Based on Article 30 of the Law on Classified Information (Official Gazette of the Republic of Macedonia, no. 9/2004), the Government of the Republic of Macedonia at its session held on 16.11.2004, passed the

DECREE
ON PHYSICAL SECURITY OF CLASSIFIED INFORMATION

Article 1

This Decree regulates the measures and activities for physical security for the protection of classified information, to be implemented by the state bodies, organizations, institutions and other legal and natural persons.

Article 2

The assessment of the possible breach of security of classified information is carried out from the aspect of:

- the number, classification level, form and flow of classified information;
- the immediate surrounding of the building where classified information is kept and the set-up of the security strap around the building; the security and administrative zones within the building; the physical construction, walls, doors and windows of the building;
- the condition of the wider surrounding of the building;
- the personnel working inside the building;
- the threat from intelligence activities, sabotage, terrorist or other types of criminal acts aimed against the classified information; and
- the procedures for handling of classified information and their safeguarding in the building.

Article 3

Plans for physical security shall be developed for each building separately, based on the assessment of the organization.

Article 4

The plan on physical security shall determine the security strap around the building where classified information is handled.

The security strap presents the minimum distance to the building which prevents, with utilization of active and passive means, the disclosure of the contents of the classified information.

Article 5

The plan on physical security shall also determine the security areas and administrative zones within the building where classified information is handled.

Class I and Class II security areas and administrative zones shall be identified in the building.

The marking of security areas and administrative zones shall be made visible.

Article 6

The areas where information classified CONFIDENTIAL and above is handled, need to be organized and structured so as to correspond to one of the following measures:

a) The entrance of the Class I security area, where information classified CONFIDENTIAL and above is handled, shall require:

- a clearly defined and protected perimeter through which all entry and exit is strictly controlled;
- an entry controlled system which admits only those individuals appropriately cleared and authorized to enter the area; and
- specification of the level of classification and the form of the information normally handled in the area, i.e. the information to which access is authorized.

b) Class II Security Area, where information classified CONFIDENTIAL and above is handled shall be protected from access by unauthorized individuals by controls established internally and such area requires:

- a clearly defined and protected perimeter through which all entry and exit is strictly controlled;
- an entry controlled system which admits unescorted entry only to those individuals who are security cleared and authorized to enter the area; and for all other individuals, provision shall be made for escorts or equivalent control for protection of classified information, to prevent unauthorized entry to areas subject to technical security inspection.

The stipulated conditions in this Article present the minimum standards for the Class I and Class II security areas, unless it is differently regulated by another regulation or international agreement.

Article 7

Those areas, which are not occupied by duty personnel on 24-hour basis, shall be inspected immediately after normal working hours to ensure that classified information is appropriately protected.

Article 8

An administrative zone shall be established around or leading up to Class I and Class II security areas. Such a zone requires a visibly defined perimeter within which the possibility exists for the control of individuals and vehicles. Only information classified RESTRICTED and UNCLASSIFIED shall be handled in the administrative zones.

Article 9

Besides the identification of sites and buildings requiring protection, the arrangement of the physical protection also includes the following multi-layer security measures:

- security fence;
- security lighting;
- intrusion detection system;
- access control;
- guards, i.e. guard service;
- closed circuit television;
- entry and exit control;
- visitor control; and
- approved equipment.

Article 10

The fence presents a physical barrier and identifies the boundary of an area requiring security protection. The level of protection offered by the fence shall depend on its height, construction and material used and any additional security features used to increase its security performance and effectiveness, such as: topping, perimeter intrusion detection systems, lightning or closed circuit television.

The effectiveness of the security fence shall depend on the level of security of the points of access. Gates shall be constructed to the same security standards as the fence. As required, certain gates shall have access control systems installed in order to provide appropriate protection.

Article 11

Security lightning shall be placed according to the minimum requirements for closed circuit television in order to enable continuous direct surveillance by the guards, and its installation shall correspond to the designated requirements.

Article 12

The intrusion detection systems on the fence shall be installed to enhance the level of protection. In order to avoid possible false alarm, additional alarm verification system (closed circuit television, guards, etc.) shall be used.

The intrusion detection systems may be used in buildings and rooms in place of, or to assist, guards.

The systems referred to in paragraphs 1 and 2 of this Article shall be supplemented by response force.

Article 13

The response force shall include at least two persons to any point of a security disorder on the site, without weakening site protection elsewhere.

The reaction of the response force to alarms or emergency signals shall be within a time limit evaluated as capable of preventing intruder's access to the classified information being protected.

The reaction time limit of the response force shall be tested regularly in order to ensure efficient and timely intervention.

Article 14

The access control shall be exercised in a building or buildings or to areas or rooms within a building. The control may be electronic, electro-mechanical, by a guard or receptionist, or physical. The personal recognition system governing the regular staff shall control entry into Class I and Class II security areas.

Article 15

Depending on the level of risk and any other security systems or equipment in place in the buildings where classified information is handled, a guard service may be employed.

The guards shall be appropriately cleared, trained and supervised.

Article 16

Closed circuit television shall be put in place to assist the guard service in verifying incidents and in addition to the alarm systems installed on the security fences or bigger buildings.

Article 17

The installed system for physical protection shall also include entry and exit control in order to deter the unauthorized introduction of materials in the rooms, or the unauthorized removal of classified information from the buildings. The entry and exit searches may be established with a warning notice displayed to indicate the implementation of such a security measure.

Article 18

Access to buildings and rooms in the security areas and administrative zones shall be permitted with access clearance.

Entry of vehicles in the security areas and administrative zones shall be permitted only if necessary.

A detailed check by an authorized person shall be carried out before each entry of the vehicle in the areas and zones referred to in paragraph 1 of this Article.

Article 19

The escorted or unescorted access of the visitors to security areas and administrative zones shall depend on: the previously competed security check of the visitors, the application of “need-to-know” principle, whether the visitor is a countryman or a foreigner and on the possible requirement for additional control.

Visitors who require escort shall be accompanied at all times. When visiting a number of departments or other members of staff, the visitors shall be handed over to authorized escorts in those departments and a note of the transfer shall be made in the access clearance.

Visitors who are permitted unescorted access to the buildings and sites requiring protection shall be required to wear an identification pass that shall differ from the pass of the staff members.

Article 20

When information classified CONFIDENTIAL and above is stored on open shelves or displayed on charts, maps, etc., in vaults and open storage areas constructed within Class I or Class II security areas, the walls, floors, ceilings and doors with locks must be approved by a competent authority according to the prescribed standards.

Article 21

Information classified TOP SECRET shall be stored within a Class I and Class II security areas.

Storage of the classified information referred to in paragraph 1 of this Article shall be done under some of the following conditions:

a) security containers, approved by a competent authority, with one of the following supplemental controls:
   - continuous protection by cleared guard or duty personnel;
   - inspection of the security containers not less than every two hours, at randomly timed intervals, by cleared guard or duty personnel; or
   - an intrusion detection system, approved by a competent authority;

b) in an open storage area which, besides the measures referred to in Article 26 of this Decree, is equipped with an intrusion detection system; or

c) in a vault equipped with an intrusion detection system.

Article 22

Information classified SECRET shall be stored within Class I and Class II security areas.

Storage of the classified information referred to in paragraph 1 of this Article shall be done under some of the following conditions:

a) in the same manner as prescribed for TOP SECRET information referred to in Article 21 of this Decree; or

b) in approved security containers or vault without supplemental controls; or

c) in an open storage area, in which case, one of the following supplemental controls is required :

- continuous protection of the location that houses the open storage area by cleared guard or duty personnel;
- inspection of the open storage area once every four hours by cleared guard or duty personnel; or
- installed intrusion detection system.

Article 23

Information classified CONFIDENTIAL shall be stored in the same manner as prescribed in Articles 21 and 22 of this Decree, except that supplemental controls are not required.

Information classified RESTRICTED shall be stored in office furniture (desk, wooden or metal cupboard, etc.) with a lock.

Article 24

Keys of security containers shall not be taken out of the office building.

Combination settings of security containers shall not be written down by individuals needing to know them. Spare keys and a written record of each combination setting for use in an emergency shall be held in sealed opaque envelope by persons within the organization authorized to handle classified information.

Working and spare security keys shall be kept in separate containers.

The keys, combinations and the envelopes shall be given security protection no less stringent than the information to which they give access.

Knowledge of combination settings of security containers shall be restricted to the smallest possible number of staff members.

Article 25

The keys and combinations settings shall be at regular intervals not exceeding 12 months.

The keys and combinations settings shall be changed :

- on the procurement of the container and before the first use; or
- whenever a change of personnel knowing, i.e. using the combination occurs; or
- whenever a justified suspicion of their compromise has occurred.

Article 26

The level of physical security of the information and communication devices, the copying and microfilming devices and machines and other devices processing or storing classified information is required to be equivalent to the level of classification of the information stored in or used by those devices and machines.

Article 27

The open storage areas for classified information shall have:

a) perimeter walls, floors and ceilings made in solid construction without assembling elements;

b) construction done in a manner so as to provide visual evidence of unauthorized penetration;

c) doors shall be constructed of wood, metal or other solid material. Entrance doors shall be secured with a built-in approved three-position combination lock, or in special circumstances, other locks approved by a competent authority, only for rooms where SECRET and CONFIDENTIAL information is stored. Additionally, doors shall be secured from the inside with either deadbolt emergency egress hardware, or a rigid wood or metal bar which extends across the width of the door, or by other means approved by the authorities;

d) vents and ducts larger than 620 square centimetres (or over 15 centimetres in its smallest dimension) that enter or pass through an open storage area shall be protected with either bars, expanded metal grills, commercial metal sounds baffles, or an intrusion detection system;

e) all windows shall be made of sound material or equipped with blinds, drapes, or other coverings.

Windows at ground level, or other easily reachable windows (from roofs, verandas, and building annexes) will be constructed from or covered with materials that provide protection from forced entry.

The protection provided to the windows need be equivalent to the strength of the contiguous walls.

For the open storage areas that are located within a controlled compound or equivalent it is not required to provide protection against

forced entry if the windows are made inoperable, either by permanently sealing them or equipping them on the inside with a locking mechanism and they are covered by an intrusion detection system, either independently or by the motion detection sensors within the security area.

Article 28

During transfer of classified information outside the security areas and administrative zones, appropriate protection shall be provided according to the level of classification.

Classified information shall be transferred outside of security areas and administrative zones sealed in an envelope and by certified couriers.

For information classified TOP SECRET:

- written records shall be maintained of all individuals having taken part in the transfer;
- transfer shall be done by a specific equipped vehicle; and
- the courier shall be accompanied by at least one person.

Article 29

Buildings and sites that naturally require audio protection of information classified SECRET and above, shall be protected against methods and devices for passive and active eavesdropping, by taking measures for sound physical security and access control to sites where the risk warrants it.

Prevention of the leakage of classified information by wired microphones, radio microphones or other implanted devices requires a technical and/or physical security inspection of the structure of the room, its furnishings and fittings and its office equipment, including office machines (mechanical and electrical) and communications.

These inspections shall be undertaken by trained security staff authorised by the head of the organization.

Article 30

Areas which have been protected against audio eavesdropping are to be designated as technically secure areas with specially controlled entry.

When not occupied, the rooms must be locked and/or guarded in accordance with physical security standards and any keys treated as security keys.

The areas referred to in paragraph 1 of this Article shall be regularly inspected and, if necessary, periodically, as well as in circumstances of any unauthorised entry or suspicion of such and entry by external personnel for maintenance work or redecoration.

Article 31

Before being allowed into technically secure areas, the furniture and equipment shall be appropriately examined for possible eavesdropping devices by qualified security staff. A record of the type, serial and inventory numbers shall be maintained of items moved into and out of these areas.

Article 32

Telephones shall not normally be installed in areas which are technically secure, unless necessary. If a telephone has been installed, it shall be provided with a positive disconnect device or shall be physically disconnected when classified discussions take place.

Article 33

Mobile telephones and other electronic and technical items shall not be allowed to technically secure areas.

Article 34

In addition to the physical searches of the areas where classified discussions take place, regular technical security inspections shall also be exercised for possible planted devices and to investigate the telephone system or other electrical devices that could be used as an attack medium.

If necessary, critical points for the security of classified information shall be identified within the areas referred to in paragraph 1 of this Article, as a preventive measure against intelligence activities.

Article 35

Before being used in the areas where discussions are held or work is being performed which involves information classified SECRET and above, the communications equipment and electrical or electronic equipment of any kind shall be examined to asses their technical or communications security by experts qualified in technical and communications security.

Article 36

When a possibility exists for overlooking of a classified information under daylight or artificial light conditions, appropriate measures shall be taken for visual protection.

Article 37

This Decree shall enter into force on the eight day from the day of its publication in the “Official Gazette of the Republic of Macedonia”.