Safeguarding Customer Information

Poznan University for Medical Sciences is in compliance with the requirements of Safeguarding Customer Information:

Requirement	Offices Responsible	In Compliance? (Yes or No?)*
All customer information is safeguarded. This requirement applies to all nonpublic personal information in the school's possession (from students, parents, or other individuals with whom the school has a customer relationship). It also pertains to the customers of other financial institutions that have provided such information to the school.	**The President and the appointed administrator of personal information**	**Yes**
The school establishes and maintains a comprehensive information security program. This program must include the administrative, technical, or physical safeguards the school uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information. The safeguards achieve the following objectives: - Insures the security and confidentiality of customer information - Protects against any anticipated threats or hazards to the security or integrity of such information, and - Protects against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer	**Persons listed above plus the head of IT Department**	**Yes**
The school includes all required elements of an information security program: - **Designated Coordinators.** The school designates an employee or employees to coordinate its information security program. - **Risk assessment.** The school identifies reasonable foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks. At a minimum, the school's risk assessment includes consideration of risks in each relevant area of operations including: o Employee training and management o Information systems, including network and software design, as well as information processing, storage, transmission, and disposal o Detecting, preventing, and responding to attacks, intrusions, or other systems failures - **Safeguards testing/monitoring.** The school has implemented information safeguards to control the risks it identifies through risk assessment, and regularly tests or otherwise monitors the effectiveness of the safeguards' key controls, systems, and procedures **- Evaluation & Adjustment.** The school evaluates and adjusts its information security program in light of the results of the required testing and monitoring, as well as for any material changes to its operations or business arrangements or any other circumstances that it has reason to know may have a material impact on the school's information security program. **- Overseeing service providers**. The school takes reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue and requires the service providers by contract to implement and maintain	**As listed above**	**Yes**

Details are provided by Personal Data Policy of Poznan University of Medical Siences established by The President of PUMS, policy is available here:
http://bip.ump.edu.pl/?app=zarzadzenia&nid=3777&y=2019&which=Rektora
(currently policy is available in Polish only, translation to English will be available shortly).