Instytut Badań i Rozwoju Motoryzacji BOSMAL Sp. z o.o.
ul. Sarni Stok 93, 43-300 Bielsko-Biała

POLICY

Number: BOSMAL/A-12-03/03	Issue date: 14.01.2025	
Title: Information security and cybersecurity	Pages: 10	Attachments: -

Table of contents

DISTRIBUTION LIST:

ZJ	ZT											
DN	NC	NA	NE	NK	NR	NZ	NL	NI	NB	NH	NP	IOD
DB	BD	BH	BM	BS	BW	BP	BE	BR				
NSZZ „S"				ZZ PRAC.			-					

Only for use within BOSMAL

Papier copy: ZJ

Written by:	Checked by:	Approved by:
Joanna Faber, PhD Eng. (dr inż. Joanna Faber)	Arkadiusz Stojecki, PhD Eng. (dr inż. Arkadiusz Stojecki)	Piotr Świątek, PhD Eng. (dr inż. Piotr Świątek)
(Signature)	(Date, Signature)	(Date, Signature)

NOTE: This document is BOSMAL's translation. In the event of discrepancies, only the original document is binding. You can find it at www.bosmal.com.pl

1. AIM

To collect and present organisational and technical principles for the assurance, supervision and management of information security, including the protection of personal data at BOSMAL, in order to ensure the confidentiality, availability and integrity of processed information.

2. AREA OF APPLICATION

This policy defines the basic principles of information security management and applies to all organisational units within BOSMAL.

3. SCOPE OF APPLICABILITY

The policy applies to all organisational units and all BOSMAL employees.

4. DIVISION OF RESPONSIBILITIES

Described in point 6.2

5. DEFINITIONS AND ABBREVIATIONS

5.1. Definitions

Definition	Description
Information security	understood as: – maintaining confidentiality, integrity and availability of information, – restricted access to BOSMAL’s rooms, – restricted access to information (the principle of necessary knowledge) – appropriate behaviour in terms of information security and cybersecurity (cyber hygiene)
Cybersecurity	protection of IT systems against cyber threats
TISAX	Trusted Information Security Assessment Exchange, a standard concerning information security in the automotive industry
IT system	in line with BOSMAL/P-4-12, a set of computer devices, together with specialized software, that performs data and information processing. BOSMAL’s IT system may consist of smaller subsystems
User	in line with BOSMAL/P-4-12, every employee who has access to the BOSMAL information system using an active login and password
Confidentiality	only authorised persons with legitimate interests have access to information

Definition	Description
Integrity	inviolability, consistency and completeness. Ensuring that changes are not made in an unauthorised manner and that no destruction (of information, assets, etc.) occurs
Accountability	assigning an owner of an asset, resource, etc.
Accessibility	a property specifying that on request the information is available for use by a person authorised to access the information, within a specified period of time
Informational assets	in line with BOSMAL/P-1-06, all information resources (information) that is of value to BOSMAL
Supporting assets	in line with BOSMAL/P-1-06, assets for the processing of informational assets

5.2. Abbreviations

Term	Definition
BOSMAL, the Institute	BOSMAL Automotive Research and Development Institute Ltd (Instytut Badań i Rozwoju Motoryzacji BOSMAL spółka z ograniczoną odpowiedzialnością)
IS	Information Security
CS	Cybersecurity
ISMS	Information Security Management System
ITSA	IT System Administrator
DSA	Data Security Administrator
PDSA	Personal Data Security Inspector
VDA ISA	VDA Information Security Assessment, a TISAX evaluation/requirement matrix

The names of BOSMAL’s organisational units – in line with the current organisational regulation BOSMAL/R-0-03.

6. INFORMATION SECURITY MANAGEMENT SYSTEM

6.1. ISMS policy and BOSMAL Board Declaration

BOSMAL Automotive Research and Development Institute Ltd introduced an Information Security Management System (ISMS) to meet the requirements of interested parties and legal requirements regarding information security, cybersecurity and data protection. The Board of the Institute constantly undertakes activities aimed at protecting information, implementing and applying the principles of safe handling of information and assets, appropriate response to events and incidents, risk identification and ensuring the continuity of the Institute’s activities and appropriate knowledge and awareness of staff. To this end, the ISMS covers all BOSMAL organisational units and the information security requirements were integrated with other management systems implemented at BOSMAL.

The "Information security and Cybersecurity" policy is communicated within BOSMAL and is consistent with the strategic directions of the Institute's activities and integrated with business processes. The ISMS policy is also made available to interested parties via its publication on BOSMAL's website (www.bosmal.com.pl).

BOSMAL's management shows its commitment and declares its full support for the activities undertaken in the field of maintaining, developing and improving the ISMS and provides the necessary resources and resources to achieve the objectives, including the implementation and maintenance of the necessary organisational, physical, technical and personnel safeguards.

In order to ensure the effective functioning of the ISMS, specific rules of conduct are established, communicated to employees and periodic training and awareness-raising of employees are carried out to emphasize their role in information systems. Actions taken are planned, reviewed and improved. This "Information Security and Cybersecurity" Policy is reviewed periodically (at a minimum during Management Systems Reviews, but also in response to changes in terms of legal requirements or those relating to stakeholders). Where necessary, the Policy is updated, approved and published.

6.2. Roles, responsibilities and powers

In order to ensure the effective functioning of the ISMS, the Management Board of the Institute has appointed:

- its representative to supervise, develop and improve the ISMS, coordinate improvement activities and assess the effectiveness of these activities (Management Board Representative for. Management Systems),
- an individual responsible for ensuring information security and cybersecurity and for technical maintenance of the information system (Information Systems Administrator),
- a representative supervising the provision of data protection (Data Protection Officer).
- an information security and cybersecurity team.

The appointed persons report directly to the Management Board on the effectiveness of the ISMS and communicate the requirements and rules of conduct at the Institute.

The effectiveness of the implemented activities, proper conduct and protection of information and data are the responsibility of the managers of organisational units, who are the owners of information and assets in their subordinate areas.

All employees of the Institute are obliged to apply the established and described rules of conduct in the ISMS and to handle and protect information and assets appropriately.

All employees are obliged to maintain the confidentiality of the information obtained or produced, as certified by each employee's own signature on the document bearing the title "A commitment to confidentiality and impartiality".

Each employee is obliged to report events affecting the security of information or incidents to the immediate supervisor and in accordance with point. 7.9.

Newly admitted employees, apprentices, trainees are informed about the principles of information security and data protection as part of the initial instruction.

Internal auditors, trained in information security, are responsible for the effective assessment of the functioning of the ISMS and reporting irregularities and potential improvements to the ISMS.

6.3. Objectives of the ISMS

The implementation and maintenance of the ISMS aims to:

- ensure protection of information and personal data against unauthorised access, and, loss, leakage or unauthorized modification,
- ensure the confidentiality, availability and integrity of information (security attributes of information) and personal data processed at BOSMAL,
- protect against the negative effects of attacks, incidents and violations,
- ensure continuity of BOSMAL’s operations, in particular in the area of key informational assets,
- ensure that users have appropriate knowledge and awareness,
- describe and provide a uniform way of proceeding within the information system, including in the case of identified incidents and threats.

6.4. Range of the ISMS

The Information Security Management System at BOSMAL covers all BOSMAL organisational units and all job functions and positions. The implementation of the ISMS includes:

- requirements of ISO/IEC 27001 (current edition) and TISAX (current VDA ISA assessment sheet),
- legal requirements,
- stakeholder requirements and the context of the organisation (the current list is held by the Board Representative for Management Systems).

The protection of IS and CS are subject to the processing of assets and information (including personal data) generated by BOSMAL and also that provided by BOSMAL customers for the purposes of carrying out their work (products or services).

7. RULES OF CONDUCT

7.1. General principles

The rules of conduct, safeguards and solutions implemented ensure the preservation of the three basic attributes of information security: confidentiality, availability and integrity.

The following rules shall apply within the ISMS:

1. **The principle of authorised access:** each employee has access to resources only to the extent necessary and in accordance with the rights which have been formally granted.
2. **The principle of necessary powers:** each employee has the right to access only the information and resources that are necessary to perform the tasks entrusted to him or her.
3. **The principle of necessary knowledge:** each employee has knowledge of the system to which he or she has access, limited only to the issues that are necessary to perform the tasks entrusted to him or her,

4. **The principle of necessary need:** user access rights only to the means of processing information (assets) necessary to perform the user's official duties for BOSMAL and to limit user access to other means.
5. **The principle of collective awareness:** all employees are aware of the need to protect the information resources of BOSMAL and actively participate in this process.
6. **The principle of individual responsibility:** specific, named individuals are assigned the security of individual components of the ISMS.
7. **The principle of necessary presence:** only authorised persons have the right to be in certain places.
8. **The principle of constant readiness:** the information system and its components are constantly working. Critical elements of the information system are constantly updated to maintain information security and data protection.
9. **The principle of completeness:** effective security is possible only if a comprehensive approach is used, taking into account all degrees and all elements of the information processing process in general.
10. **The principle of appropriateness:** the mechanisms used must be appropriate for the situation.
11. **The clean desk principle:** protect documentation and data from bystanders. Do not leave documentation and data carriers in visible, unsupervised places.
12. **The clean screen principle:** when leaving a computer workstation, it should be blocked.
13. **The clean bin principle:** documents should be destroyed in dedicated shredders, rather than being thrown into the bin.
14. **The clean printer principle:** printouts from the printer should be received immediately after being printed.

The specific obligations of users are described in the "Information system management" procedure BOSMAL/P-4-12.

7.2. ISMS Documents

The ISMS at BOSMAL is described in this policy and the Quality Book of the Integrated Management System. Detailed information on how to proceed in specific areas is described in the relevant procedures and instructions (paragraph 8 of this policy).

7.3. Classification of information and assets

Information at BOSMAL is classified as: public, operational or confidential. The level of protection of information, assets supporting information, the owners of assets and information are thereby established.

The classification and handling of information and assets and the supervision of documents and records are described in the procedure BOSMAL/P-1-06 "Management of documented information"".

7.4. Classification of projects

TISAX projects implemented at BOSMAL are subject to normal or high protection, in accordance with TISAX ('normal protection needs' and 'high protection needs'). Details of how TISAX projects are handled are described in the “Tendering and conclusion of commercial contracts” procedure BOSMAL/P-6-07.

7.5. IT System

The IT system at BOSMAL is supervised to ensure information security and data protection, and the activities are unified throughout the Institute. Details of the procedure are included in the “Management of the information system” procedure BOSMAL/P-4-12, in which – among other things – the rules of conduct in the field of information system and access control in BOSMAL are described, including the password and authentication policy, the security of computer equipment, phones and data carriers, granting/receiving permissions, as well as applied security and network security, change management, supervision of software and backups, rules for the use of e-mail, vulnerabilities and changes and user obligations.

The handling of personal data is described in the “Security management of personal data processing” procedure BOSMAL/P-12-01.

7.6. Physical safety

The Institute has been divided into five access zones: green (general access), yellow (limited access), red (restricted access), blue (rooms for tenants), grey (rooms excluded from use). For each of the zones, graphic designations were introduced and a minimum security level was defined; access to the zones was limited in accordance with the principle of necessary presence. Details of the access rules and the technical safeguards applied to the facilities and supporting assets are described in the “Physical security” policy BOSMAL/A-12-02.

7.7. Human resources and staff awareness

BOSMAL has a human resources policy aimed at attracting the best qualified, experienced and skilled staff to achieve the objectives and tasks of the Institute. The rules applicable to the employment of employees, the necessary training and initial and on-the-job instructions are regulated in the “Personnel Management” procedure BOSMAL/P-2-02.

In order to continuously increase the awareness of staff in the field of IS and CS and their role in the maintenance and improvement of the ISMS, internal training and interviews with employees are conducted; information and training materials for self-education are also prepared.

7.8. Risks and probabilities

BOSMAL takes measures to identify information security risks. To this end, asset and hazard identification, risk (and risk consequence) and vulnerability analyses are carried out and risk mitigation measures are determined on the basis of the results of the risk analysis. The identified risks are periodically reviewed and updated.

The procedure is described in the “Risk management” instructions BOSMAL/I-1-07, including handling of risk in processes related to the execution of the order, risk in information security. In addition, the manual defines how to determine the context of the organisation and the stakeholders.

7.9. Occurrences, incidents and non-conformities

BOSMAL has established means and channels for reporting events and incidents related to information security, cybersecurity and personal data protection. Details of the approach are described in the “Incident Management” procedure BOSMAL/P-12-02. All BOSMAL employees are obliged to report the identified situation or suspected possibility of a dangerous/undesirable situation occurring in the area of information security (as broadly understood):

– information security notifications for information systems cybersecurity or access to resources should be addressed to BOSMAL's ITSA,

– notifications regarding personal data should be addressed to BOSMAL's DSA and/or DSI,

– notifications regarding physical access, infrastructure, media and malfunctions should be directed to the Head of the Maintenance Department,

– notifications regarding purchasing and IT service suppliers should be addressed to the Head of the Purchasing Department,

– notifications of management systems, including ISMS and IS non-conformities should be addressed to the Management Board Representative for Management Systems.

Submissions are subject to registration, analysis and, in justified cases, remedial actions, corrective actions or improvements (in line with BOSMAL/P-1-03). In the event of non-compliance in any area, a non-compliance card is issued and appropriate action is taken, as recorded on the non-compliance card; in cases requiring it, an internal audit is carried out in the area. Incidents and incompatibilities in the ISMS are reported to the Board of BOSMAL.

Conscious or intentional non-compliance with the established ISMS rules or violation of IS/data protection by personnel constitutes a disciplinary offense and is punishable for violation of the order and discipline at work, in accordance with the "Work regulations" BOSMAL/R-0-04.

Interested parties have the opportunity to report adverse situations or incidents through the contact details provided on the website (www.bosmal.com.pl).

7.10. Continuity of operations at BOSMAL

Ensuring the continuity of BOSMAL's operations and resilience to crises is crucial for achieving the Institute's business goals. The approach is described in the "Business continuity" procedurę BOSMAL/P-12-04 which describes the practices and assignment of responsibilities in the event of a crisis. In order to efficiently restore business activity after a crisis, business continuity plans are developed for critical areas; the timeliness of such plans and the adequacy of established procedures are checked during systematic tests.

7.11. Effectiveness of the ISMS and improvements to it

The effectiveness of the ISMS implemented in BOSMAL is assessed during internal audits and among the top management during reviews of management systems. Tasks and responsibilities aimed at improving the ISMS are determined on the basis of input data.

7.12. Supply chain and commercial relationships with suppliers

BOSMAL information technology service providers are subject to supervision, under which they are subjected to periodic assessments, risk analysis and – if necessary – audits. Information security requirements are communicated in the supply chain in the form of a Suppliers' Manual, which also includes a supplier self-assessment sheet in terms of the technical and organisational measures it uses to ensure information security. The methodology for ensuring the security of BOSMAL information provided to suppliers and requirements for suppliers are described in the "Production of IT services in IS" instructions BOSMAL/I-6-03 and in the "Supplier management" procedure BOSMAL/P-6-10.

NOTE: This document is BOSMAL's translation. In the event of discrepancies, only the original document is binding.
You can find it at www.bosmal.com.pl

8. RELATED DOCUMENTS

Term	Description
KJ ZSZ	Quality Book of Integrated Management System
BOSMAL/A-12-03	Physical security
BOSMAL/R-0-04	Labour regulations
BOSMAL/P-1-03	Improvement and corrective actions
BOSMAL/P-1-06	Management of documented information
BOSMAL/P-2-02	Personnel management
BOSMAL/P-4-12	IT system management
BOSMAL/P-6-07	Tendering and concluding commercial contracts
BOSMAL/P-6-10	Supplier management
BOSMAL/P-12-01	Security management of personal data processing
BOSMAL/P-12-02	Incident management
BOSMAL/P-12-04	Business continuity
BOSMAL/I-1-07	Risk management
BOSMAL/I-6-03	Implementation of IT services in BI
BOSMAL/I-6-03 Zał. 1	Suppliers' manual
PN-EN ISO/IEC 27001	Information security, cybersecurity and privacy protection. Information security management systems. Requirements
VDA ISA	VDA Information Security Assessment, a TISAX evaluation/requirement matrix

9. ATTACHMENTS

9.1. Forms

Document type	Document title	Storage period (in years)
-	-	-

9.2. Attachments

Document type	Document title	Storage period (in years)
-	-	-

VERSION HISTORY		
Date of issue	**Version**	**Description of changes**
10.05.2022	01	
06.09.2024	02	
14.01.2025	**03**	Prototype definition removed. Provisions in the document contents clarified. Changes in the content marked.

NOTE: This document is BOSMAL's translation. In the event of discrepancies, only the original document is binding.
You can find it at www.bosmal.com.pl