INFORMATION SECURITY POLICY

1. Purpose

The purpose of this Policy is to establish standards for protecting the information and assets of Nimbus Software or its information system from various threats and to ensure business continuity, minimize damage, maximum return on investment, legal compliance and improve the image.

2. Scope

This Policy applies to all employees of Nimbus Software. It also applies to Nimbus Software's contractors, consultants, temporaries, third parties, further appointed in this document as Nimbus Software cooperators.

This Policy applies to all equipment that is owned or leased by Nimbus Software.

3. Information Security Policy

Information regardless of the form in which it is (written, spoken, printed, and electronic) is a primary asset for the business, that has its value and therefore it is necessary to adequately protect it. Information together with other components (people, facilities, equipment) makes up the information system of Nimbus Software.

In order to protect the information and assets of Nimbus Software or its information system from various threats (computer fraud, espionage, hacker attacks, viruses, floods, fires, earthquakes, etc.) and to ensure business continuity, minimize damage, maximum return on investment, legal compliance and improve the image, the Management Board of Nimbus Software has approved the security policy that sets goals and fundamental principles for establishing effective information system security.

The Management Board is directly responsible to provide clear and concrete support in the implementation of security policy and monitor its application in daily operations by delegating responsibilities and establishing an appropriate organizational structure.

To achieve the goals, Management Board appointed a person responsible for information security, Information Security Manager. His role and duties are governed by a special act, *Information Security Manager Responsibilities.*

The Information security manager is the owner of the Information Security Policy.

To meet the security goals, it is necessary to take measures and implement security controls to protect and ensure the three basic principles for information system security:

Confidentiality - protecting information from unauthorized disclosure and access.

Integrity - ensuring accuracy and completeness of information and information assets.

Availability - ensuring only authorized users will access to information and information systems whenever they need.

By protecting and securing the principles of information security, Nimbus Software:

- Will ensure compliance with criminal and civil law, statutory, legal or contractual obligations that have established safety requirements.
- Will educate all users of information system for security awareness of threats to business, how to protect information and also how to care for the information system and to uphold its objectives and principles in everyday work.
- Will implement appropriate checks for every new employment according to *Human Resources Manual*.
- Has inventory of all equipment and other assets and regularly update each change in order to prevent unauthorized dealing, theft, appropriation, misuse or removal of funds from Nimbus Software.

- Will analyze the risks associated with information system assets and measure the impact on the operations of Nimbus Software whenever necessary (introducing a new product, service, asset, etc.).
- Will establishes a system of classification, labeling, storage and use of information in order to prevent unauthorized access, theft, misuse, destruction or alteration of their contents.
- Will not allow entry or use of unverified or illegal equipment and software in computer information systems, unauthorized access to information and information assets, loss, damage or unauthorized modification of information, interruption of business processes, theft or misuse of the information and assets of processing information
- Will provide appropriate level of security of information and information resources in all parts of the organization by establishing security zones and limited physical access.
- Through regular monitoring and reporting of human errors, defects, damage, security incidents or unauthorized activities, Nimbus Software constantly learns and improves and thus decreases the effects of isolated and hidden threats to security of information and information assets.
- Will ensure continuity of critical business processes in case of unavailability of information systems in a reasonable and acceptable time frame, through the development, implementation and testing of Business continuity plans.
- By regular annual internal and external audits ensures compliance of the information system with security policy and international standards ISO / IEC 27001 and performs its constant improvement.

The above principles represent the direction and support to establish a system for managing information system security, in accordance with the requirements of standards.

In order to support the security policy, additional documents, policies, regulations, procedures and guidelines are created.

4. Enforcement

Any employee found violating this policy may be subject to disciplinary action, up to and including termination of employment.