AGENCY OF THE UNIVERSITY OF LATVIA
P. STRADINS MEDICAL COLLEGE OF THE UNIVERSITY OF LATVIA
Registration Nr. 90000031813, Vidus prospekts 38, Jūrmala, LV-2010
Telephone 67752507, fax 67752214, e-mail: st-skola@apollo.lv

APPROVED
By the College Board
of the P. Stradins Medical College
of the University of Latvia
in session of January 21, 2020,
protocol Nr. 1

INFORMATION SAFETY POLICY

Jūrmalā

Issued in accordance with the General Data Protection Regulation and the Personal Data Processing Act

1. Definition of the terms used

College	P. Stradins Medical College of the University of Latvia, Reg. Nr.90000031813, Vidus prospekts 38, Jūrmala, LV-2010.
Employee	An individual employed at the college.
Direct manager	A representative of the College, specified in the Employment or other contract, or appointed by an order of the College as the immediate supervisor of the Employee.
Management	The administration and / or any other person in the College to whom management functions and powers have been delegated.
Policy	This Information safety policy.
Third person	An individual or a legal person who is not an employee of the College.
Network security breach	Such security breaches include, but are not limited to, access to data if the Employee is not the intended recipient, or logging in to a server or account which the Employee is not expressly authorized to access, unless such access is granted to the Employee in connection with a particular College project;
Copyright	A set of personal non-material and economic rights of an author to his/her own intellectual work in its material form.
Information	A message or set of messages in any technically possible way of capturing, storing or transmitting.
Personal data	Any information relating to an identified or identifiable individual ("data subject"); an identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as his/her name, identification number, location data, online identifier or one or more physical, physiological, genetic, factors of spiritual, economic, cultural or social identity.
Personal identification data	Name, surname, identification, birth data.
Data subject	Identified or identifiable individual.
Server	A computer or system that transfers information to other computers called clients. These clients can access the server computer at fault via a local area network) or the Internet.

Account	A security mechanism used to control access to a computer system or network. The user account contains information about the user's name, password, their rights, and possibly other information that allows the user to be identified.
IT	Information technologies
User ID	A unique customer identifier by which the College identifies users accessing the Information Systems.
Information system	A structured set of information technology and databases (such as, but not limited to, hardware, software, operating systems, any storage environment, network accounts, e-mail accounts, browser systems) that provide, generate, compile information necessary to perform the College's functions; storage, treatment, use and disposal.

2. Purpose and volume

2.1. The purpose of the College information security system is to protect the College staff, partners and students from illegal or harmful direct or indirect, intentional or unintentional actions of persons by processing information and data available to them and using certain equipment to perform their duties.

2.2. The policy governs processing of information in any information system involved in the processing of data / information by the Authority, regardless of whether the processing of data / information is related to the internal activities of the College or the external relations of the College with any Third Party.

2.3. This Policy also governs the use by College Staff of the equipment and tools available to them to perform their duties.

2.4. The Policy may be applied in conjunction with any other policies, rules, procedures and / or guidelines adopted and implemented periodically by the College.

2.5. For all information security system issues and information / data security issues not covered in this Policy, Employees should contact the computer network maintenance administrator.

2.6. This Policy must be communicated in writing to all Employees and ensure that they understand it. Where necessary, staff training should be provided to develop a common and sound understanding of IT and personal data protection issues.

3. Information classification

3.1. Any information / data that becomes available to Employees in the performance of their duties, if such information / data relates to the College and its activities, employees, students or affiliates, shall be considered proprietary and confidential information protected by applicable laws and regulations. protection of confidential information and personal data.

3.2. To ensure the protection of information and data, the College maintains an internal classification of information. The information / data is protected regardless of whether such information has been made available to the Employee in printed, electronic or any other form.

3.3. The College uses the following general classification of information:

Category	**Description**	**Content**
Public information	Information that may be developed, processed, and disseminated within or outside the College without any adverse impact on the College, any of its Employees, students, and / or affiliates.	a) Public financial statements provided to public authorities. b) Information that is available in public resources or is otherwise in the public domain, unless it has become public knowledge because the Employee acted in violation of

		information / data security requirements.
Internal information	Any information, the use of which in any way, in violation of applicable laws, the requirements of this Policy or any other regulation adopted by the College, may harm the interests of any of its Employees, students and / or affiliates.	a) Documents developed and / or prepared by any College employee. b) Any catalogs (contacts, information, etc.) created and / or used for the purposes of the College's activities. c) Any internal document developed for the purposes of the operation of the College.
Confidential information	Any information that is so relevant to the College, any of its Employees, students and / or affiliates, that the unauthorized disclosure of which could adversely affect the business, reputation, status of the College, its Employees, students and / or affiliates in general, and any these persons may be seriously harmed.	a) Policies, procedures, internal regulations, management decisions (except for those documents whose publication is required by law). b) Information provided to the Employee as restricted information. c) Personal identification data. d) Information protected by a confidentiality agreement signed by each Employee (if any). e) Information protected by confidentiality agreements or cooperation agreements entered into by the College in the course of its activities.

4. Systems involved in data / information processing

4.1. Any information/ data used in the operation of the College is considered the property of the College. Any information systems, including, but not limited to, hardware, any storage media, network accounts, any other technical base, and tools used in the operation of the College are the property of the College.

4.2. It is the duty of each Employee to use the technical equipment and tools with due care and attention and only for purposes related to the activities of the College. The only exception is when the College has provided the Employee with technical equipment (such as a mobile phone device) with explicit consent to use it for personal purposes.

4.3. Only systems and software licensed and authorized by the College may be installed and used on the equipment used by the College. Prior to downloading or installing any software on devices owned and used by Employees for the purposes described in this Policy, permission must be obtained from IT personnel.

4.4. The College audits the systems used to process information / data to monitor continued compliance with this Policy and applicable regulatory requirements.

5. Duties of employees

5.1. Any information / data obtained by the Employee in the performance of his/her duties is treated as confidential and used in a confidential manner in accordance with this Policy and shall not be disclosed to any Third Party unless Management discloses that such information has become public or has been otherwise reclassified as information that is no longer protected under this Policy.

5.2. All personal data and other information by which an individual may be identified are to be collected and processed only if and to the extent necessary for the performance of the

Employee's duties, provided that such activities are carried out within the limits of the powers conferred on the Employee and in accordance with regulatory enactments. data protection requirements (in particular Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data) and repealing Directive 95 / 46 / EC (General Data Protection Regulation)).

5.3. Any request for information / data and / or a request for information / data processing received by the Employee from data subjects in the performance of their duties must be forwarded to Management immediately for further consideration.

5.4. Each Employee is obliged to comply with this Policy, as well as to comply with the requirements of the applicable legislation of the Republic of Latvia or international laws (for example, Labor Law, Personal Data Processing Law, General Data Protection Regulation, etc.), which stipulates information / data processing and protection.

5.5. Failure to comply with the policy is considered a material breach of the established agenda and, as a result, the College may, in the discretion of the College, impose a disciplinary sanction or terminate the employee's employment. This may result in the infringing Employee being held administratively or criminally liable.

6. Access and security management

6.1. Employees may access any of the College's facilities as required for the performance of their respective duties. The right of access to any information system does not mean that the Employee is authorized to view or use all the information in the relevant system - Employees have the right to use only the data necessary for the performance of direct work duties.

6.2. Employees are identified by a user ID. Each Employee is responsible for all activities related to the User ID, therefore the primary responsibility is to ensure that the User ID is not available to any Third Party and other Employees, unless otherwise specified by the College.

6.3. System security passwords are created on the condition that they cannot be easily remembered, they consist of at least 9 characters (including uppercase and lowercase letters, numbers, and special characters) and do not contain personal data. Security passwords are changed regularly (at least once in 3 (three) months). Each Employee is personally responsible for ensuring that his or her security password complies with this Policy and other College regulations.

6.4. The Employee will have access to confidential information / data only if such authority is provided for in the Employment or other contract of the Employee concerned and / or if such authorization has been granted to the Employee by the College.

7. Safety measures

7.1. All data and information collected and processed in any form (printed, electronic, etc.) is subject to the requirements of this Policy and any regulatory framework for the collection, processing, protection and storage of data / information and must be stored in a secure location designated by the College. The term prescribed by the applicable laws (for example, the Labor Law, the Law on Higher Education Institutions, the Law on Processing of Personal Data, etc.) and / or specified by the College.

7.2. Employees are prohibited from storing confidential information on their personal devices, except for information that is temporarily required for a specific work-related activity. All necessary confidential information should be stored only on a server approved by the College's IT staff. Any downloading of such data to computers should be avoided and should only be done if there is a reasonable need to process the information for work purposes.

7.3. If the College has a reasonable suspicion that an employee has processed unjustified data, the College's IT staff is entitled to filter and monitor the employees' internet access and activities in accordance with the requirements of applicable laws and regulations.

7.4. Any mobile, portable devices (including laptops, tablets, smartphones, and other handheld devices) and any storage location on the server must be approved by the IT staff of the College to prevent unauthorized access.

7.5. In cases where Employees use personal (home) devices to access the College's corporate resources (eg, e-mail, online / databases), Employees are required to comply with the requirements of this Policy in the same manner as when using the equipment provided by the College. It is forbidden to store any personal data related to the College on a personal (home) device. Any processing of data is permitted only through the online storage facilities used by the College.

7.6. The use of public access devices for work purposes (eg in Internet cafes, libraries, etc.) is prohibited unless it is critical and urgent in connection with the work and the Employee's immediate supervisor has given explicit written consent to do so.

7.7. In the event that an Employee is granted access to the partner storage system of the College, the Employee is required to use the assigned ID and follow the instructions for secure information / data processing requirements (including encryption system, use of passwords, data usage restrictions, use of dedicated locations). etc.).

7.8. As soon as, in the opinion of the College, the protected data / information is no longer necessary for the operation of the College, such data / information must be deleted, all copies thereof destroyed. The staff involved in the processing must delete and destroy or hand over to their direct manager College information / data no longer required for the performance of their duties, in particular when the employment relationship with the staff member concerned is terminated.

7.9. No information / data referred to in this Policy must be transmitted, forwarded or otherwise provided to a Third Party unless necessary for the performance of the Employee's duties. In the event that data is transferred or provided to a third party, data protection must be ensured and all appropriate security measures must be taken.

7.10. The IT specialist must perform a risk analysis of the information systems (both before the start of operation of these systems and regularly - at least once a year). The risk analysis must be documented.

7.11. The IT specialist must ensure regular recording and monitoring of information system events.

8. Prohibited activities

8.1. Under no circumstances and by no means may any equipment or systems belonging to the College be used for purposes other than those of the Employee or for the purposes of the activities of the College.

8.2. The following activities are strictly prohibited:

8.2.1. infringing the copyrighted rights of any person or the College, including, but not limited to, installing, copying, distributing or storing any illegal software, online platforms, any other electronic content not licensed by the College on any system or equipment of the College;

8.2.2. infringement of the rights of any person through the excessive and unnecessary collection and processing of personal data of the data subject;

8.2.3. access to Personal Data for purposes other than the College activities or the performance of the employee's duties;

8.2.4. exporting software, technical information, encryption software or technology in violation of this Policy;

8.2.5. export of any data or information to which the College has ownership and / or confidential value, unless required in the course of the College's activities or the performance of the Employee's duties and / or in violation of the College's internal regulations and applicable laws and regulations;

8.2.6. disclosure of an employee's password to other persons and permission for other persons to use the employee's account (including, but not limited to, the employee's family members);

8.2.7. implementation of network communications security breaches or interruptions;

8.2.8. use any program or send any kind of message to disrupt a user's work session.

9. Reporting security incidents

9.1. All security incidents or suspected incidents of information / data processing errors must be reported immediately to Management, which will take steps to prevent the potential damage, eliminate the consequences of damage caused, and restore the previous security situation.

9.2. In the event of a personal data breach, the College Management must, within 72 hours of becoming aware of personal data breach, notify the Data Protection Inspectorate of the personal data breach, unless the personal data breach is unlikely to pose a risk to an individual. rights.

9.3. The College must document all personal data breaches, indicating the facts surrounding the personal data breach, its consequences and the corrective actions taken.

9.4. The College must take the necessary steps to prevent the recurrence of an identical or similar security incident.

10. Concluding remarks

10.1. The College provides its staff with access to the Policy on "Internal Quality Assurance System" on the College server.

10.2. “Information Security Policy” will enter into force on January 21, 2020.