NITOMANI SCHOOL INC'S DATA SECURITY POLICY

Nitomani School has hereby decided on May 24th, 2018 to accept this information security policy.

The information security policy determines the principles, responsibilities, methods and monitoring, that are followed in Nitomani School's activities in relation to managing and developing information security. The information security policy is reinforced by a registry caption and an information security plan.

1. INTRODUCTION

Information security means a space, where threats to information, information systems and traffic's confidentiality, integrity, and usability do not cause a significant risk. Information security means protecting personal information from unauthorized and harmful use and handling.

Information security policy determines the principles, responsibilities, methods, as well as monitoring and supervision that are followed in fulfilling and developing information security. Information security is reinforced by a registry caption and an information security plan.

2. COVERAGE

The information security policy covers all information management tasks related to every activity of the operating department.

Every employee, contract partner and user of the operating department's information systems must know this information security policy, and obey guidelines and orders based on it. Operatives, reporters and other parties outside the company are to adhere to this information security policy, national norms, and instructions, that are conditions for task-compatible accessing to the information systems of the company and its services, as well as their information material.

3. INFORMATION SECURITY

Information security means the protection of information handling and archiving. Information security builds from the confidentiality, integrity, accessibility, usability, and undeniability of information, as well as the monitoring of information handling.

Information security includes a person in charge of security, the practices of information handlers, the methods, tools, and actions of protecting information, the resources allocated to work, as well as the security properties of equipment and working spaces.

Information security following an accepted information security policy must be implemented as a natural part of all activity. The monitoring, development and upkeep of information security's legality is a part of the company's common security practice, risk management, and internal monitoring.

4. INFORMATION SECURITY WORK

Information security work is monitoring, as well as planning and executing task operations, in order to achieve information security. The goal of information security work is to secure an uninterrupted performance for information systems and networks that are important to the operating department, prevent information and information systems from getting to outside parties, as well as prevent unauthorized use, intentional or unintentional destruction or corruption of information and

minimizing the resulting damage. On top securing the information handling of normal activity, we will prepare for threats that interrupt operations and how to recover from them.

5. ORGANIZING AND RESPONSIBILITIES

Information security is primarily lead and monitored by the board of Nitomani School Inc., which has given the responsibility to and authorized the CEO accordingly:

The CEO decides the goals, organization, resources and authorities of development operations of different areas of information security, and names the registry keeper and, if needed, information handlers.

The CEO is in charge of defining, evaluating and reporting the operating department's information security level, as well as other administrative information security. They oversee the performing of information security practices, monitoring the execution, advancing the general knowledge of information security, and secure practices within the company and the services it has bought, as well as reporting to the board for their monitoring purposes.

The CEO oversees the protection and monitoring of user registries, as well as other security of use.

The CEO oversees the security of hardware and software, as well as the security of working space and technology in collaboration with suppliers/subcontractors.

The CEO oversees employee security in information security matters.

All company information systems belong under the responsibilities of the CEO. The CEO is responsible, on the part of information systems, for defining the requirements of activity and security of the information systems when needed and admitting and monitoring usage rights.

The board of Nitomani school oversees the guidance, informing and monitoring of information security matters.

Every employee, information handling administrator and user of information systems or networks is on their own part, under laws and regulations, responsible of executing information security and following information security guidelines. Each personnel has a duty of reporting to the Nitomani School board and CEO about any threats and errors.

6. THE EXECUTION OF INFORMATION SECURITY

The basis of executing information security is this formally written information security policy, which is informed to every employee and information systems user, as well as other potential contract- and collaborative partners.

The operating department's information security principles are based on the European parliament and council's regulation (EU) 2016/679 about protecting individuals in the handling of personal information, its free movement, and the regulations, instructions and standards of directive 95/46/EY (general information security decree), that guide and oblige national, general and industry specific information security, user registry, good manner of information management and information quality. The changes in rule of law and guidance are taken into account in the development of the information security of the operating department.

The execution and administration of information security is depicted in detail in the information security plan. The achieving of information security goals is a continuous process that happens through administrative and technical solutions. User activity is guided by user guidelines in the

information security plan, as well as by verified and available guides and information security training. Every employee, collaborative- and contract partner of the company must sign an information security commitment. On the part of collaborative- and contract partners, signing the commitment is required if other personal information than those of the partners themselves is exchanged.

When they receive the right to use the information systems and materials in accordance with their tasks, the user must sign the information security commitment.

7. THE ADMINISTRATION AND MONITORING OF INFORMATION SECURITY

The users and administrators are to report of security risks, misuse of information security or suspected breach of information security to the Nitomani School board or CEO.

The Nitomani School board and CEO are have the task of overseeing the execution of information security in the company.

The CEO’s task is to follow and monitor the execution of the information security of the information systems and begin procedures in order to fix any noticed weaknesses in the information security.