Guideline

on information security

Information on the document	
Title	IS1-4 IA Guideline on information security
Document abbreviation / referencing:	IS1-4
Creation on:	16.10.2024
Last edited on:	16.10.2024
Page number:	6
Confidentiality level:	Public
Version number:	2
Processing status:	Freigegeben
Subject to release:	Yes
Released on:	14.08.2024
Released by: Management / ISB	Release by demonstrable release of a valid main version on the intranet page of the IS staff unit by the ISB and GF
Regulation enters into force on:	01.09.2024
Document owner:	ISB
Scope of application:	Entire IDEAL Automotive Group worldwide (IA)

Table of contents

The management hereby adopts the following guideline on information security as part of its strategy:

1. Importance of information processing

Information processing plays a key role in our business operations. All key strategic and operational functions and tasks are significantly supported by information and communication technology (ICT). It must be possible to compensate for a failure of ICT systems as a whole at short notice. Our business must not collapse, even in certain areas. As our core competence lies in the partnership-based development of innovative products in collaboration with customers and suppliers, protecting this information from unauthorised access and unauthorised modification is of vital importance.

2. Overarching goals

The availability of our data and our ICT systems in all technology-dependent and commercial areas is secured in such a way that the expected downtimes can be tolerated. Malfunctions and irregularities in data and ICT systems are only acceptable to a limited extent and only in exceptional cases (integrity). The requirements for confidentiality are at a normal, legally compliant level. Information that is categorised as confidential or secret due to internal classification or contractual requirements of our customers must be given special protection.

The standard security measures must be economically justifiable in relation to the value of the information and ICT systems worthy of protection. Cases of damage with a high financial impact must be prevented.

All employees of the company comply with the relevant laws (e.g. laws and regulations on data protection), internal procedures and work instructions and contractual provisions. Negative financial and immaterial consequences for the company and its employees due to violations of the law and breaches of contract must be avoided.

All employees and company management are aware of their responsibility when dealing with ICT systems and support the security strategy to the best of their ability.

2.1 Detailed objectives

Delayed or incorrect management decisions can have far-reaching consequences. It is therefore important for management to have access to up-to-date control data when making important decisions. A high level of security must be ensured for this information in terms of availability and integrity.

Data protection laws and the interests of our employees require us to ensure the confidentiality of employee data. Personal data of our employees is therefore subject to a high level of confidentiality protection. The same applies to the personal data of our business partners.

Enquiry and quotation data from and about our customers as well as design data from our customers and our development department are subject to very high confidentiality requirements. Their loss or theft can result in competitive disadvantages or claims for damages against us. Confidentiality is protected and manipulation is prevented by technical and organisational measures and a high level of employee awareness.

System availability and fault-free operation are ensured for the logistics areas and production plants. Downtimes are only acceptable to a very limited extent, as they can lead directly and indirectly to a reduction in revenue and have a negative impact on customer satisfaction.

The use of the Internet and portal applications to obtain information and for communication is a matter of course for us. E-mail serves as a substitute or supplement to other communication channels. Appropriate measures are taken to ensure that the risks of use are minimised.

3. Information security management

A security organisation has been set up to achieve the information security objectives. An Information Security Officer (ISB/CISO) has been appointed. The Information Security Officer reports directly to the Management Board.

The information security officer is provided with sufficient financial and time resources by the management in order to receive regular training and information and to achieve the information security targets set by the management.

The ICT security administrators and the information security officer must be supported in their work by the ICT users.

The information security officer must be involved in all projects at an early stage in order to take security-relevant aspects into account as early as the planning phase. If personal data is involved, the same applies to the data protection officer.

ICT users must comply with the instructions of the Information Security Officer in security-related matters.

4. Safety measures

A responsible person is appointed for all procedures, information, ICT applications and ICT systems, who determines the respective protection requirements in collaboration with the information security officer.

Deputies must be set up for all responsible functions. Instructions and sufficient documentation must be provided to ensure that the deputies are able to fulfil their tasks.

Buildings and premises are protected by adequate access controls. Access to ICT systems is protected by appropriate access controls and access to data is protected by a restrictive authorisation concept.

Computer virus protection programmes are used on all ICT systems. All Internet access is secured by suitable firewall systems. All protection programmes are configured and administered in such a way that they provide effective protection and prevent manipulation. Furthermore, ICT users support these security measures by working in a security-conscious manner and informing the relevant authorities in the event of anomalies.

All ICT systems, applications and all information must be handled using suitable technical and organisational measures in such a way that the protection objectives can be achieved at all times. The technical and organisational measures must be reviewed regularly and adapted if necessary.

Data loss can never be completely ruled out. Comprehensive data backup therefore ensures that ICT operations can be resumed at short notice if parts of the operational database are lost or obviously incorrect. Information is standardised, labelled and stored in such a way that it can be retrieved quickly.

In order to limit or prevent major damage as a result of emergencies, security incidents must be responded to swiftly and consistently. Emergency measures are compiled in a separate emergency preparedness concept. Our aim is to maintain critical business processes even in the event of a system failure and to restore the availability of the failed systems within a tolerable period of time.

If ICT services are outsourced to external organisations, we will specify concrete security requirements in the service level agreements. If suppliers need to be given access to data requiring a high level of protection in order to fulfil the contract, we place them under a separate and explicit obligation to maintain confidentiality. The right to control is defined.

ICT users take part in training courses on the correct use of ICT services and the associated security measures. The company management supports needs-based training and further education.

5. Improving security

The information security management system is regularly reviewed to ensure that it is up to date and effective. In addition, the measures are also regularly analysed to determine whether they are known to the employees concerned, whether they can be implemented and whether they can be integrated into operational procedures.

The management supports the continuous improvement of the security level. Employees are encouraged to pass on possible improvements or weaknesses to the relevant departments.

The desired level of security and data protection is ensured by continuously reviewing the regulations and ensuring compliance with them. Deviations are analysed with the aim of improving the security situation and keeping it up to date with the latest ICT security technology.

6. Consequences of non-compliance

Failure to comply with the provisions of this guideline can have serious consequences for the company. Depending on the severity and circumstances, violations may result in disciplinary or legal consequences.

7. Reference to IA Policy Statement

The IDEAL Automotive policy statement, which is regularly reviewed and amended as necessary, is superordinate to this guideline. All employees are obliged to inform themselves about the current content of the policy statement and to ensure that their actions are in line with the principles set out therein.

8. Procedure for changes

Changes to the information security guideline are implemented systematically and transparently. Every planned change is first reviewed and approved by the information security management team. The new or amended content is integrated into our training programme to ensure that the requirements are understood and implemented.

9. Scope of application

This policy applies to all employees, external partners and service providers of the company who have access to the company's information and systems. It covers all physical and digital information as well as the corresponding technical and organisational measures to protect this information.

Bamberg, 31.10.2024

- Management -

Stefan Frey

s.frey@ideal-automotive.com, Jan 08,2025 11:11:39 AM UTC

- Information security officer -

Martin Schnapp

m.schnapp@ideal-automotive.com, Oct 31,2024 09:14:18 AM UTC