ANNEX no. 1

Domains concerned by the minimum security measures

I. Security policy and risk management

Providers of public electronic communications networks or of publicly available electronic communications services have the obligation to:

1) establish an adequate security policy;

2) set up a risk management framework that should:

a) define the scope and basic criteria for the risk management process (risk evaluation criteria, impact criteria, risk acceptance criteria);

b) identify risks, by identifying the respective provider's assets, threats, vulnerabilities, the existing measures and the consequences that the loss/breach of security could have on the assets;

c) estimate the risks by assessing the possible impact of a threat that exploits a vulnerability of an asset and by assessing the incident likelihood;

d) evaluate the risk;

e) assess the options available for risk treatment, select risk treatment measures, setting the objectives of these measures and justify the accepted risks that do not meet the risk acceptance criteria;

3) establish an appropriate structure of the roles and responsibilities in ensuring the security and integrity of networks and services;

4) establish a policy regarding the security requirements for procuring products and services from third parties and for ensuring the maintenance or the management of products and services by third parties (IT services, software, interconnection, databases, associated facilities etc.).

II. Human resources security

Providers of public electronic communications networks or of publicly available electronic communications services have the obligation to:

1) perform background checks on candidates for employment, contractors and third parties in accordance with the applicable laws, regulations and ethics, proportional with the perceived risks;

2) ensure that their personnel have sufficient security knowledge and are provided with regular training regarding the security and integrity of networks and services;

3) establish an appropriate process for managing changes in personnel or changes in their roles and responsibilities;

4) establish a disciplinary process for employees who have committed a breach of security or integrity of electronic communications networks and services.

III. Security and integrity of networks, associated facilities and information

Providers of public electronic communications networks or of publicly available electronic communications services have the obligation to:

1) establish an appropriate physical security of the network and of the associated infrastructure (establish and maintain measures that should adequately protect against unauthorised physical access, damages produced by fire, flood, earthquakes, explosion, civil unrest and other forms of natural or man-made disaster);

2) establish appropriate security of supporting facilities, such as electric power, fuel or cooling;

3) establish appropriate security measures for (logical) access to the network and to the information systems;

4) establish appropriate security measures to ensure the protection of electronic communications networks and services against potentially malicious codes, unauthorised mobile codes and cyber attacks, including DoS/DDoS.

IV. Operations management

Providers of public electronic communications networks or of publicly available electronic communications services have the obligation to:

1) establish operational procedures and appropriate responsibilities;

2) establish procedures for the management of changes in the electronic communications network and in the application system software;

3) establish asset management procedures in order to verify asset availability and status.

V. Incident management

Providers of public electronic communications networks or of publicly available electronic communications services have the obligation to:

1) establish processes and procedures for managing incidents that affect security and integrity of electronic communications networks and services (internal incident reporting, incident assessment, incident response and escalation), including by defining roles and responsibilities;

2) establish an incident detection system;

3) establish an appropriate procedure of incident reporting to the National Authority for Management and Regulation in Communications, as well as to other responsible authorities, and to establish incident communication plans to third parties (affected providers of electronic communications networks and services, media, customers, business partners etc.).

VI. Business continuity management

Providers of public electronic communications networks or of publicly available electronic communications services have the obligation to:

1) establish a strategy for ensuring the continuity of the provision of electronic communications networks and services in the event of serious perturbations of the network or service operation;

2) establish capabilities for implementing the continuity strategy and establish continuity and recovery plans.

VII. Monitoring, testing and auditing

Providers of public electronic communications networks or of publicly available electronic communications services have the obligation to:

1) establish policies for system monitoring, as well as logging policies;

2) establish policies for testing, including by exercises, of the continuity and recovery plans in the event of serious perturbations of the network or service operation;

3) establish policies for testing equipment, systems and software, especially before their connection/connecting them to existing systems;

4) establish an appropriate policy for assessing and testing the security of all assets (equipment, systems and software etc.);

5) establish a policy for compliance monitoring and auditing, with a process for reporting compliance and addressing audit deficiencies.