Classification Information Policy and ensure the incorporation of comments arising during assessment controls.
- Update of information classification when and where needed, and problem solving in applying this policy due to force majeure.

In case information and/or data is managed by more than one unit within the execution of their duties, the owner of information defined by the unit bears ultimate responsibility for information use and management. The owners of information, in the context of the information security policy, cooperate with the information security officer in the design, development and review of the information systems security and other policies regarding the security of information systems and in particular for:

- The classification of systems based on the confidentiality of information they manage, their integrity and their criticality.
- Ensure that the security measures that surround the systems are adequate and consistent with the information security policy and ensure the appropriate way to access and manage information according to its classification, in accordance with the Classification Information Policy, with particular emphasis on ensuring the confidentiality of sensitive information.
- Ensure that all procedures related to information systems managing information are distinct, recorded, accurate and up to date.

An official list of Owners of information per system or per data item should be maintained.

2.1.3. Administrator

An administrator is an official who is charged with overall management responsibilities of computer / information systems of the Company. The responsible administrator shall cooperate with the Information Security Officer and any administrators of individual networks, systems and applications, to enforce security.

Some of the key responsibilities regarding the security of information systems are:

- Maintaining security backup (back-ups).
- Enabling security configuration in the systems (operating systems, applications, databases, networks) on the basis of individual processes.
- The application of information security policy and supporting processes.

- Tackling security events.
- The upgrade of systems based on the latest versions of security (updates, patches, hotfixes, versions).
- Monitoring and maintenance of information security systems (e.g. Antivirus, IPS, network monitoring software, monitoring tools, etc.).

3. Human resource security

Human resource (HR) is the most important organizational asset and at the same time it can become its greatest threat. This policy outlines the activities that need to be performed before, during, upon termination or change of the contract, agreement.

3.1. Prior to employment

The objective is to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

- The HR department should always carry out a screening process including background verification checks on all candidates for employment or contractors in accordance with applicable laws, regulations and ethics.
- Verification checks should be proportional to the Company's operational requirements, the classification of the information to be accessed and the perceived risks. It should consider all relevant privacy, protection of personally identifiable information and employment-based legislation and where permitted include any other check i.e. accuracy and completeness of applicant's curriculum vitae, criminal records.
- When someone is hired for a specific information security role the Company should ensure that the candidate has the necessary competence to perform the security role and can be trusted to take on the role.
- The contractual agreements with employees and contractors should state their and the Company's responsibility for information security.

3.2. During employment

The objective is to ensure that employees and contractors are aware of and fulfil their information security responsibilities.

- Management should require all employees and contractors to apply information security in accordance with the established organisational policies, processes and procedures. Management should act as role model and should demonstrate support of information security policies, processes and procedures.
- All Company employees, and where relevant, contractors should receive appropriate awareness education and training in organisational policies, processes and procedures relevant for their duties and job function. An information security awareness program should be planned and established in line with the policies included in this document and their supporting processes, aiming at making employees aware of their responsibilities for information security and the means by which those responsibilities will be discharged.
- The Company should establish a formal and communicated disciplinary process to take action against employees who have committed an information security breach.

3.3. Termination and change of employment

The objective is to protect the Company's interests as part of the process of changing or terminating employment.

- Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced.
- Any responsibilities or duties still valid after termination should be included in the employee's or contractor's terms and conditions of employment.

4. Asset management

The objective of this protocol is to define guidelines for the protection and proper management of the Company's tangible and intangible information assets. All information assets must be recorded in an inventory of assets or asset registry and have an owner who will be responsible for their protection and maintenance.

4.1. Inventory of Assets and Asset Ownership

The aim is to identify and maintain organizational assets associated with information and information processing facilities and define appropriate protection responsibilities.

- All assets (tangible and intangible) should be identified, and a process should be in place for such purpose.
- An Asset Inventory or Registry should be created which should be accurate, consistent, up to date and aligned with other inventories i.e. asset inventory kept for accounting purposes. For more effective and efficient asset identification and management purposes, each asset should bear an Id or Asset Code as the one kept in the Company's accounting system.
- Assets identified and recorded should be relevant to the Company's information lifecycle and include creation, processing, storage, transmission, deletion, and destruction.
- Assets recorded and maintained in the inventory / registry should be owned by Company resources having approved management responsibility for the asset lifecycle.
- A process should be in place to assign asset ownership upon identification and creation of assets.
- The Asset Owner should be responsible for the proper management of an asset over the whole asset lifecycle including:
- The classification of assets in accordance with the requirements of the Information Classification policy.
- The maintenance of the asset inventory / register. In the case of information systems and software applications the inventory should be maintained in collaboration with the Company's IT department.
- Safeguarding the protection, availability, operation, integrity and confidentiality of the assets

4.2. Information Classification

The purpose of this paragraph is to ensure that information within the Company receives an appropriate level of protection in accordance with its importance to the Company.

Information managed and administered by the Company should be protected according to the classification they have throughout their life cycle, from creation to destruction. Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

Information managed by Company is classified according to the Information Classification Policy, which aims to establish principles and rules and create the mechanism to ensure the proper management and protection of the confidentiality of the information managed by Company relating both to commercially sensitive information obtained by Company during the performance of his duties and other information and data that support its operation.

5. Acceptable use of Information Systems

All users of the Company's Information Systems are responsible to protect Company information in both printed and electronic form and be accountable for every action that is contrary to the requirements set out in this policy document.

Furthermore, users of Information Systems are responsible for maintaining the confidentiality of sensitive information managed by the Company. At the same time, users of Information Systems are allowed to make use of application systems and technological infrastructure for operational purposes, always within the context of their responsibilities and duties.

5.1. Use and protection of information

Any use of Company information that falls within the following categories is prohibited:

- Use of information that may cause any form of loss/damage to Company (e.g. loss of reputation, reduce profitability, fraud, etc.).
- Use information that prevents the business and development.

5.2. Acceptable Internet usage

The Internet service offered by the Company to its employees is intended for servicing on corporate functions and in carrying out their operational duties. More specifically, all users of Information Systems should comply with the following safe use of Internet services:

- Minimize the use of the Internet for personal reasons, except in cases where there is an operational need and subject to approval by the Information Security Officer.
- Minimize the use "online news" (messengers, chat rooms, etc.), except in cases where there is an operational need and subject to approval by the Information Security Officer.
- Access is denied to non-acceptable websites based on their content and management decision.
- May not post any information in corporate Internet sites without formal approval from the owners of information.

- Update of the pages of the website is exercised under the responsibility of the responsible internal units/departments and the information page owner's approval.

User access at Internet Services Web pages should not be taken for granted. The selection of the scope and nature of Web pages that allow access is an exclusive right of the Company who may modify the corresponding access policy in order to reduce the risks, or to conform to regulatory requirements that govern its operation.

It should be noted that the ability to link to websites of non-relevant content to Company operations, does not imply that access is permitted by the Company.

More specifically, web categories considered to contravene the acceptable use policy are as follows:

- Sexual Content.
- Content security mechanisms violation (Anonymous Proxies, Proxy Bypass, Hacking etc.).
- Personal dating (personals) & news websites (Chat).
- Criminal content, offensive content and violence content.
- Sale and advertising-drugs, firearms, drugs, alcohol, cigarettes etc-gaming, gambling, computer games.
- Purchase of Clothing and grooming products.
- Job Search.
- Religious, racial and political content.
- Sports content.
- Audio and Video Downloads in real time (Streaming Media).

Information Security officer should maintain a list of categories of Web sites or individual Web pages to which access is denied to users of the Company's Information Systems.

5.3. Acceptable use of e-mail

The email service offered by the Company to its employees is intended for servicing on corporate functions only and in carrying out their operational duties. However, due to the possibility of easy and widespread data transfer, file and information, use of the e-mail system should be carried out with due care.

More specifically, each user of Information Systems that access and uses the e-mail system should be aware of their responsibilities and comply with the requirements, as described in this section. For the security of e-mail services, the following is a list of requirements for the Company:

- Outgoing information messages of Confidential nature or that will be entered into Company e-mail upon approval by the responsible Owner information.
- Sensitive information of users of the Company's information systems or any 3rd parties will be handled via e-mail upon approval of the Owner only to appropriate information and to access this information by authorized persons. If the owner finds it necessary, the correspondence will be encrypted properly with appropriate encryption and restrict access, depending on the level of classification of the information contained therein.
- Use of company e-mail for personal purposes should be avoided.
- E-mail Distribution Lists that may be created by the administrator of the e-mail system, upon official request, must have the approval of the responsible Owner Information.

- Anti-virus protection must be enabled for e-mail systems, and it should always be updated with latest virus definitions / engines. All incoming and outgoing emails must be checked by the antivirus software that is pre-installed.
- There is a number of file types that are considered suspects or dangerous for transport of viruses and other malicious programs and must be controlled and prevented from sending/receiving. Examples are files with extension exe, mpeg, avi, rm, qtm, wav, mp3, midi, aif, au, voc, dll, reg.
- It is prohibited to send or forward spam messages and chain mails.
- Users of Information Systems should be informed about incidents of Phishing via email messages.
- Sending or forwarding spam messages and chain mails is forbidden.
- Social engineering attempts through e-mail to the elicitation of information from unsuspected users about Information Systems Company - must be prevented and if detected to inform the Company.
- Upon user resignation, user accounts should be removed immediately. For this reason, human resources management directly informs Company staff.
- Users need to check the recipient list before sending e-mail messages to verify that only authorized persons will have access to specific information.
- It is prohibited to send e-mail messages with intimidating or hateful content, or offensive material for people with regard to their sex, race, color, religion, political beliefs, nationality, sexual orientation or potential disabilities. In General, it is prohibited to send or forward messages of advertising, political and religious content.
- It is prohibited to send or forward file and software of questionable origin or material that is contrary to regulations and copyright obligations.
- It is forbidden to read emails and especially use the attached material derived from an unknown sender.
- It is prohibited to send electronic messages without disclaimer.
- Company specifies the size of the messages exchanged and the allowable size of user mailboxes depending on the requirements of each Information Systems user for the accomplishment of the tasks set.
- Any user of Information Systems becomes aware of malicious use of the email system, must follow the procedure described in Management of Security Incidents section.

5.4. Use of fax, photocopy and telephony

Fax, photocopy machines and telephones will be used for the daily activities of official functions of the Company and not for personal purposes.

Particular attention should be applied when sending and/or copying of sensitive and critical data and information and especially with regard to commercially sensitive information of users and any 3rd parties.

Specifically, Company employees should:

- Check the equipment at the end of each working day so that there are no exposed documents and information (e.g. task execution fax reports)
- When sending a fax, and especially for sensitive and critical information, the sender must take care of receiving and safekeeping receipt of successful receipt. Third parties (external partners, providers, supervisors) are forbidden to use Fax equipment and/or

Photocopy without the approval and supervision of a Company employee.
- Use telephony services, especially phone calls with increased costs, in accordance with Company's policies.
- It is forbidden to photograph undisclosed of confidential information or Company premises.
- In addition to the above, in the case of commercially sensitive information of market participants, sending them by fax is permitted only upon approval of the information owner and only to authorized persons.

5.5. Software licenses and use of non-approved Software

The Software License agreements should not be violated. For this reason users of Information Systems should treat all kinds of software in accordance with the terms of the software license. Specifically it is prohibited any kind of use, installation, software copy that is not in accordance with its license agreement. Additionally, all users shall consider that every software is subject to copyright, unless there is a specific statement that clearly expresses the opposite.

It is strictly forbidden any use and/or installation of unapproved software or equipment in the Company technological environment. Unauthorized software and equipment is considered each program and system that does not belong to the Company and that has not been installed by the responsible Company staff. Company will need to maintain a file of software usage approved by Company. Installation rights are controlled from Active Directory (all permissions to end-users to install software are removed), except when there is an operational necessity and upon approval by the people in charge of the operational department and Company.

5.6. Personal computer Users security rules (Desktop Policy)

The following section describes the security rules that must be followed by end-users when using their personal computer:

- All PCs are subject to the security of one or more active corporate directories or other similar outline infrastructure users.
- End-users should not have local administrator rights on their computers. In case it is needed (e.g. due to use of certain applications), it should be given official approval by the people in charge of the operational department and Company.
- Software installation, beyond authorized and approved by Company is prohibited. Company reserves the right to perform checks for installed software.
- Each user has personal responsibility for software installed on his/her personal computer.
- It is strictly forbidden to use a modem or any other form of communications interface with the Internet or other external network, unless this has been explicitly approved by Company.
- Screen saver should be activated after 5 minutes of inactivity on the computer and passwords should be required to restore the computer to function.
- Laptops should be stored in a secure location after the end of work and when not in use.
- Users do not have the right to deactivate antivirus / malware protection programs.
- The ability to execute DOS commands (commands) should be disabled, except when

there is an operational necessity and upon approval by the people in charge of the operational Department and Company.

End-users will be informed dully by Company with the latest developments regarding obligations and rules of security related to the use of Company information systems.

5.7. General use of information systems and equipment

- Staff should not use information systems and equipment that does not belong to Company inside the company's premises, without prior approval by Company.
- It is prohibited to install software or change equipment in Company information systems without the prior approval from Company. Any additions considered necessary will be carried out by the responsible staff from Company.
- Users of Information Systems have no right and should not read, modify, delete, or copy a file that belongs to another user without the approval of the responsible information Owner. The ability to read, modify, delete or copy files that belong to other users does not imply license to perform these activities.
- It is strictly forbidden any intentional behavior that can adversely affect the proper and continuous functioning of Company information systems.
- It is strictly forbidden any attempt to bypass control and protection mechanisms that have been enabled by Company on information and networking systems and applications.
- It is prohibited to attempt to obtain unauthorized access to Company information systems or third parties.
- No staff should possess or disable passwords, cryptographic keys, or any other access control mechanism which could enable unauthorized access to information systems.

6. Operating systems and application security

The purpose of this section is to identify security requirements on operating systems, databases and applications used in Company and ensure that they are properly parameterized in terms of security, managing and protecting from unauthorized access. The term ‘system’ means the operating systems, databases and applications of Company.

The following general rules for systems customization should be followed for all operating systems, databases and applications of Company:

- Services and applications which are not used should be deleted or disabled.
- The latest updates and patches must be installed in the system after they become available (time of application will depend on criticality of issues involved), if this procedure does not affect the smooth operation of the system and does not violate the operational requirements. Before installing security versions they will be checked with the software manufacturer for compatibility issues with the systems used by the organization.
- Accounts with high rights (root or admin) must not be used for actions that may be carried out with low account lower allowances.
- Use of administrator accounts and users with high access rights (root or admin) should be limited.

Company should maintain the official list which describes Company applications, business operations, technical characteristics (OS, databases, network, and communication links), business managers, managers of information technology and the physical location of the IT infrastructure.

There should exist and be kept official documents by type of technology (e.g., Unix, Windows, SQL, Oracle, SAP), which describe the basic security parameters that are enabled (hardening).

7. Network and communication security

The transportation and handling of data and information, and system and application software is one of the most crucial Company functions to achieve day-to-day work. Consequently, the design and operation of network infrastructure to ensure high performance, reliability and user access control is a top priority.

Security settings to achieve security of the communications network, including wireless networks are described in the following paragraphs.

The aim of this section is to outline the framework of protection measures (principles and rules), which relate to the security of information handled internally through Company data network (Enterprise Network) from/to external bodies.

7.1. Network architecture

The network infrastructure design and the determination of security requirements is essential for adequate and effective protection of information processed in Company systems. There should exist and be maintained, updated topologies / network diagrams. These documents contain highly confidential information for network security. Simplified diagrams without technical details may be given to external partners. These documents could include:

- Topographical network diagrams by area/facilities.
- Physical network topology Diagrams.
- Internal network diagram (network equipment and registered IP addresses).
- Chart on foreign networks (network equipment and registered IP addresses).
- Circuits (name, service, source/destination determination, applications that use alternative routes).
- Devices (provider, model, serial number, settings, criticality).
- Wiring (type, origin/destination, alternative routes, details of conservation).

The design of network architecture must include and be based on the following:

- Facilitate the development and interconnection with other networks through appropriate planning and on the basis of known capacity and bandwidth requirements, so that the selected network technologies can manage existing Web traffic and tolerate with increased volume in case of network expansion.
- The combination of static and dynamic routing methods, to ensure easy handling and routers fault tolerance.
- Where applicable, main network devices should perform the function for which they were supplied, while nonessential services and functions they can perform should be disabled or deleted.
- Use of separate sub-networks, which are protected through rules (e.g. use of routers with access control lists ACLs).

- The grouping of common servers, in order to achieve better management of network traffic.
- The limitation of network entry points to what is strictly necessary to achieve Company operational objectives.
- The use of designated and approved access and communication ports.
- The use of identification mechanisms for specific services, whether based on IP addresses or a combination of username-password.
- Enable of network management reports and maintenance logs.

7.2. Network resilience

The communications infrastructure and devices that have crucial role in the continuity of network services must be identified and recorded, so that appropriate measures be taken to limit the points of failure and thus limit the risk of malfunctioning equipment, critical links and services.

Methods for limiting points of failure:

- Automatic re-routing of communications in case critical points fails, so re-route traffic and to respond to changes in the network infrastructure or corresponding technology.
- Critical connections/communication routing through more than one external centers.
- Provide duplicated or alternative secure network devices, such as switches, firewalls, gateways.
- Existence of alternative power supply.
- Fallback Mechanisms for re-route through alternative channels of communication.

7.3. Segregation

A very common method of controlling the security grids are dividing them into isolated logical network domains each of which is protected by a predefined 'security zone' (security perimeter), created through a firewall. The distribution of Company network should rely on access control requirements, incorporating appropriate technologies (network routing or gateways). However, it should also be considered the incurred cost and effects on network performance. Division of the network into isolated logical domains must be based on virtual local area networks (VLANs), as for example in groups of information services, and information systems.

7.4. Network traffic and Access control

The network access to Company must be controlled through compulsory routes, certification and identification methods, separation of networks, routing and filtering controls. It is also needed to use network access control zones (DMZ) where devices that need access from different networks are placed.

Especially for systems open to the Internet to provide Web services (e.g. Websites, eMail, VPN, etc.), special care should be taken to operate only in the specific areas of the Company network (DMZ), managed by Company.

The minimum acceptable requirements for the recognition of Information Systems users include using a combination of unique user ID and password. The internal addressing plan should not be visible from external links.

7.5. Configuration/settings of network devices

All critical devices (router, switches, firewalls, IPSs) should be properly parameterized so as not to endanger the security of the network. In addition, use of network devices must comply with the manufacturer's instructions as well as with those of security policy and non-essential services should be disabled. In addition, they should be regulated so as to inform about network overload conditions or other specific situations, problems or possible breaches.

7.6. Filtering

To ensure that undesired or unauthorized traffic is not allowed on the network, the traffic will be routed through specific filtering devices, such as routers with functions for filtering, application proxies/firewalls, IPS. These devices need to filter specific types of packets and to prevent the transmission of specific types who are suspected or dangerous.

Filtering should be based on a set of rules, identified, documented and approved. Filtering should be based on minimum access logic, developed by certified staff and inspected by Company. All relevant details will be updated on the basis of the requirements of the information security policy and be confirmed to ensure their accuracy. Any changes will be subject to specific change processes.

7.7. Network security

Network checks will be carried out periodically to detect vulnerable systems in known vulnerabilities (reviews of vulnerabilities). All scanning and detection activities are coordinated by the Company, in collaboration with the managers of the systems or applications. In addition, the responsible managers will be asked to correct or to implement specific security measures in cases weaknesses are pinpointed in networked systems.

On a per case base, and if required, apart from vulnerabilities assessments, penetration tests should be performed in the network infrastructure to determine the range and threats from malicious internal or external users. Penetration tests provide a more realistic assessment of risks, using real-world scenarios of attacks and exploits tests to accurately assess the risk.

8. Antimalware - Protection from malicious software

8.1. Requirements

All user systems linked with Company network should have antivirus software (Antivirus), properly installed, parameterized, enabled, and updated with the latest virus definitions before connecting to the network, except in cases where the use of such software is preventing the proper functioning of the system for achieving business goals. In any case

Company should approve not using antivirus software on any system.

Users should not have the ability to disable services. If antivirus software is inoperative for any reason, users should activate and perform a full scan of the system before using it. The responsible system administrator dealing with malware should check daily proper operation of the system, operation of the software in all necessary informational resources and record any security incidents associated with malicious software.

To prevent the spread of viruses on the network, computers that are infected by viruses or other forms of malicious code, are disconnected from the network until virus is/are removed.

The following rules and requirements must be kept strictly:

- Virus definitions should be updated daily, automatically.
- All files on all hard drives should be scanned periodically.
- All portable media (CD/DVD, USBs, etc.) must be scanned and checked for viruses.
- Protection against viruses, must be enabled for e-mail systems, and should always be updated with latest virus definitions.
- All attachments of electronic messages (incoming and outgoing) should be scanned for viruses (from e-mail server) before sending to final recipients.
- There are a number of file types that should be blocked from sending/receiving who are considered as suspects or dangerous for transport of viruses and other malicious programs.
- Company reserves the right to prevent the arrival of incoming electronic messages that exhibit characteristics of bulk mail, viruses, trojans or anything else that could threaten the services or the network infrastructure.
- The parameter "real-time virus scan" (or equivalent function) should, where possible, be triggered when accessing files.
- Any data or programs from external sources, need to be scanned before they can be used by users Information Systems.
- Antivirus software must be installed by Company and configured to provide continuous virus scanning, as well as periodic updates (automatic periodic facilities the latest updates of virus definitions).
- The functions and operations of antivirus must be configured centrally.
- Antivirus programs must be constantly active on all hosts of local area networks (LAN) and personal computers (PCs) which are connected to the Company network. Excluded are systems that are not compatible with the use of antivirus software, for which Company should be aware and record and monitor extensively.

When an attack from malware is detected and is spreading Company should inform all users to exercise caution. In this case, each user will need to enable the Antivirus software to scan all files on all hard disks, using the latest available virus definitions updates, as defined in **"Security Event Management".**

8.2. Third party software management

Third party data and programs (external partners, etc.) must be loaded in a particular isolated system (test), which can be monitored and detected for viruses or other malicious programs, before they settle on other systems on Company network. Visitors’ laptops should have been updated (Antivirus) and tested before using them on the internal network.

9. Access control

The purpose of this policy is to establish a set of security requirements concerning connection and access to systems and applications.

Access to systems and applications must be approved and implemented only if there is a business need and always on the basis of the principles of:

- “need to know / minimum necessary knowledge” and
- “least privilege”.

Access should be granted only to the set of information that requires a person to perform his/her work. Also, access to systems and applications should in any case take account of the classification of related information and systems.

Additionally, for systems and applications for which access is granted to users of Company, access will be granted subject to similar terms and conditions. In any case any provision of access to the above, should ensure the confidentiality, availability and integrity of commercially sensitive information.

9.1. Access Procedure

The following procedure should be followed to grant access rights to all users of information systems. Access to systems and applications is determined upon recruitment of employees to work for the Company (see Human Resources procedures). Upon completion of recruitment procedures, Human Resources informs the user for his/her obligations and rights with regard to security and then notifies the Company through e-mail for the recruitment and placement of the new user.

Specifically:

- Hiring and Update about responsibilities and rights in information systems use. User notification about security aspects.
- Human Resources notifies Company through e-mail about the placement of the new employee.
- The responsible unit's Owner Information completes the form in which identifies applications and specific access rights authorized to have under the operational role and the principle of separation of duties. The user access to Information Systems must be approved by the head of each unit.
- Request is sent to the address of Company for analysis and implementation. Company analyzes and implements the request providing unless technical or other problem arises.

Furthermore the following rules must be followed in the application, analysis and grant of access rights:

- Regarding access rights to operating systems, Company has the responsibility to determine the categories of users and the access rights at operating system level information systems/infrastructure.
- Permission to manage, change settings and maintenance of information systems should be given only to authorized personnel.
- Especially for external partners or other third parties the adoption provision of access to the systems must be recorded and supplied by the relevant Information Owner that has direct cooperation with external partners. The access should always be terminated upon the completion of the tasks assigned.

This is the main process to grant accesses rights to Company systems. A similar process is followed when an employee changes organizational unit / role.

In order to give authorization to extra access privileges to a user a relevant application from the respective information owner should be submitted. To access central systems of the computerization infrastructure, approval must be given by Company.

In case of temporary need for extra rights (e.g. specific task or assignment) and access to third parties, the respective manager should notify Company about the end of the work in order to terminate the access.

Upon user resignation, Human Resources should inform Company in order to take the necessary actions and to remove that user's access.

In all cases, update must be done under formal procedures (e-mail notification), using appropriate forms.

9.2. Access with administrator privileges and User Accounts with administrative privileges

User accounts with administrative privileges should be strictly limited to persons who are directly responsible for the management of systems and/or their security. Accounts with administrative rights systems should, where practicable, be limited to two people per informational system, while in each case the required separation of responsibilities of administrators should be applied. An official file should be maintained with the respective managers of information systems. The default names of administrator’s accounts should always be changed. In systems necessary to have more than two accounts, the approval of Company is required.

9.3. Access with administrator privileges and Access rights control procedure

The access rights for all users of Information Systems should be reviewed on an annual basis from Information owners. Particular attention should be given to cases having access rights that are not consistent with the operational responsibilities of the privileged accounts and user accounts. System administrators must keep records of all applicable access rights. This file will be checked and will be reviewed by Company.

The existence of systems and applications which are able to bypass the access checks must be limited and monitored/controlled accordingly. System administrators must keep a detailed log of such cases, including the relevant explanations and necessary approvals.

Functional testing of systems and predefined checks must be carried out regularly, as described in the Operational Audit Security Controls section to ensure data integrity.

10. Third parties’ security management

10.1. Third parties and requirements

The interconnection of Company with any third company and/or external partner should be implemented only if there is official documentation of the business necessity.

The minimum requirements and security standards in regard to network links of third parties (including those of suppliers, cooperating institutions and companies) to Company network and their access to it, as well as links from Company network to networks of third parties are:

- Security Survey: Every new connection with Company infrastructure must pass through security screening and get approval. Security checks are used to assure that all accesses comply with the security requirements and the principle of minimum access.
- Interconnection Agreement with Third Parties: All new connections between third parties and Company presuppose that the representatives of the Parties and Company have agreed.
- Interconnection Procedure with Third Parties: all practicing third party connections must be accompanied by a valid business justification, written and approved by Company and the information owners.
- Point of Contact (for third parties): Third parties must identify a person who will be the contact person for their connection with Company. If the contact person changes, Company should be informed immediately.
- Services offered: list of services or access provided to Third Parties, should be agreed in detail on both sides, be posted clearly and be signed in agreement with the third parties. If public networks (e.g. the Internet) are used for the exchange of information encryption mechanisms should be used (e.g. VPN). Third parties must handle the data with at least the same privacy level with that applied in Company. For this purpose Company legal service should arrange for the signature of appropriate agreements.

10.2. Interconnection creation

All units that need a new interconnection should apply to Company. Each Unit must provide full information on the nature of the proposed access. Company, before the implementation of the request, will communicate with the responsible Information Owner in order to identify any confidentiality of information issues raised. The new link will be based on the principle of minimum access, in agreement with the accepted operational requirements.

Company may rely on third parties for the protection of the network or its resources. All links of Third Parties may be considered safe based on security requirements and related SLAs and should be protected at least by firewalls. Only necessary transaction types (based on signed agreements of third party links) should be allowed by the firewall device to Company internal network.

In line with the above, the relevant units, in cooperation with Company will implement interfaces to critical infrastructures.

10.3. Changes to the interconnection

All changes to access must be accompanied by a valid business justification and subject to security checks by Company. The changes must be implemented through change management processes as described in the relevant section. Third parties in are responsible to notify Company in cases of hardware change and/or parameterization on the originally supplied information (on their side) so that security and connectivity is amended accordingly. Company shall communicate with the responsible Information Owner in order to safeguard confidentiality of information issues discussed before the implementation of any change in the interconnection and/or access by third parties.

10.4. Termination of access

When access is no longer required, the third party or unit that had originally requested this link, must notify Company to terminate the access. In addition, Company must carry out a check for the links on an annual basis to ensure that all existing connections are still needed and that the supplied access meets the needs of the interconnection.

Links that seem not often used, and/or not used anymore, will be terminated immediately. In the case where there is a Security Incident or found that a circuit is not used often or at all the Information Security Officer will be notified.

10.5. Remote connection security and requirements

The purpose of this special section is to set the requirements for connecting remote users to Company network, aiming to minimize the potential exposure to risk, due to unauthorized users. Such risks may threaten the confidentiality, integrity and availability of critical data, personal data and systems.

- Remote user access to the network must use safe methods and are subject to audit to ensure safe recognition, identification and access authorization.
- Remote access must be requested to and approved by Company.
- Remote access to Company network should be permitted only to authorized users of Information Systems.
- Company users need to follow the "Code Administration" section. If possible, a powerful authentication method should be used, such as one-time passwords or public/private keys with strong passphrases or even device one time password-tokens, rather than simple passwords.
- Under no circumstances should users of remote access provide link details or email the codes to other people.
- Simultaneous multiple remote connections from the same user are disabled.
- Remote access users must ensure that their computer or Terminal is not connected to any other network during their remote connection to Company. Possibilities for split-tunneling or dual-homing should be eliminated.
- All computers are allowed remote access to Company network must use up-to-date antivirus software, as defined in the section for protection from Malicious Software-Antivirus.
- Established connections which shows no signs of traffic for more than 10 minutes shall automatically terminated
- It is the responsibility of each user to ensure that the remote connection is not used by third parties to gain access to the systems or data of Company.
- Each user that has been given remote access should directly notify the Company where such access is not required. Moreover, every 4 months Company will check and document the need for all remote connections by users and deactivate those not used in order to achieve Company operational objectives.
- Access to critical systems should be governed by strict controls and all the

aforementioned restrictions. In addition, access should be constantly monitored to use approved and appropriate authentication services and encryption systems. Access should take place through application as defined according to the technical specifications of the relevant system.

10.6. Outsourcing

When outsourcing, the following should be included in the relevant contracts:

- The rights and obligations of the Contracting Parties.
- The agreed service level (Service Level Agreement - SLA).
- Accountability for installation and maintenance of hardware and software.
- The possibility of renegotiation of the contract in case of changes to Company security requirements.
- Procedures for validity termination of the contract, which include the prediction for the event of a sudden termination.
- Delivery of source code procedures and data.
- Property issues (ownership), licensing and copyright rights for data, information and computing resources (H/W, S/W, etc.).
- Change management procedures.
- Hierarchical escalation procedures for solving problems.
- Evaluation criteria and control procedures.
- Implementation, on the part of external partner, of all the required audit mechanisms and procedures (controls) pertaining to the confidentiality and integrity of data and the availability of information in Company like:
  - Resource protection procedures e.g. information hardware, and computer software
  - Physical security mechanisms
  - Protective mechanisms against malicious software
  - Procedures and mechanisms of identification, reporting and recording violations at Company
  - Return procedures or proper destruction of information when they are no longer useful
  - Limitation and ensuring the use of the information only within the frameworks defined etc.
- Education and awareness raising of external partners on issues, methodologies and procedures relating to the security.
- Access Control Policy which covers:
  1. Possible reasons that may justify access to third parties.
  2. Permissible methods of access and use of unique identification methods, e.g. access codes.
  3. List of users of the system and the privileges of those within the system.
  4. A written declaration to ban access to authorized users of the system. System privileges recovery procedure.
- Reporting procedures of any incident associated with system security breach.
- Control the use of information and removing privileges to access them.
- The right of access in the processes and systems of external partners and access to results of the checks carried out by independent bodies
- Task continuation plans and requirements for availability and reliability at any time.
- Legal responsibilities in ensuring compliance with legal requirements, taking into

account any different legal parameters governing the operation of Contracting Parties.

- Matters of copyright rights.
- The existence of a contingency plan, which relates to the re-taking of the assigned activity from Company or delegated to third parties if the service provider is unable to fulfill its contractual obligations, so as to ensure the proper functionality of the system.
- In particular, concerning security, conditions relating to the following must be included:
- Ensuring confidentiality, integrity, availability of information, such as confidentiality agreements, compliance with audit trails etc.
- The authentication of trading parties and non-waiver trades.
- The security of interconnections between Company and external partner.
- Ensure of the necessary qualifications on human resources, replace individuals who commit proven malicious actions or are reluctant on security issues.
- Penalties on cases of security breach.
- Right to Audit on behalf of Company.
- The type and frequency of the reports or files that will exchange both parties.
- Follow-up work plans and disaster recovery of the external partner.
- In cases of collaboration with suppliers or service providers, particular emphasis should be placed on ensuring the confidentiality of information which accesses the provider or supplier through an appropriate agreement of confidentiality.

10.7. Third party management

The Company for each contract with third parties should name a responsible manager to control the contract and monitor and evaluate the provided services.

Manager’s responsibility is to contact the third party and resolve any issues may arise. In addition, he/she will supervise third-party services, with a view to ensure the quality of these services as well as compliance with this security policy.

An official list of employees responsible to manage third party contracts should exist and be maintained.

11. Password management

Passwords are an important measure of protection and security access control to Company information systems. Safe and correct use of passwords is a prerequisite to operate other measures of protection.

This section describes the security requirements concerning the creation, use, and management of passwords used for identification and access to Company information systems as well as the principles governing proper use and ensuring protection of passwords and of information systems.

The following instructions should be the reference point for the creation of strong passwords, protecting them and the frequency of their edits.

The requirements described relate to all users who have access to Company systems and consequently possess or are responsible for an account/password.

11.1. Password security requirements

- Users must not under any circumstances use the same password to access systems that belong to external networks (e.g. Internet Web servers) with the one used to gain access to any Company information system infrastructure.
- Passwords should remain secret and under no way transmitted (oral, electronically etc).
- Passwords provided by the manufacturer must be changed during the first use.
- Original password given when issuing user account from Company when creating new user or new access, should apply only for the first, initial connection.
- The transmission of original passwords must be managed with safe mode and avoid sending unencrypted electronic data messages. During the first user's logon the information system should require the user to change the password. This should be carried out before the system allow any other activity to the user.
- Passwords must not be identical to the user's account.
- Passwords must consist of at least 8 characters.
- Passwords should include uppercase and small characters (e.g., a-z, A-Z) and may contain digits and punctuation (e.g., 0-9,! @ # $% ^ & * () _ + | ~-= \ ' {} []: "? ' < >?,./) and should contain at least one alphabetic and one non-alphabetic character.
- Passwords should not be ordinary words, nor rely on personal information such as your username, birthday date, and calendar days or by phone numbers. In particular, you must not consist of key words, derivatives of user identities and common character sequences (e.g. "123456").
- In case of administrator passwords, they should not indicate the level of access (e.g. admin, operator, etc.).
- Passwords used in information systems are classified as NON-DISCLOSURABLE information.
- All types of passwords should be changed every 3 months.
- User passwords should not be the same as the past five passwords.
- An account will be locked after 3 failed attempts to login.
- In case of incorrect password entry a general error message should be displayed without revealing the exact description of the error.
- Locked user accounts will be activated by the administrator only after intervention of the reason for blocking.
- Wherever possible, users will be directed to automatically follow the aforementioned restrictions on security codes by activating the respective parameters in Information Systems.
- Any suspicion concerning the violation of any password system should be considered as a Security incident and be managed in accordance with the procedure envisaged for the management of security incidents.

11.2. Special password requirements for Users/accounts with Permissions

User accounts with administrative privileges should be strictly limited to persons who are directly responsible for the management of systems and/or their security.

Accounts with administrative rights should be limited to two people per information system, while in each case separation of responsibilities of administrators should apply. In systems in which it is necessary to have more than two accounts, the approval of Company is required.

Staff with administrative privileges should have at least two user accounts. One of these accounts must have the necessary privileges for system administration and the other must be a simple user account that will be used for conducting usual daily functions, such as access to the Internet or send and receive email, etc.

12. Operational audit security controls

The goal of this section is to establish monitoring requirements and security checks in order to ensure the safe and proper use of Information Systems and early recognition and prevention of possible information security incidents.

12.1. Operational procedures

The objective of this protocol is to ensure that operating information security processes and procedures are properly documented and communicated to all users who need them. Operating procedures should be monitored for correct, secure and comprehensive implementation. At the same time internal checks should be carried out at regular intervals to ensure early identification of technological and procedural security weaknesses.

12.2. Logging and monitoring security incidents

The objective of logging and monitoring is to achieve the timely generation of events and the generation of evidence. Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

Logging facilities and log information should be protected against tampering and unauthorized access and change of log information.

12.3. Event logging requirements

In all critical information systems logging events are related to security. Recorded events must be stored at least for all critical systems, applications and network devices. Administrators are responsible for updating the event logs for a specific period of time (depending on the criticality of the system). After this period, the logs must be archived.

The determination of the requirements for recording Security events is the responsibility of the Company. The recording of events depends on the criticality of the systems, but also the requirements imposed by the existing legal and regulatory framework.

Event logs can contain sensitive data and personally identifiable information and appropriate privacy protection measures should be taken. Where possible, system administrators should not have permissions to erase or de-activate logs of their own activities.

The log should be performed to the maximum extent possible that does not affect the functionality of the system. Log actions mechanisms should record all the operations carried out in the security and surveillance systems, such as access and administrator actions on systems and applications, such as enabling, disabling, changing settings, changes in information systems security settings etc.

The logging requirements are set out below, categorized for networks, systems, databases and applications.

12.3.1. Network log files

The following events from devices that implement access control at the network level (especially when these networks link different classification levels) should at least be recorded:

- Time and date of each entry.
- Failed attempts to access network resources.
- Source/Destination Address and Network service.
- Settings changes in device setup.

12.3.2. Operating systems logs

At systems level the following events will be recorded:

- Date and time of each entry.
- Successful and unsuccessful attempts to access.
- Source/Destination Address and system service.
- User logon and Logoff Time.
- Password change on the system.
- Change of system security settings.
- Log of successful and failed attempts to add/delete users to/from the system.
- Unsuccessful attempts to access system data.

12.3.3. Database log files

At database-level the following events should be recorded:

- Date and time of each entry.
- Successful and unsuccessful attempts to access.
- Source/Destination Address and system service.
- User logon and Logoff Time on application.
- Change passwords at the DB.
- DB security settings Change.
- Log of successful and failed attempts to add/delete users to/from the basse.
- Commands and actions that were issued to the DB (select , update, delete).

12.3.4. Application logs

At the application level the following events should at least be recorded:

- Date and time of each entry.
- Successful, unsuccessful attempts of the user to access the system if the authentication is performed at the application level.
- Source/Destination IP address and application service.
- Change passwords in application.

- User logon and Logoff Time.
- Application's security settings Changes.
- Unsuccessful attempts to access data and application resources.

In addition, in cases where the application supports payments/transactions should at least be recorded the following events:

- Complete history of executed transactions for each session.
- Time, date of transaction.
- User id.
- Logon/logoff (sign-on/sign-off).

12.3.5. Clock synchronization

The correct setting of computer and information system clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases.

Time synchronization is a very important factor in control of security, because it provides time accuracy and reliability in the audit logs. Time synchronization should be based on the Network Time Protocol (NTP-Network Time Protocol) that allows synchronization to provide credibility and authenticity to whatever system keeps logs events for the Company's network.

12.4. Periodic inspection

12.4.1. Operations Security Audit Inspection

All functions related to monitoring information systems security events should be subject to periodic inspection by administrators of their respective systems. This check should include:

- Effectiveness of the Security events log settings.
- Effective management of media.
- Effective protection of Security events log files (e.g. administrator access permissions).
- Efficient monitoring of the systems.
- Compliance with the recorded Security Policy.

The reports with the results of checks, spotted weaknesses and suggestions for improvement, will be sent for update and measures to the relevant units.

12.4.2. Regular checks by Information Security Officer

The following checks must be carried out by those responsible for information security at least once every four months

- Weaknesses evaluation.
- Risk Assessment.

- Network Detection to locate:
  - Not approved network devices.
  - Unauthorized personal Web servers.
  - Unsafe device sharing.
  - Unauthorized modem usage.
- Operating systems and software licenses.
- Operating systems and Software Updates, according to the newest security advisories.

In case after regular checks any security or non-compliance issue is discovered, the Security Event management process must be followed, as defined in the appropriate section

12.4.3. Compliance checks

Compliance checks must be carried out periodically by the security officer or by outside companies and include the following controls:

- Security mechanisms and procedures to comply with this security policy.
- User Compliance with the requirements of the security policy.
- Compliance with legal and regulatory frameworks.
- Compliance with the necessary regulatory requirements governing the Company.

12.4.4. Security assessments

Extra checks and security assessments to Company information and network infrastructure should be carried out at regular intervals (per year) and exceptionally, in case of installation of new systems or applications. These evaluations could be entrusted to independent operators or free-lancers, for the objective evaluation of the network infrastructure.

These evaluations include:

- Security ratings and Vulnerability Assessments to identify susceptible to known system vulnerabilities. The responsible managers will be asked to correct or implement specific security measures in cases weaknesses are pinpointed in networked systems.
- Penetration Tests should be performed in the network infrastructure, in order to determine the range and the threats from malicious internal users, external users, or the Company.
- Risk Assessment for all systems and ranking of systems based on weaknesses identified in the security assessments.
- Periodic inspection for implementing the necessary controls and rules, with a view to aligning the company with the terms imposed by the regulatory requirements.

13. Physical and environmental security

This section refers only to the central storage and operation facilities of information systems and should always apply as a standard procedure. Physical security is one of the most important parameters of computer and information systems security and information systems services.

Important or sensitive information management facilities should be housed in secure areas, protected by a certain perimeter security, with appropriate security restrictions and input controls. The objective is to prevent unauthorized physical access, damage and interference to the Company's information and information processing facilities.

13.1. Physical security perimeter

The following general rules should apply to all buildings belonging to Company and house Central or critical computer systems:

- Company premises should be accessible only from Central entrances.
- Security guardians (if any) should control access.
- The entrance of employees in critical facilities should be controlled, either by using special cards or by pin codes.
- In the case of visitors, there should be verification of personal identity information before entering the premises. There should be communication with the responsible personnel before visitor the entrance. Input and output times, names, identity number and the reason for visit will be recorded in a log. During their stay, visitors should wear identification mark titled "visitor" and are not allowed to be left alone inside restricted areas. They should always be under the supervision of a personnel member.
- Security Windows and doors should be used in high-risk facilities, which must be locked.
- Circuit security cameras (CCTV if applicable) should exist in the perimeter of buildings and monitored by competent authorized personnel.

13.2. Data room/center security requirements

The following rules are the minimum security standards that must be followed in places that host critical systems and applications:

- Access to computer facilities and critical information, such as Data Centers, must be controlled and permitted only to authorized personnel. Access control mechanisms are to be used. Company maintains the official entry list of authorized users to the Data Room. Visitor entrance on computerized centers should be recorded in the register entry of the building.
- There should be specific and isolated area for delivery/receipt of equipment and consumables intended only for Data Centers.
- Third persons/visitors must be accompanied continuously.
- There must be cameras at the entrances and inside Data Centers. All activities must be recorded.
- Windows and non-controlled entry points to Data Centers should be as little as possible.
- Control mechanisms should be adopted, in order to reduce the risk from natural and environmental hazards, such as air conditioning.
- Cooling-heating systems, UPS etc. should be maintained according to the manufacturer's specifications.
- Non-smoking area.
- Installation of automatic fire extinguishing systems and smoke detectors within the

area.

- UPS and voltage protectors capable to power the Data room for at least 20 minutes.

13.3. Equipment - Placement and protection

The equipment must be placed in appropriate places, in order to minimize the unnecessary access to workplaces. Devices that require special protection must be isolated to reduce the overall level of physical protection required. Computer peripherals should be placed in secured cabinets and machinery must be insured in non-moving cabinets.

13.4. Security copies storage

Security copies are distinguished from backups in that security copies typically include only vital (essential) records. A backup may be used as a security copy if it is created and stored in a manner that allows retrieval of a complete set of vital records.

Security copies should be stored in a secure location, typically stored off site. In cases of disaster magnetic copies stored in safe place outside Data Room should be used. Backup magnetic tapes / disks should be stored away from large metal objects, in order to avoid damage by magnetic fields that could cause sparks.

14. Information security Incidents and Events Management

The purpose of this section is the description of actions to be performed when a security incident is detected and reported by employees, by external collaborators Company or a security event monitoring system. Security event management is an important part of information systems security risk management.

Such events can arise from a variety of reasons and can cause problems in availability, integrity and/or confidentiality of data on individual systems or across the entire network of Company and logistical equipment used.

The following requirements relate to all employees, vendors, or partners, and to all individuals, legal persons or organizations that have access to the information systems of Company.

14.1. Event management

The Company security event management involves direct and quick concentration of events that have been identified by their partners and employees at a predetermined benchmark. All events will be recorded carefully for analysis, with a view to implementing measures that will prevent the occurrence of similar events in the future. Also, in cases of intrusion events in information systems, sufficient evidence should be collected for further investigation and possible initiation of legal proceedings.

Definitions

Security Event: refers to a dangerous incident in an information system or network or to threat of such an event. Such events may affect the confidentiality, integrity and availability of information systems and include:

- Malfunctions (such as system/software problems, errors of transmission etc).
- Loss of data, equipment or installations (such as loss of external communication networks/tasks, blackout, system security attacks etc).
- Overload (such as job delay, insufficient response time, etc).
- Human errors (such as setup errors, network errors, handling errors etc).
- Non foreseeable impact of changes (such as consequences of the implementation of new/upgrade application software or by changes in the telecommunications equipment or critical systems etc.).
- Infringement of rights of access (such as introduction of electronic viruses, unauthorized internal or external access, unauthorized modification of files/databases).
- Unauthorized access to the network.
- Viruses or malicious software.
- Unusual processes running and require excessive processing time and clearly affect performance/speed system, network, services.
- Steal of software or hardware, service failures, overloads, etc.

14.2. Information security event reporting

Security incidents can be spotted and reported in two ways: either by staff and external partners or by automated methods and detection systems. All staff and users of Information Systems should report immediately to Company any abuse, threat, weakness or malfunction of information systems and Company network.

14.3. Staff and external partners

Any security incidents should be immediately reported to Company. If there is evidence of a virus in an information system, the user must inform Company and cooperate for the removal of the virus and reconnection of the system to the network.

Company should record each error message or other pertinent information associated with the event. Company should directly inform all relevant units. Company will also inform if there is any indication that the malfunction comes from some weakness in system security.

Staff or users Information Systems should not try to investigate or resolve security incidents, unless authorized.

14.4. Recording and escalation of events

After an incident is reported, it will be recorded and priority-based, by Company. The priority of events should be determined on the basis of ' Event ' Priority Categories, which determine how to deal with incidents. Based on this categorization strange or unexpected incidents should be treated or be escalated for immediate investigation.

14.5. Event management and hierarchy

14.5.1. Priority 1 or 2 : Reduced or Negligible impact Events

Low risk events that have been detected by scanning or detection systems inside and outside environment of Company. Examples are individual cases of known electronic viruses, easily controlled by computer software viruses, non-unauthorized file usage, possible known weaknesses of systems, bad or unauthorized use of privileged system accounts etc.

Events that are assigned priority 1 or 2 and are reported by internal users or external partners should be evaluated, managed and logged by Company especially if they can influence the integrity, availability and confidentiality of information and systems. If the incident requires the involvement of specialized personnel, such staff must be advised to take over the investigation of the incident. If there is evidence of fraud or illegal acts, the event should be forwarded to the Law Department.

When there is no direct solution, then all occurrences of priority 1 and 2 should be assigned to the corresponding information systems support staff. All events should be monitored and resolved by the support staff based on hierarchy. When there are Service Level Agreements, any incident will be resolved within the terms of the service contract.

14.5.2. Priority 3 or 4 : Moderate or high impact Events

Medium-or high-risk events that are not automatically detected. Examples are cases of new electronic non-traceable virus, malfunction of critical systems etc. The events in this category are likely to diminish Company image / fame among current and prospective users of Company systems and may also have negative financial impact.

The Administration should engage in any exceptional event and events designated priority 3 or 4. Company should immediately inform the administration of any detected high-risk incident.

Every case of violation of the integrity, access restrictions, and in general the security of information designated as "Confidential" or "Secret" should be considered as an event of great impact and managed the appropriate way.

Following the confirmation of the incident and categorization of priority 3 or 4, the Administration will need to activate the event response procedure, which should include five stages: Confirmation, Elimination, Recovery, Restoration and Review.

14.6 Incident recording and monitoring

- Each event that is considered critical and affects the integrity, availability and confidentiality of Company systems, should be recorded centrally and the relevant supporting material should be filed. Each event log should contain information such as: code, description, priority, cost, impact assessment and response measures etc. in order to be able to quantify the effects and monitoring by Company. Such information facilitates identifying high-risk events or recurring events and help in finding additional or improved control and security procedures, in order to avoid similar incidents in the future.

- Company should maintain a database or log files on breaches of Security Policy and produce periodic reports to the administration of Company. Access to these files should be restricted only to authorized personnel.

14.7. Event investigation

- For any serious security incident, which may have legal implications, Company should collect all necessary electronic proofs (using electronic forensic evidence gathering methods) or other necessary information.
- Pooling, auditing, archiving and preservation of evidence is of greatest importance to any legal investigation.
- Evidence produced in order to be accepted in form of a court must satisfy the following conditions: the information should concern the event, be reliable and properly guarded, under the section "physical security".
- Depending on the characteristics of the event, Company should be consult during the investigation Company legal department, competent authorities or external partners, in order to ensure the accuracy of the evidence and the legal proceedings that should be followed.

14.7.1. Security Violations

In the event of a deliberate breach of security, the Administration must be advised immediately. If the intention is not clear, the violator should be recommended to take steps to correct/prevent the error. In any case, security violations should be recorded, and the corresponding files be kept for future reference.

14.8. Threats and Vulnerabilities Assessment

Company will need to be updated constantly for new threats and risks associated with information systems (e.g. by participating in auto-updated electronic directories) and take the necessary measures to overcome them, depending on the effects that may have on Company.

Information levels are:

- Informational level –simple notification.
- Advisory level – figure out possible impacts to be evaluated.
- Warning – proposed actions to avoid effects.
- Immediate reaction – immediate response.

Company should inform users about new threats related to information systems, such as new electronic viruses. Information about technical content threats should be promoted only in specialized technical personnel.

14.9. Education, testing and review of the Security Event Management Process

Education program should also include general sections for managing basic scenarios of possible incidents, for example threat from electronic viruses, failed or successful penetration attempts in systems, significant malfunction of key systems, natural disasters etc.

The Information Security Event Management process should be evaluated at regular intervals. The evaluation should include full or partial execution of the process. A complete functional test should be performed at least annually. The tests must be scheduled at times that they do not impair Company functions.

Specialized independent auditors should evaluate the Information Security Event Management process to ensure integrity and compliance with the policies and procedures.

15. Business Continuity Management (BCM)

Information security continuity should be embedded in the Company's BCM systems. The Company should determine its requirements for information security and the continuity of information security management in adverse situations e.g. during a crisis or disaster.

A Business Continuity and Disaster recovery procedure is implemented in order to timely and optimally restore Company systems after stops due to disaster or failure in security issues (which might be, for example, the result of natural phenomena, accidents, equipment failures or even intentional acts), to an acceptable level, through a combination of preventive and remedial actions.

Company should ensure, as far as possible, the restoration of the most crucial systems and applications and business continuity through a set of specially designed mechanisms and procedures.

The disaster recovery management process must include checkpoints (controls) that identify and reduce risk factors (risks) and mitigate the effects of damaging incidents and ensure the timely recovery of the critical functions of the organization.

15.1. Backup

A key component for the planning and implementation of disaster recovery plan and business continuity is to determine a detailed and documented process for the management of security copies to protect against loss of data.

15.1.1. Storage Types and Backup Stages

The following instructions apply to storing data in the Company:

- Disk backup (daily) for the Company central computing infrastructure.
- Tape backup (daily and weekly) for the Company central computing infrastructure.

15.2. Safekeeping, checking and documentation of Storage Media

The media will be kept within the building of the system. Media retention periods will vary according to the system concerned. The locations for the safekeeping will be selected on the basis of Security and ease of Access.

Backup copies are audited periodically as to their integrity to ensure that the data they contain can fully and successfully be recovered. For centrally controlled systems, period checks depend on the system and the possibility of recovery.

Apart from the continuous control of the backup process, it is recommended every six months to plan for volume and storage capacity, in order to determine the functional requirements for the next two years. The outcome of these plans is to be used for reviewing the effectiveness of existing material, the current process and management and to determine the need for possible changes.

Company will develop and update a file Backup procedure. This procedure contains a list of the systems as well as a reference to the data to be stored and their sites. Marking and record- keeping of Backup Tapes is done automatically from the tape library.

15.3. Disaster recovery Plans

Company must have an approved disaster recovery Plan to be applied in cases of catastrophic events that can cause prolonged shutdown of a critical system. A disaster recovery plan should take into consideration business impact analysis and risk assessment, based on which it will:

- Identify all critical functions and systems-resources used.
- Identify all risks that threaten critical functions and will be ranked according to the likelihood of their occurrence and their possible effect on the systems and functions.
- Weigh the costs of eventual interruption of critical operations and the activation of the disaster recovery plan and identify the conditions that will trigger the implementation of such a plan.
- Determine recovery time and recovery point of critical functions. The disaster recovery plan, will:
- Be written in plain and intelligible language and be communicated to all staff. Any classified information of the project (e.g. passwords, security keys, etc), should be disclosed only to authorized personnel.
- Be kept in a suitable place at a safe distance from the computer center Such a plan should include:
- Classification of systems based on operational need. This ranking should, among other things, indicate recovery time of each system as well as the minimum estimated performance after recovery.
- The procedures to estimate the extent of the destruction and the respective parts of the plan that should be activated.
- Activation procedures of plan, personnel alert and emergency teams.
- The actions to be performed in specific emergencies, which should ensure staff security in case of danger/damage (e.g. fire, earthquake etc).
- Alternative workspaces, equipment to be used, and required specifications.
- Preparation and activation procedures of alternative data center.
- Alternative systems, infrastructure and network topology.
- List of suppliers with whom there are support contracts, the services that they offer and their expected response times in case of emergency.

- Procedures to ensure that the plans are maintained, adapted and updated after any change in Company operating procedures.
- Staff training procedures in accordance with the responsibilities they assume in the implementation of the project.

15.4 Testing procedures.

It should be stressed that due to the complex (or simplistic) nature of specific systems of Company the existence of a disaster recovery plan does not necessarily mean the existence of double alternate data center (Disaster Recovery Site).

16. Supply, Development and Maintenance of Information Systems

Any new system implementation and/or technology infrastructure should be assessed and adequately controlled for security vulnerabilities which may endanger Company business functions.

The introduction of control and security mechanisms in the design and development of new systems and applications is considered necessary and imperative to meet the security requirements in such a way as to ensure compliance with the existing legislative framework, customer confidence and continuity of operations.

Security Countermeasures are economical and efficient when incorporated in the development of applications. All security requirements, systems under development/applications must be identified during the phase of project requirements and must be justified, approved and documented.

Requirements for the development, installation and maintenance of information apply to all Company units and suppliers responsible for the development, installation and maintenance of information resources.

Each project which includes any form of development/implementation of information system or individual application, shall meet the essential security requirements, as defined below.

16.1. Security requirements

To ensure security in all systems under development, all security requirements of systems should be determined during the design and project requirements phase. The justification, approval and documentation of security requirements should be part of the description of the systems requirements. In order to ensure that the above are met, Company is actively involved in all phases of the System Development Lifecycle.

Requirements and security checks must take into account the value of the information considered as well as operational damage which may be caused by the absence or failure of security measures. The context in which analysis of security requirements and the determination of security checks is performed, is directly linked to the evaluation and management of risk that must be performed by Company and Information owners.

17. Change and configuration management

Changes to the organization, business processes, information processing systems and facilities that affect information security should be properly controlled.

Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Changes to the operational environment (i.e. transfer of systems applications from test to production) can impact on the reliability of software applications.

17.1. Change management requirements

The purpose of this policy protocol is to address these changes / alterations / modifications / updates in a logical and predictable manner so that staff, in cooperation with Company management make the necessary planning. The changes require serious preparation, careful monitoring and assessment of the outcome and potential impacts, so as to limit the impact on the normal operation of systems and operations.

Company should design and implement specific mechanisms and procedures to monitor, record and manage any kind of change that may endanger the smooth operation of business functions and security of systems and information. The changes that may take place in an organization can be legal / regulatory (e.g. changes to the legislative framework), organizational (e.g., mergers or restructuring), human resources (e.g. recruitment, transfers, retirements), systems (e.g., introduction of new systems in the technological environment).

The Change Management process must ensure:

- Identification and registration of changes in the business needs the systems support.
- Company support staff for Change Requests.
- User rights to request changes.
- Change Request Initiation and Control.
- Impact Analysis/Assessment on security issues
- Control of Changes - programming and testing the after changes - Change Approval.
- Review of security checks and integrity procedures to ensure proper functionality after changes.
- Documentation and Procedures – establishment of a procedure to maintain technical documentation.
- User awareness of changes / alterations, before the system enters in production.
- Authorized Maintenance.
- Software Release Policy.
- Distribution of Software.
- Allow for system recovery procedures to previous situation due to possible incompatibilities or other unexpected malfunctions of the system after implementing changes.
- Version Control (using dedicated tool).
- Maintain calendar control (audit log) for all requests for changes.
- Changes related to security in each component of information systems should be reviewed with the "owners" of the systems and Company.
- Small changes in hardware and software due to daily use must be documented by the person responsible for implementing the changes.

17.2. Configuration management and control

Configuration management and control mechanisms should be used to keep control of all implemented software as well as the system documentation and should comply with the following rules:

- Changes in systems should first be conducted on systems for development and testing, and then, after appropriate checks and official approvals, transfer to the productive environment and only by authorized persons.
- Changes in the configuration of the operating system and database changes should be made from Company.
- Review integrity and security parameters to ensure that they are not affected by the changes.
- Software, data files and database entities that need corrections, changes or alterations must be identified.
- Version control should be kept for all software updates, with the use of and appropriate tools, so that there is separation of versioning and rollback to a previous version.
- Any change or upgrade will not take place if it has not been tested.
- In cases where it appears that there is a need for immediate intervention in a production system, this will be carried out only by authorized individuals and then the reason for this will be documented.
- All changes are kept.
- Check security configuration after changing the operating system or other System Software. Periodically this may require changing the operating system, such as for example when upgrading to new versions. Immediately after the change, system integrity is reviewed to verify that it is not affected by the change of the operating system.
- Communicate early warnings about upcoming changes.

18. Compliance and deviations from policy

18.1. Compliance with legal and contractual requirements

The objective of this control is to avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

All relevant legislative, statutory, regulatory, contractual requirements and the Company's approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system and the Company.

18.2. Privacy and protection of personally identifiable information (PII)

Privacy and protection of PII should be ensured as required in relevant legislation and regulation where applicable.

The Company should develop and implement a Data Policy for privacy and protection of PII, and be communicated to all persons involved in the processing of PII.

Compliance with this policy and all relevant legislation and regulations concerning the protection and privacy of people and PII, is best achieved by the appointment of a person responsible for guiding managers, users and service providers on their individual responsibilities and the specific procedures that should be followed.

18.3. Compliance with the information security policy

Company management should regularly review the compliance of information processing and procedures within their area of responsibility with this policy and other security requirements.

If any non-compliance is found as a result of the review, managers should:

- identify the causes of non-compliance
- evaluate the need for actions to achieve compliance
- implement appropriate corrective action
- review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses

Results of reviews and corrective actions carried out by managers should be recorded and records maintained.

19. Cryptography

Cryptographic keys are required to access data and systems which utilize encryption. The organization takes the following approach in the management of these keys:

• Access to cryptographic keys in Active Directory must be restricted to authorized staff only.

• Procedures must be in place to ensure that requests for cryptographic keys can be appropriately authorized, provided in a timely manner and appropriately recorded.

• If a cryptographic key is provided for recovering access to a computer, the existing key must be revoked, and a new key must be generated to prevent data leakage and use of such keys is recorded.

• Cryptographic keys must be securely managed and protected though their whole lifecycle from initial generation and storage to archiving, retrieving, distributing, retiring and eventual destruction.

• Cryptographic algorithms, key lengths and use must be in accordance with all relevant organizations policies, procedures and in accordance with professional best practices.

• Cryptographic keys must be protected though their whole lifecycle against

modification, loss, unauthorised access/use or disclosure.

• Equipment used to generate, store and archive keys must be physically protected using appropriate, secure access controls.

• Awareness of encryption/decryption passwords for devices, media or systems must be limited to authorized personnel only.

• In the event of a cryptographic key being compromised, the existing key must be revoked and a new key (or key pair) must be generated.

Conclusion

Required conformity with the GDPR is of importance. Not only because administrative fines can be imposed to businesses which can be exhaustive but also because of liabilities that not the GDPR but some legislative, country specific laws, impose, as is the case for example in Greece. Prison sentences of up to one year may be enforced by National Law number 4624/2019 in Greece as it is stated in its article 38.

The documents that are suggested in the paper are not intended to cover all the aspects of data protection conformity but rather to define a basic frame with the must have prerequisites in order for a data controller to prove its conformity with the regulation. The record of processing activities, the privacy policy and the security policy are the minimum required documents to prove such conformity. In the following table finally we can compare the contents of only those three documents against the basic principles of processing to realize their usefulness.

Principle	Meaning	Document
lawfulness	Choose an appropriate legal basis	Records of Processing Activities (ROPA)
fairness	Provide information	Privacy Policy (PRIPO)
Transparency	clear and plain language be used	Privacy Policy (PRIPO)
purpose limitation	Only processed for the reason collected	ROPA
data minimization	What will be processed	ROPA
Accuracy		
storage limitation	How long will be retained	ROPA
integrity and confidentiality	Measures for security and access	Security Polic(SEPO)
accountability	Prove the above	All the above

TABLE 6. Mapping of principles to documents

References

ISACA, 2023, Privacy in Practice.

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), OJ L 119 4.5.2016, p. 1-88, http://data.europa.eu/eli/reg/2016/679/oj.

ISO/IEC 27701:2019, Security techniques — Extension to ISO/IEC 27001 and ISO/IEC27002 for privacy information management — Requirements and guidelines

ENISA, DATA PROTECTION ENGINEERING, From Theory to Practice, JANUARY 2022

ARTICLE 29 Data Protection Working Party, "Opinion 10/2004 on More Harmonised Information Provisions," 2004.

ARTICLE 29 Data Protection Working Party, "Guidelines on transparency under Regulation 2016/679," 2018.

L. Edwards and W. Abel, "The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services," 2014.