



Company policy according to CSN EN ISO 9001 and CSN ISO/IEC 27001

Our company has been operating in the field of server hosting services since 1996. Thanks to the success on the foreign hosting market and our role of a reliable international IP connectivity supplier, MasterDC has gradually specialized itself as a leading operator of data centres in the Czech Republic. Currently, our main goal is to assist companies in the analysis and technical implementation of server projects, corporate data security and their access. With the rising price of electricity, we also focus on the latest technologies to reduce consumption.

We are aware that we can achieve consistent high quality only with a policy that covers all activities of our company and its employees. Meeting our customers' needs is a permanent part of our daily work and a presentation of our company's quality principles.

The scope of the system in our company includes our company, all its internal and external aspects and interested parties. The scope of our company is worldwide. Our important customers are companies from various industries, especially providers of internet content, data processing and storage.

1. Quality

Quality is a top priority in our company. We guarantee it through qualification and an active approach of our employees. We realize that the quality processes in our company ultimately determine our future.

2. Respecting our customers

We provide our services and products in the required quality and set deadlines. We maintain close relationships with our customers and we are able to react to all their requests, needs and expectations promptly.

3. Economy and efficiency

We have been developing cooperation partnerships with our suppliers. We have taken measures that allow us to lower expenses and prevent all forms of inefficiency.

4. Colleagues

We respect all creative and professionally adept employees and co-workers who are willing to educate themselves further in their respective field. We strive to motivate them constantly to be productive, thereby creating conditions for continuous improvement of customer satisfaction. We support steady development of our key employees, both in their professional competence and in knowledge in management, communication and teamwork.





5. Information security

Implementing the information security system serves to secure the so called Business Continuity in our company, to minimize insurance claim risk by preventing security incidents and reducing their impact on the company, on our customers and interested third parties, to protect company information assets against internal, external, targeted or accidental security incidents and reduce the impact of their eventual emergence to a tolerable level, to protect information against unauthorized access, to ensure information confidentiality, consistent care for information integrity and availability in business processes, to adopt and apply measures resulting from legislation that applies to the operation of the company, to set up a Business Continuity plan and then ongoing maintenance and testing on the topicality of critical conditions, to provide regular training on information security for all employees and to report any present or anticipated security incidents to the person responsible followed by a careful analysis.

The company's management is committed to continuously improving the effectiveness of the quality management and information security system and to the responsibility for this effectiveness. It is aware of its risks, which it reduces thanks to planned measures, internal and external aspects, all in the context of the organisation. Integrity is ensured when planning and implementing changes in our company. Our company constantly meets the relevant requirements of laws and regulations, as well as customer requirements, which are determined and understood.

The annual goals of our company are based on the Policy. The company's management commits to meet all applied requirements relating to ISO 2007 and 9001. The quality and information security policy is reviewed once a year as a part of the Review.

The Integrated system policy is issued as a separate document in the company and all employees are familiar with it.

In Brno, 4th May 2021,

Ing. Filip Špaček, Ph.D., PVIS
