GRS IT Security Policy

Preamble

GRS - Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH - is a scientific and technical research and expert organisation. In rendering its services in research and development aimed at assessing and improving the safety of nuclear installations, it relies heavily on the provision and availability of information and communication (IT) technology.
Moreover, obligations to ensure IT security exist towards customers and project partners pursuant to legal provisions and contractual obligations.

1 Definition of IT security

IT Security is referred to as the protection of the IT Installations against misuse, manipulation and sabotage.

2 Significance of IT security

IT security has high entrepreneurial significance.

The General Management of GRS has therefore decided to introduce together with the IT Security Officer and the IT Service Provider of GRS an IT security procedure for the handling of IT installations.

For all employees and external users, the IT Security Policy shall be a call and an obligation to act in conformity with the law and to handle the IT infrastructure of GRS responsibly. The IT Security Policy of GRS is to be brought to the attention of all users of the IT installations of GRS in a suitable form, and each user is to be committed to compliance by written statement.

3 IT security objectives

GRS protects its interest and public image as well as its trustworthiness to customers and partners by ensuring its ability to operate with regard to its IT-based systems, programs, and data.

The guarantee of the general IT security requirements of availability, confidentiality and integrity is part of the corporate philosophy.

The IT security objectives of GRS are as follows:

- GRS shall ensure the availability of its data and IT installations and shall thereby support the continuity of its work processes:
  Provision of IT services at the required quality and time without impairment due to disturbances caused by security-related events. Data shall be protected against loss.
- GRS shall ensure confidentiality:
  Protection of project-related data and working results against unauthorised access. Data worthy of special protection (personal data, classified information) shall be specially protected.
- GRS shall protect the integrity of its IT installations:
  Protection of the data and installations against falsification and unauthorised modification.
- GRS shall protect its IT installations against manipulation and misuse (improper use, use by unauthorised persons).
- GRS shall protect its IT network against unauthorised access (attack, data manipulation) from outside.
- GRS and its employees shall abide to the relevant laws and other legal provisions regarding IT.
- GRS shall protect its employees' personal rights.

4 Responsibility

The General Management of GRS shall be responsible for the IT security of GRS. The General Management shall delegate the implementation of the IT Security Policy and the supervision of compliance to the IT Security Officer of GRS. The employees' compliance with the IT security measures shall be checked as part of the disciplinary process.

The IT Security Officer of GRS shall fulfil his function in close co-operation with the IT Service Provider of GRS.

5 IT security process

The IT security process is the subject of a specially dedicated IT security concept. This IT security process is guided by the Basic Protection Standard of the Federal Office for Information Security (BSI). The person responsible for the process shall be the IT Security Officer of GRS.

6 Strategy, implementation and measures

To guarantee IT security at GRS according to the IT safety objectives listed above, the following measures shall be implemented:

- Provision of the technical and human resources needed for IT security
- Guidance of the users of the IT installations in the use of the latter regarding safety-relevant aspects
- Co-ordination between project managers and the IT Security Officer regarding security aspects already at the stage of project initialisation
- Consideration of the IT security requirements in the co-operation with partners and external service providers
- Definition of sanctions in the event of any violations of IT security regulations
- Planning and supervision of the realisation of IT security measures in the technical, organisational, personnel and infrastructure areas by the IT Security Officer
- Introduction of an Information Protection Policy as accompanying measure of the IT security process
- Training of employees in IT security