Decree of the Rector of Saint King Tamar University of the Georgian Patriarchate, NCLE (non-commercial) legal entity

№069/01 December 5, **2018, Tbilisi**

On Approval of Information Technology Management Policies and Procedures of Saint King Tamar University of the Georgian Patriarchate

According to the Law of Georgia - Article 35 of the Civil Code of Georgia, "On the Approval of the Statute and Fees for the Authorization of Educational Institutions" of the Minister of Education and Science of October 1, 2010 № 99 /, non-commercial legal entity – Saint King Tamar University, Pursuant to Article 4, Part 3, Article 14, Part 1, Part 3, Paragraphs "B", "E", "F" and "L" of the Charter of the named University and Part 4, I decree:

1. The information technology management policies and procedures of Saint King Tamar University of the Georgian Patriarchate to be approved in accordance with the Annex.
2. A copy of this order shall be made public.
3. To send this order to the structural units / staff of the University within their competence.
4. I shall personally control the execution of the order.
5. The order may be appealed in accordance with the rules established by the legislation of Georgia.
6. The order shall enter into force upon signing.

Professor, Archimandrite Adam (Vakhtang Akhaladze)

Annex

Information Technology Manageent Policies and Procedures of the Saint King Tamar University NCLE of the Georgian Patriarchate

Article 1. General Provisions

1. This document defines the information technology management policy, information technology management procedures, information technology infrastructure and development mechanisms in the administrative activities and educational process of the University of Saint King Tamar University of the Patriarchate of Georgia (hereinafter - the University).

2. Adherence to the relevant parts of the present rule is mandatory for all persons who use the information technologies and resources of the University in their administrative, technical, academic, scientific or student activities.

3. University Information Technology User (hereinafter - User) is obliged

In addition to this rule, to comply with the requirements established by the legislation of Georgia regarding the protection of intellectual property, information technology security and personal information.

Article 2. Objectives of IT Management Policy

1. Information security policy ensures the establishment of information security control mechanisms at the University.

2. Areas of information security policy protection are:

a) Electronic information infrastructure of the University;
b) Basic data and information available at the University;

b) Persons who use or administer information systems;
c) Persons who manage key data and information.

3. The policy defines:

a) Protection of the University in terms of confidentiality, integrity and accessibility of information;

b) Responsibilities for information security.

Article 3. Physical security

1. The University exercises control over unauthorized access to information assets to prevent interference, kidnapping or injury.

2. It is mandatory to ensure the security of computer systems and networks by physical, with technical, procedural and environmental safety control mechanisms.

3. The University exercises physical access control over devices that contain or process highly critical and / or sensitive information. Such devices are placed in a physically protected place.

Article 4. Information Security Incidents

1. The University is obliged to identify security incidents, which also includes the study, description and adequate response to each incident.

2. The person (s) responsible for the operation of the University Information Technology System shall periodically report on information security incidents, their sources (internal, external), their forms (DDoS, Keylog, etc.), along with correction and optimization recommendations.

Article 5. Communications and Operations Management

The University carries out constant control over information processing devices to ensure their correct and safe use.

Article 6. Development and planning of a new system

In the process of planning and implementation of systems, the technical and functional capabilities of the systems should be taken into account in order not to interfere with the proper operation of critical systems.

Article 7. Control over malicious programs

Control of critical systems is essential to prevent the use of malicious or fraudulent software.

Article 8. Protection against viruses

1. The University shall exercise appropriate control to prevent the spread of viruses within the University and for the cause of the University - outside it.

2. Backup of all critical systems, applications and basic data is done synchronously on the university Google drive.

Article 9. Computer Network Management

1. Mac addresses of computers and devices connected to both the physical and wireless network at the University that belong to the University assets are pre-written in the router, which assigns a pre-selected IP address.

2. Devices that do not belong to the assets of the University and use the University Wireless Network (WiFi), use a special dedicated network, through which they can access only the category of allowed web pages,

Which are pre-selected.

Article 10. Security of systems during testing and design

1. Systems are tested in an isolated environment to protect critical systems from accidental destruction and / or damage.

2. The business continuity strategy developed and its operation should ensure the reduction of the risk of sudden interruption in the process of processing information of the University and its timely recovery.

3. In case of failure of the main router, the backup router is switched on within 10 minutes after the result.

Article 11. Information Technology Infrastructure and Access

1. University IT infrastructure includes:

a) Technical equipment, including:

aa) physical servers with appropriate software;

ab) computer programs operating in the structural units of the University;

ac) computers / laptops, projectors (including several interactive ones) and copiers; "

b) software (Microsoft Windows, Microsoft office, Adobe (Photoshop, Premiere, Dreamweaver, Illustrator, InDesign), Lira, Sketchup, Autocad, Mathcad, Dev-C ++, Oris, Opera, Codex, Web Browser (Chrome, Mozilla); and Other, which are distributed as needed in structural units;
c) Internet, which is accessible to all computers located in the university building (s).

2. The IT infrastructure of the University is available to the University staff and students:

a) Computer equipment connected to the Internet:

aa) The so-called "Computer classes" - during the course of lessons (hours);

ab) on computers located in corridors and in the library - at any time;
ac) equipment placed in work rooms - relevant staff;

b) Wireless Internet - at any time (is free, without password);

c) Projectors - during the auditory lessons (hours), as well as at any time, if necessary;

d) Copiers - during university working hours.

Article 12. Information Technology Management Procedures

1. The IT management of the University is provided by the University Records and Information Support Service. These procedures include:

a) Server management:

aa) technical support (assembly, further exploitation);

ab) Software (installation, further exploitation).

b) Management of computer equipment:
ba) technical support (assembly, further exploitation);

bb) Software (installation, further exploitation).

c) Internet management:

ca) Internet call hardware and software;
cb) Restriction according to the needs of the Internet.

d) Software management: retrieval; Installation and operation.

e) Website administration: design development, information retrieval and software;

f) Management of the job posting registration system (access devices): technical control, adding / deleting the user / restoring the user card (based on the report card);

g) Management of the video-surveillance system: technical control and storage in accordance with the rules established by law, disabling / activating the video recording, viewing the video recording / allowing other persons to see it (based on the legal act of the Rector);

h) Management of technical damage cases: clarification of the problem, preparation of a conclusion (if necessary), removal of the necessary parts from the warehouse, correction of the technical defect (if it can be solved at the current stage through the resources available at the University);

i) Software damage case management: problem correction and software bug fix.