



ეროვნული თავდაცვის აკადემია NATIONAL DEFENCE ACADEMY

Appendix N1



LEPL - Information Technology Management Policy of the David Agmashenebeli
Georgian National Defence Academy

Gori

2021

Article 1. General provisions

1. Management Policy (hereinafter referred to as the Policy) defines the information technology management policy and procedures implemented at the Georgian National Defence Academy (hereinafter referred to as the Academy), the rules for the use of information systems and electronic services, regulations, and development mechanisms;

Article 2. Purpose of the Policy

The goal of information technology and systems management is to provide and support cadets/trainees, academic and visiting staff, teachers, instructors, civilian and military personnel with appropriate infrastructure and effective information systems in the process of teaching, learning and administrative work. The goal of the policy is to ensure network security, accessibility and smooth operation.

Article 3. Information Security Management and Responsibilities

1. The Academy's Distance Learning Center and the G6 Service of the Academy's Headquarters are responsible for implementing the policy and ensuring its updating;
2. Continuous monitoring is being carried out to monitor security and eliminate threats through the Cyber Security Bureau of the Ministry of Defense, the Information Technology Department of the Ministry of Defense, the Information Technology Division of the Communications and Support Center of the Defense Forces General Staff, and the Defense Forces J-6 (Communications and Information Systems Department).

Article 4. Business continuity

1. In the field of information technology, the Academy has outlined the categories of risk factors in its business continuity plan document, where one of the risk factors is the "technological" factor, which implies:

- a) the potential risk of disruption/disruption of internet telephony services;
b) the potential risk of cyberattacks.

2. In order to eliminate risks, the business continuity plan includes a list of preventive measures:

- a) Alternative means of communication, 2 telephone lines (digital, analog radio stations);
- b) Regular antivirus updates, constant updating of programs, LEPL - control of the Cybersecurity Bureau of Georgia.

3. The Academy's network and server equipment and all computers are equipped with an uninterruptible power supply (UPS), which ensures the elimination of the risk of information loss in the event of a power outage and the uninterrupted operation of the systems. The long-term continuity of the entire system is ensured by a backup generator connected to the Academy's power supply;
4. For the purpose of storing information, so-called backup copies (backup, replication) have been created, which are located on the Academy's servers and are stored for 7 days.

Article 5. Infrastructure

1. The Academy is equipped with all the necessary material and technical resources for the implementation of the educational process. Including: classrooms equipped with the Internet, an examination center equipped with appropriate software, a library equipped with computers, a CISCO equipment and network study laboratory equipped with computers, a physics laboratory, a chemistry laboratory, and an electricity study laboratory. Projectors are installed in the classrooms, and SMARTBOARDS are installed in the language school classrooms;
2. The Academy will allocate a laptop computer to each cadet, the technical maintenance and updating of which will be provided by the G-6 Service of the Academy Headquarters;
3. The G-6 Office of the Academy Headquarters, prior to the start of the academic semester, takes into account the requirements of the higher education program, based on which computer classes, laboratories, or other spaces are provided.

Article 6. Management of computer networks

1. Since the Academy is a LEPL of the Ministry of Defense of Georgia, the Academy's computer equipment is integrated into the internal network of the Ministry of Defense. In addition, a cable and wireless network (WI-FI) has been implemented throughout the entire territory of the Academy for providing Internet access;
2. The Academy's internal network, which is managed from the servers of the Ministry of Defense, receives IP addresses from a list (Range) allocated by the Ministry of Defense, which is assigned statically, while the addresses of computers and devices connected to the wireless network (Internet) are assigned to the router, which automatically (DHSP) assigns the address;
3. Correspondents who use the global network have access only to the allowed categories of web pages;
4. For the smooth and uninterrupted operation of the internal network and to prevent the spread of viruses, the Academy's network has been installed with Symantec antivirus, which is managed from the servers of the Ministry of Defense. The majority of users are included in the Ministry of Defense domain;
5. The G6 service of the Academy Headquarters, in particular, the Information Technology System Administration Specialist, ensures the full and uninterrupted operation of the network.

Article 7. Information Technology Administration.

1. Access to the necessary information is carried out in accordance with the requirements of the educational processes;
2. Access to information for the administration and other users is carried out in accordance with the established procedure; if necessary, access to information is provided in agreement with the commander of the academy or deputy commanders;
- . Employee access to Academy information is subject to control (by blocking IP addresses of unwanted sites, placing them in a “black list”, which is provided by the G6 service of the

1.1.2. Timely translation of information into English is ensured by translators from the Academy's library;

