



Razvojni center
IRC Celje, d.o.o.

Information Security Policy

The key goal of our organization is to offer the complete projects and technological solutions in the field of business informatics and information technology, in order to consistently fulfil the expectations and demands of our customers, and to justify their confidence in all respects. We achieve this goal with high quality, reliable and safe software products and solutions.

Information and information systems are essential components of our business, and considering the nature of our work a very important support to all processes of our clients too. Information, software and hardware are the objects of potential and real threats, criminal acts, sabotages, other defects and disasters. Considering that facts we defined basic elements and goals of our Information Security Policy, which is implemented on all levels of our organization, and respected by all employees. We, the employees of the Development Center IRC Celje:

- **Maintain** the security of all application software and information, correct and safe operation of all information processing devices within organization, and information appliances which could be accessed by third parties. We also maintain the integrity and availability of all information processing and communication services.
- **Protect** the confidentiality, authenticity and integrity of information, software, software services, and support infrastructure. We also protect critical business processes from the influences of the bigger failures and disasters.
- **Ensure** the proper level of protection of information and information devices, and the access. This policy applies to information security of all IT projects and support activities, portable computers and teleworking devices; it also applies to the responsibility for information processing performed by "third party" ("*outsourcing*").
- **Control** unauthorized access to computers and information in information systems, damage and disruptions in business areas, loss, damage and misuse of the equipment, interruption of business activities, violation or theft of information and information processing equipment, damage interruption of business activities, unauthorized modifications, and misuse of the information being exchanged between organizations, data losses, changes or misuses of the customer data in application systems.
- **Manage** the risks of human failures, thefts, cheating, or misuse of the equipment, damages of the security incidents and defects, and we learn from all these cases. **Detecting** unauthorised activities is a part of risk management process.
- **Avoid** violation and breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.
- **Educate** all information system users in order to raise their awareness concerning threats to information security, and to care about information security. Users are trained in order to support and implement organization information security policy during their daily work.

These information security principles support the implementations of the information security management systems (ISMS), which is compatible to the requirements of the international standard ISO/IEC 27001:2005. By performing internal ISMS audits and third party audits on temporary basis, we ensure its compliance to information security policy, and reference standard.

Dr. Ivan Vežočanik
- general manager -

Celje, May 17th, 2006