Pursuant to Article 10, paragraph 1 of the Law on Information Security (Official Gazette of the Republic of Montenegro 14/10) at its session held on 16 September 2010 the Government of Montenegro adopted the following

DECREE
ON INFORMATION SECURITY MEASURES

I. GENERAL PROVISIONS

Subject

Article 1

The present decree shall establish the measures of information security that provide basic data protection on physical, technical and organizational level.

Obligation to Implement

Article 2

The measures referred to in Article 1 of the present decree is addressed to national authorities, state administration bodies, local self-government units authorities, legal entities with public authorisation (hereinafter "authorities") and other legal entities and natural persons having access to or handling the data.

Meaning of Terms

Article 3

Some terms in the present Decree shall have the following meaning:

1) **hardware** shall be the physical component of information system;

2) **cryptographic protection** shall be data and information protection system which shall ensure safe data transmission through computer and telecommunication network;

3) **IT media** shall be any media where it is be possible to transmit or store data in electronic form;

4) **safe storage** shall be safe, cash register or other storage space equipped by device that prevents unauthorised access to stored data;

5) **software** shall be any operating system, programme, user and service application;

6) **risk** shall be potential cause that may damage the data or information system using the data;

7) **safe location** shall be place to keep the data stored in IT media or outside the premises of the authority, legal entity or natural person referred to in Article 2 thereof, equipped by technical devices which prevent unauthorised access to devices and data;

8) **administrative zone** shall be space or premises in the building where the data are kept and devices on which the data are stored and which requires adequate physical protection.

9) **encrypted data protection** shall be application of software solutions or devices for data protection that ensure integrity, confidentiality and availability of data.

II. PHYSICAL PROTECTION

Types of Measures

Article 4

Measures of information security of physical protection shall be the following:

1) administrative zone establishment;
2) development of physical protection plan;
3) assessment of the effectiveness of physical protection measures;
4) control of persons;
5) data storage;
6) physical protection of information systems.

The Goal of Implementing Measures

Article 5

Measures of information security of physical protection shall be implemented for:

- preventing unauthorised or forced entry of persons into buildings and premises where the data are located, i.e. devices with data;
- preventing and detecting abuse of data by employees;
- detecting and responding to risks.

Criteria for defining measures

Article 6

Measures of information security of physical protection shall be defined depending on the type, number, form and manner of data storage, data access authorisation and security assessment of potential risks.

Administrative Zone Establishment

Article 7

Administrative zone shall be established for data usage in controlled, visibly indicated space where it is possible to control access of persons.

Development of Physical Protection Plan

Article 8

Authorities, legal entities and natural persons referred to in Article 2 thereof, for the building

or premises to which they have access, i.e. where they handle the data, shall develop physical protection plan that identifies requirement to implement physical protection measures, in accordance to information security standards.

Assessment of the Effectiveness of Physical Protection Measures

Article 9

Authorities, legal entities and natural persons referred to in Article 2 thereof, at least once a year, shall assess the effectiveness of information security measures of physical protection of buildings and premises where the data are stored, as well as when there is a change of location or elements in the information system.

Control of Persons

Article 10

Authorities, legal entities and natural persons referred to in Article 2 thereof shall control persons at the entrances and exits of the buildings or premises where the data are stored and keep record about it, to prevent unauthorised transfer of data or bringing in the prohibited items that can threaten data security.

Data Storage

Article 11

Data shall be stored in the adequate IT media, which is disposed and kept in safe storage.

Physical Protection of Information Systems

Article 12

The premises with computers for database management and mainframe computer of information system (servers), network or communication equipment of information system, shall be organised as administrative zone.

III. DATA PROTECTION

Data Protection Mechanisms

Article 13

Computer for database management and mainframe computer of information system (server) shall be equipped by:

1) system for safe log in with the possibility to record the realised accesses, so that the server access may be controlled and limited;

2) mechanism for preventing unauthorised taking out and bringing in data by using portable IT media, communication ports and connections for printing data;

3) protection mechanism against computer viruses and other harmful programmes.

Database Access

Article 14

Database access shall be allowed only to persons responsible for maintenance and development of information system.

Access to Telecommunication, Computer and Application System

Article 15

Access to telecommunication, computer and application system for data processing shall be allowed with entering appropriate user name and corresponding password.

User name and corresponding password shall not be exposed to and used by any other person.

User Access System Management

Article 16

User access system management shall include development, implementation and maintenance of information system in a way that allows unambiguous identification and reliable guarantee of user's identity.

Data Storage Obligation

Article 17

Authorities, legal entities and natural persons referred to in Article 2 thereof shall store all data from information systems in IT media by using methods that guarantee security, confidentiality, integrity and availability of the stored data.

Daily, Weekly, Monthly and Annual Data Storage

Article 18

Databases shall be stored in portable IT media at least once a day, week, month and year for the purpose of database update.

Information system data shall be stored in as many copies as there are working days in a week.

Weekly information system data storage shall be performed in the last working day of the week, after finishing daily data storage in as many weekly copies as there are last working days in the week.

Monthly information system data storage shall be performed in the last working day of the month, separately for each month.

Annual information system data storage shall be performed in the last working day of the

year.

Each copy of annually stored data shall be kept for the time stipulated by the regulations governing recording activity.

Each copy of portable IT media with stored data shall be designated by a number, type (daily, weekly, monthly and annually), storage date and name of a person storing the data.

Authorities, legal entities and natural persons referred to in Article 2 shall keep record of IT media where the data are stored.

Location for Disposal of Stored Data

Article 19

Information system data stored daily in IT media shall be disposed in at least one safe storage in the premises of the authority, legal entity or natural person referred to in Article 2 or in other safe location.

Information system data that are weekly, monthly and annually stored in IT media shall be disposed in safe location.

Checking Backup Integrity

Article 20

Usability of data backup shall be checked at least every six months along with checking the database recovery process stored in IT media, so that the recovered data after the check are complete, confidential and available for use.

Time Periods of Checking the Media Quality

Article 21

Data stored annually in IT media shall be recovered after expiration of the half of guaranteed period of record duration in that type of media.

Encrypted Data Protection System in Transmission through Information and Telecommunication System

Article 22

Authorities, legal entities and natural persons referred to in Article 2 shall establish encrypted data protection system in transmission of the data through information and telecommunication system.

IV. INFORMATION SYSTEM PROTECTION

Placement, setup and installation of server, computers and computer network

Article 23

Computer for database management and mainframe computer of information system (server)

and computer network shall be setup and installed by qualified person, in line with project documents, applicable norms, standards and technical instructions.

A copy of project documents referred to in paragraph 1 of this Article shall be kept in the premises of authority, legal entity or natural person referred to in Article 2 thereof, in a safe place, and shall be submitted for review at the request of state administration body responsible for information society affairs (hereinafter "state authority").

Controlling Information Systems Connection

Article 24

Controlling Information Systems Connection shall include defining of requirements for connecting information systems as well as recording and connection monitoring.

Controlling the Use of Information Systems

Article 25

Controlling the use of information systems involves recording activities of information system user, as well as measures to prevent the abuse of information system by installing system for detecting unauthorised intrusion to computer network, defining, reviewing and analysing record of information system operation and analysing information system vulnerability.

Records, Monitoring of Access and Unauthorised Attempt to Access the System

Article 26

Each access to information system for data processing and storage shall be automatically recorded by username, date and time of login and logout.

Each attempt of unauthorised access to information system shall be automatically recorded by username, date and time and, if possible, by the place from which such access was attempted.

The person referred to in Article 14 thereof shall notify the Body Administrator, Manager of Legal Entitiy, i.e. natural person about any attempt of unauthorised access to information system.

Fire Precautions

Article 27

Information system shall be located in the premises that have fire detectors and automatic notification of fire.

The premises where the information system is located shall have fire extinguishers, and in the vicinity, in and in front of the premises, in visible and easily detected places there shall be displayed instructions of the procedure in case of fire.

Measures to protect against electrical and magnetic fields, electrostatic electricity and ionising radiation

Article 28

In the vicinity of computer and telecommunication equipment there shall not be placed the

following:

1) source of strong electric or magnetic field;
2) source of electrostatic electricity;
3) source of ionising radiation.

Measure to Protect Against Moisture, Cold and Heat

Article 29

In the premises where the information system is located the adequate humidity and temperature shall be maintained.

Measure to protect against corrosive and highly flammable liquids, explosives and similar compounds

Article 30

In the premises and in their vicinity where the information system equipment is located there shall not be corrosive and highly flammable liquids, explosives and similar dangerous and harmful chemical compounds.

Implementation of Cryptographic Protection

Article 31

Data confidentiality, integrity and availability shall be provided by using cryptographic methods approved by the competent authority.

Establishment of Security Policies and Personnel Education

Article 32

Authorities, legal entities and natural persons referred to in Article 2 thereof shall establish security policies in order to ensure information security of data to which these persons have access, i.e. persons handling with them.

Security Policies referred to in Article 1 thereof shall include:

1) internal rules for employees;
2) education and professional development of employees.

Plan to Act and Procedures in Emergencies

Article 33

Planning emergency response shall include analysis of potential risks of information system operation and establishment of procedures to address these risks as well as other methods of using information system resources in case of unavailability of information system, in order to maintain continuous functioning, i.e. operations of authorities, legal entities and natural persons referred to in Article 2 thereof.

Action planning in emergency situations shall include the following:

1) developing a plan of continuous functioning, i.e. operations of authorities, legal entities and natural persons referred to in Article 2 thereof.
2) developing procedures to be followed in case of incidents.

Plan for Continuous Operation

Article 34

Plan for continuous functioning, i.e. operation shall include establishing and testing adequate procedure for safe data storage in order to return the information system and data into their original state after the incident, which includes information system failure, natural disasters and effects of computer viruses.

Development of Procedures to Be Followed in Case of Incidents

Article 35

Development of procedures to be followed in case of incidents shall include planning and defining activities of preventing, detection and recovery from the effects of the incident, which affect confidentiality, integrity and availability of data or information system, including reporting the incidents.

V. INFORMATION SECURITY RISK MANAGEMENT

Risk Management

Article 36

Information security risk management shall include planning, organising and directing activities to provide such conditions that risks do not jeopardise continuous functioning, i.e. operations of authorities, legal entities and natural persons referred to in Article 2 thereof.

Planning referred to in paragraph 1 of this Article shall include defining the level of risk acceptability, for the purpose of its acceptance, reduction or avoidance (hereinafter "risk analysis").

Acceptance, Reduction and Avoidance of Risk

Article 37

The risk may be accepted if the occurred damage would be less than damage caused by non-implementation of particular activity.

Reducing risk shall be carried out by applying the measures set up in plan of activities referred to in Article 38 thereof, to prevent destruction, alienation, loss and unauthorised data access.

Avoiding risk shall include taking organisation and other required measures to avoid actions that could cause risk.

Plan of Activities

Article 38

After risk analysis, authorities, legal entities and natural persons referred to in Article 2 thereof shall develop a plan of activities which defines implementation of required measures.

Reconsideration of the Plan

Article 39

Results of risk analysis shall be reconsidered regularly, according to the requirements of authority, legal entity and natural person referred to in Article 2 thereof, resulting from internal or external modifications.

VI. FINAL PROVISION

Entry into Force

Article 40

The present Decree shall enter into force on the eighth day following its publication in the Official Gazette of the Republic of Montenegro.

Number: 03-7797
Podgorica, 16 September 2010

Government of Montenegro
Prime Minister
Milo Djukanovic