Pursuant to Article 38 of the Law on State Administration (Official Gazette of the Republic of Montenegro 38/03 from 27 June 2003, 22/08 from 02 April 2008, 42/11 from 15 August 2011), The Ministry for Information Society and Telecommunications adopted the following

Rulebook on Information Security Incident Management

General Provisions

Article 1

CIRT shall develop and maintain a plan for responding to information security incidents reflected in defining the procedures relevant to incident management.

The minimum required for the plan shall include:

1) Clear responsibilities for each member of CIRT.
2) Strategy for reducing security incidents.
3) Operational processes, rulebooks and procedures for detection and analysis, isolation, eradication, recovery and reporting information (including network services) security incidents.
4) Processes and procedures for:
   a) limited access;
   b) testings or adjustments;
   c) penetration tests for the preferred systems;
   d) Handling the incidents and their reporting
   e) Incidents database maintenance.

Reporting Security Incidents

Article 2

2.1 Reporting security incidents

The right to report security incidents shall have national authorities, state administration bodies, local self-government units authorities, legal entities with public authorisation and other legal entities and natural persons having access to or handling the data.

The incidents shall be reported in one of the following manners:

1. at the official CIRT website (www.cirt.me)
2. e-mail notification to official CIRT e-mail address (kontakt@cirt.me)
3. notification through CIRT contact phone number

Person reporting the incident shall specify all the required details on the incidents.

The person reporting the incident shall not undertake any action to make corrections, but shall immediately report the incident to the identified internal CIRT's contact or other competent national authorities.

2.2 Reporting the Weaknesses of Information Security

All the employees, contractors, and involved third parties shall report on the observed weaknesses of information security to CIRT official as soon as possible in order to prevent information security incidents.

The employees, contractors, and involved third parties shall not test without authorisation the suspected security weaknesses. Testing the weaknesses may be considered as possible abuse of the system and may cause damage to the information system or service and as a result produce a legal responsibility for the person who did the testing.

Handling the Security Incidents
Article 3

3.1 Incident Analysis and Verification

The team responding to the incident situations with computer systems shall work immediately to analyze and validate each incident by documenting each step they take.

When CIRT has reason to believe that the incident occurred, they shall immediately do the initial analysis to determine the scope of incident, such as:

1) Which networks, systems or services have been infected;
2) Who or what created the incidents; and
3) How the incident is developed (e.g. which tools or methods to attack are used, which vulnerabilities are exploited).

The initial analysis shall provide sufficient information for CIRT to prioritise the following activities such as incident isolation and further analysis of the effects of incident.

CIRT shall take into account security of the data related to incidents (e.g. data on exploited vulnerabilities, recent security hackings, and users who may have performed inappropriate actions).

In order to reduce the risk that sensitive data be inappropriately published, CIRT shall ensure that access to data related to incidents is limited (e.g. only the authorised personnel shall have access to database on incidents, e-mails related to incidents shall be encrypted so that only the sender and the intended recipient can read them, etc.).

3.2 Categorisation of Incidents and Assessment of Organisation

CIRT shall document all incident management processes and procedures to prioritise, categorise, assess, and mitigate incidents of organisations under the present Rulebook.

All identified information security incidents shall be categorised and prioritised in accordance to the negative effects they shall have on the data and/or information system of the organisation.

Prioritisation of Security Incidents
Article 4

Prioritisation of incident processing is perhaps the most critical decision point in the process of handling the incident. Due to limited resources, incidents shall not be processed according to the method of arrival, i.e. by the principle of first come, first processed. The priority in incident processing shall be determined on the basis of two factors:

1) Current and potential technical effect of the incident

CIRT shall consider not only the current negative technical effect of the incident (e.g. unauthorised level of user's access to the data), but also the possible future technical effects of the incident in case it was not immediately isolated (e.g. compromising the administrator account). For example, a worm that spreads among workstations may currently cause a minor damage to the organisation, but after a few hours of its traffic, it can cause a greater breakdown in the network.

2) Criticality of threatened resources

The resources threatened by incident (e.g. firewalls, main network / system equipment, support systems, services, internet connections, users' workstations and applications) have different meaning for the organisation. Criticality of resources is primarily based on their data or services; users; relation of trust and interdependence from other resources; and visibility (e.g. public web server against internal sectoral web server).

Categorisation of Security Incidents
Article 5

Categorisation shall be based on two criteria: incident type and incident category, as described below.

1) Incident type

All information security incidents shall be classified as either Type 1 or Type 2, as described below, depending on the type of security violation.

Type 1 Incidents

Type 1 incidents shall be successful incidents that potentially may seriously disable network infrastructure and user information systems. The following items shall be defined as Type 1 incidents:

Type 1 Information Security Incidents:

Compromising/hacking the system;
Loss or theft of equipment/system;
Incidents with malicious code;
Incidents of unauthorised use of network infrastructure; and
Access violation.

Type 1 Service Security Incidents

Service loss;
Disabling service access; and
Incidents of unauthorised use of network services.

Type 2 Incidents

Type 2 incidents shall be the attempted incidents presenting potential long-term threats to user information systems or which may degrade the overall efficiency of information security programme. The following items shall be currently defined as Type 2 incidents:

1. Hacking attempt; and
2. Reconnaissance activities.

Notification of the Incident
Article 6

CIRT will through regular reports inform the management on the status of information security.

In some cases, such as major system downtime, CIRT will extraordinarily notify the management and CIRT system users. CIRT shall plan and prepare several communication methods and choose the methods adequate for the particular incident. Potential communication methods could include some of the following items:

1) E-mail;
2) Website;
3) Telephone calls;
4) Personal reporting (e.g. daily briefings).

Incident Isolation Strategy
Article 7

When an incident is detected or analysed, CIRT shall isolate it, before the spreading of incident causes major problems or before the damage is increased. The isolation process shall be considered an early phase of incident handling process. Isolation strategy shall include a part of management responsible for decision making (e.g. to shut down the system/service, etc.).

The criterion for adequate strategy determination shall include the following:

1) Possible damage or theft of resources;
2) The requirement to preserve evidence;
3) Service accessibility (e.g. network connectivity, services offered to external parties);
4) Time and resources required to implement the strategy;
5) Strategy efficiency (e.g. partial isolation of incident, complete isolation of incident), and
6) Solution duration (e.g. emergency backup solution that should be replaced within four hours, temporary solution that should be replaced within two weeks by the permanent solution).

Collection of Evidence
Article 8

Although the primary reason for evidence collection during an incident is to find its solution, it may also be used in judicial proceedings.

CIRT shall clearly document the manner in which all the evidence collected from a compromised system will be kept. All the evidence shall be collected in accordance with procedures complying with all the laws and regulations in the manner acceptable at the court.

A detailed log shall be kept for all the evidence. All the logs shall be maintained, inspected and monitored.

Should CIRT not have internal skills or capacity to eradicate the security incident or collect data about the incident, they may require assistance from the respective companies, third parties or government agencies. List of respective companies, third parties or government agencies shall be approved by the head of CIRT.

Keeping Evidence
Article 9

Evidence shall be kept in the following manner:

For paper documents: the original shall be kept in a safe manner along with the data of the person finding the document, where and when the document was found and who witnessed this event;

For the data on computer media: “mirror” images or copies of any portable media, hard disk or memory shall be created to ensure accessibility; record of all the actions during the copying process shall be kept and there shall be witnesses of the process in question; original media and log (should this not be possible, than at least one “mirror” image or copy) shall be safely kept and shall not be modified.

Any forensic works may be performed only on the copies of evidence material. Integrity of all the evidence material shall be maintained. Copying of evidence material shall be monitored by the competent personnel and a record shall be made about when and where the copying was made, who did the copying and about the tools and programmes used.

When a security event is initially detected, it may not be obvious whether it will become the subject of a judicial proceeding. Therefore, there is a risk that the necessary evidence may be destroyed deliberately or accidentally before the seriousness of incident is realised. It is recommended that the competent national authority is included in the early phase of any discussion about taking legal actions and to consulted about the necessary evidence.

Lesson Learned from Information Security Incidents
Article 10

CIRT shall be continuously developed in order to consider new threats, improved technology and lessons learned.

Meetings shall be held with all the involved parties after a serious incident, and periodically after minor incidents, in order to:

1) Analyse the incident;
2) Analyse main causes of the incident;
3) Take corrective and effective actions (in terms of processes, people and technology), and
4) Take possible preventive measures to reduce possibility of incident repeating.

Entry into Force
Article 11

The present Rulebook shall enter into force on the day of its signing by the Body Administrator.

Number:
Podgorica, _____ 2012

THE MINISTER
Vujica Lazovic PhD