PKP POLSKIE LINIE KOLEJOWE S.A.

Information Security Management System in PKP Polskie Linie Kolejowe S.A.		*Date of implementation of the ISMS:* **2013-01-02**
Information Security Policy at PKP Polskie Linie Kolejowe S.A. for the Company's Business Partners	**SZBI-Ibi-1a**	*Implementation date:* **2014-12-01**
	Version number **12**	*Version effective date:* **2026-07-01**

Information Security Policy at PKP Polskie Linie Kolejowe S.A. for the Company's Business Partners SZBI-Ibi-1a

ISMS Maintenance Team	**Paweł Krzyżek**	***/-/* Paweł Krzyżek 26.06.2026**	**ISMS Representative**	***/-/* Dariusz Bielas 26.06.2026**
Prepared by	*Agreed by*	*Date and signature*	*Approved by*	*Date and signature*

Rights holder: PKP Polskie Linie Kolejowe S.A.

Publisher: PKP Polskie Linie Kolejowe S.A. Headquarters
Information Security and Defence Affairs Office
ul. Targowa 74, 03-734 Warsaw
phone 22 47 324 00
www.plk-sa.pl, e-mail: ioi@plk-sa.pl

This document constitutes the intellectual property of PKP Polskie Linie Kolejowe S.A.

This document is intended for internal use only and may be used solely for the purposes of the operations of PKP Polskie Linie Kolejowe S.A.

Any copying, sharing, publication, modification or use of the document, in whole or in part, by unauthorised persons is prohibited.

Table of Contents

§ 1. Legal basis 4

§ 2. Objective 5

§ 3. General Provisions 5

§ 4. Objective of Information Security Managementin the Company 6

§ 5. Information Subject to Protection within the Company 7

§ 6. Rules for Handling Information within the Company 7

§ 7. Physical and Personnel Security 8

§ 8. ICT Security 9

§ 9. Information Flow and Communication with Partners 13

§ 10. Security Rules for Remote Access to the Company’s Information System Resources 14

§ 11. Incident Response 16

§ 12. Information Security Audits 17

§ 13. Security in Agreements, Arrangements, and Cooperation (Including ‘Non-Contractual’ Cooperation) 17

§ 14. Liability for Compliance with Information Security Rules in Connection with the Performed Agreement, Arrangement, or ‘Non-Contractual’ Cooperation 18

§ 15. Vulnerability and Security Incident Management for Products with Digital Elements and Related Services 18

§ 16. Table of amendments 21

§ 1.
Legal basis

The "Information Security Policy at PKP Polskie Linie Kolejowe S.A. for the Company's Business Partners SZBI-Ibi-1a", also referred to as SZBI-Ibi-1a for short, is part of the documentation of the certified Information Security Management System at PKP Polskie Linie Kolejowe S.A. (ISMS) and complies with applicable law and international standards in the field of information security management, in particular with:

1) the Act of 5 August 2010 on Personal Data Protection (i.e.
2) the regulations on the protection of personal data, i.e. Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; OJ EU L 119 of 2016, pp. 1-88), hereinafter referred to as the GDPR, and national provisions introduced pursuant to the GDPR**;**
3) the Act on the Protection of Personal Data Processed in Connection with the Prevention and Combating of Crime, implementing the provisions of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ EU L 119 of 04/05/2016, p. 89) pursuant to Article 175 of the Act of 10 May 2018 on Personal Data Protection, hereinafter referred to as the PDPA, and national regulations introduced under the PDPA;
4) Regulation (EU) 2024/2847 of 23 October 2024 of the European Parliament and of the Council on horizontal requirements on cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828, hereinafter referred to as the CRA Regulation,
5) the Act of 16 April 1993 on Combating Unfair Competition;
6) the Act of 6 September 2001 on Access to Public Information;

7) the Act of 5 July 2018 on the National Cybersecurity System,

8) the Act of 25 June 2025 on the National Cybersecurity Certification System,

9) implementing regulations issued pursuant to the aforementioned Acts;

10) ISO/IEC 27001, hereinafter referred to as the Standard.

§ 2.

Objective

1. The objective of document SZBI-Ibi-1a is to:
   1) ensure information security, including the security of information processed in the ICT systems of PKP Polskie Linie Kolejowe S.A., hereinafter referred to as the Company, by familiarising all external entities carrying out any work for the Company or cooperating with it;
   2) familiarise the external entities referred to in point 1 with the Company's minimum requirements and rules regarding information security, as well as the Company's approach to information security matters.
2. The external entities referred to in paragraph 1, hereinafter referred to as the Partners, shall be understood as entities that:
   1) are seeking or are obliged to conclude an agreement or an arrangement with the Company;
   2) cooperate with the Company, including as part of 'non-contractual' cooperation.
3. The performance of agreements, arrangements, or cooperation with the Partners involves the Partner gaining access to information concerning the Company, owned by the Company, and protected within the Company.

§ 3.

General Provisions

1. SZBI-Ibi-1a is a document that:
   1) is intended for the Partners;
   2) is based on the internal document adopted by the Company's Management Board entitled 'Information Security Policy of PKP Polskie Linie Kolejowe S.A. SZBI-Ibi-1',

hereinafter referred to as SZBI-Ibi-1, which sets out the directions and principles for information security management within the Company;

3) is known to all employees of the Company, including in particular those employees who are involved in the process of preparing agreements or arrangements with the Partners, organising cooperation with them, and supervising their performance in compliance with information security requirements.

2. SZBI-Ibi-1a constitutes a regulation with which the Partners are required to familiarise themselves in a verifiable manner.

3. SZBI-Ibi-1a is intended for publication on the Company's website.

§ 4.

Objective of Information Security Managementin the Company

The objective of information security management in the Company is to:

1) minimise the risk of threats occurring and ensure the effective implementation of information safeguards in order to ensure the continuity of performance of the Company's statutory tasks;

2) ensure an appropriate level of confidentiality, integrity, availability, and accountability of information in business relations with third parties as well as internally within the Company, in order to create optimal conditions for performing the tasks referred to in point 1;

3) ensure an appropriate level of personal data security and give effect to the rights and freedoms of data subjects whose data are processed in the Company;

4) ensure an appropriate level of information security to maintain the continuity of performance of the Company's tasks as an essential service operator;

5) ensure the protection of the Company's interests, including maintaining its positive reputation as an organisation that prioritises information security, thereby contributing to the continuity and efficiency of the Company's operations.

§ 5.

Information Subject to Protection within the Company

An analysis has been carried out within the Company which determined that information constitutes an exceptionally important asset subject to protection. The processing of information within the Company is carried out within identified asset types and groups.

§ 6.

Rules for Handling Information within the Company

The handling of particular types of information in the course of cooperation between Partners and PKP Polskie Linie Kolejowe S.A. shall proceed in accordance with the following rules:

1) if the information is classified within the meaning of the provisions on the protection of classified information, it must be handled in accordance with the provisions on the protection of classified information governing the requirements of such cooperation;
2) if the information constitutes personal data within the meaning of the personal data protection regulations, it must be handled in accordance with those regulations and the terms of the agreement or arrangement, in particular with the requirements specified:
    a) by the Company, acting as the data controller, in respect of personal data filing systems, encompassing operations performed on personal data for which PKP Polskie Linie Kolejowe S.A. is the controller and the register of which is maintained in accordance with the GDPR,
    b) by the Commander-in-Chief of the Railway Security Guard (Straż Ochrony Kolei), acting as the data controller, in respect of personal data filing systems processed in the course of activities relating to crime prevention and combating, included in the register of categories of processing activities maintained in accordance with the Law Enforcement Data Protection Act (DODO),
    c) in a personal data processing agreement (data processing agreement) concluded on the basis of these provisions;
3) if the information constitutes the Company's business secret (a trade secret within the meaning of the provisions on combating unfair competition or a business secret within the meaning of the provisions on access to public information), it must be

handled (protected) in accordance with the provisions on combating unfair competition, the provisions on access to public information, and the terms of the agreement or arrangement, in particular the requirements specified by the Company in a non-disclosure agreement (NDA);

4) if the information constitutes Partners' information obtained by the Company in connection with the performance of agreements, arrangements, ongoing cooperation with Partners, etc., it must be handled in accordance with the concluded agreements and applicable provisions of law;

5) if the information constitutes the Company's internal information generated within the Company or for its benefit, not falling within the scope of information classified into the remaining groups, it must be handled in accordance with the concluded agreements and applicable provisions of law;

6) if the information constitutes publicly available (public) information, appropriate protection shall apply to it until the moment of its publication by the Company.

§ 7.
Physical and Personnel Security

1. Prior to commencing the processing of information belonging to the Company, Partners shall meet the following conditions:

   1) where it is necessary for Partners to process information constituting the Company’s business secret, sign a non-disclosure agreement (NDA) or incorporate the provisions arising from the non-disclosure agreement into the Principal Agreement, provided that a reservation is included therein stating that the confidentiality obligations shall remain in force after the termination or expiry of the Principal Agreement for the period specified in the Principal Agreement;

   2) where it is necessary for Partners to process personal data from filing systems for which PKP Polskie Linie Kolejowe S.A. is the Controller, sign a personal data processing agreement in accordance with the template in force at the Company;

   3) where it is necessary for Partners to process personal data from filing systems for which the Commander-in-Chief of the Railway Security Guard (Straż Ochrony Kolei) is the Controller, sign a personal data processing agreement in accordance with the template approved by the Commander-in-Chief of the Railway Security Guard.

2. Employees of Partners carrying out work for the Company pursuant to a concluded agreement or non-contractual arrangement may remain on its premises under the supervision of a Company employee or security personnel of the facility (premises).
3. Partners shall ensure that premises housing documents or electronic media containing protected information of the Company are secured appropriately to the threats identified by the Partners, with particular regard to the risk of unauthorised persons intercepting protected information and the risk of its modification or deletion.
4. Appropriate security mechanisms ensuring the confidentiality, integrity, availability, authenticity, and accountability of information processed therein shall apply to all Company ICT resources made available to Partners.
5. Prior to obtaining access to the Company's information system, the Partner shall meet the requirements set out in this document.
6. The Company has a number of documents in place that ensure the security of information obtained in the course of cooperation with Partners.
7. Familiarity with the documentation of the Information Security Management System of PKP Polskie Linie Kolejowe S.A. and compliance with the provisions contained therein are the responsibility of all employees of the Company.

§ 8.
ICT Security

1. The security of information processed in information systems or ICT networks aims to maintain the primary attributes of ICT security, in particular: confidentiality, integrity, authenticity, and availability, which translates into its protection against: unauthorised access, disclosure, accidental or unauthorised destruction and modification, as well as against unjustified denial or delay of its delivery.
2. Ensuring the maintenance of ICT security attributes specified by the Company's employees or set out in an agreement with the Company is also one of the fundamental obligations of the Partners at every stage of cooperation with the Company.
3. The Partners undertake to apply, with due diligence, appropriate and properly implemented technical and organisational safeguards aimed at protecting the Company's information against unauthorised access to such information resulting from events constituting threats and risks of breach of confidentiality, integrity, and availability

of the Company's information, including, without limitation, cyberattacks, data breaches (including leaks of information contained in electronic files), provided that such safeguards shall be adequate to each type of threat and risk.

4. Only computers and devices complying with minimum security requirements may be connected to the Company's information system, and in particular those that have:
   1) an operating system supported by the manufacturer and all available security updates installed;
   2) an antivirus system installed in the operating system, the signatures of which are up to date;
   3) a firewall running in the operating system that is properly configured;
   4) software installed on the computer originating from trusted sources;
   5) software installed in accordance with the provisions of the licence agreement;
   6) software that does not infringe copyright.
5. Partners using the Company's information systems are required to ensure that authorised employees of the Partner or representatives of the Partner maintain the confidentiality of login credentials and passwords for the Company's information systems received from the Company and used in identification and authentication processes.
6. The obligation to maintain the confidentiality of login credentials and passwords for the Company's information systems referred to in paragraph 5 above includes, in particular, a prohibition on disclosing them to third parties as well as writing them down or leaving them in a place where they could be discovered by unauthorised persons.
7. The Partners undertake to keep user accounts in the Company's information systems up to date and to inform the Company of the need to remove an existing user account or create a new user account in the Company's information system for the Partner's employees or representatives.
8. Partners should not make the protection of the information system made available by the Company dependent solely on a single security mechanism, even where the technology applied is considered highly advanced and reliable.

9. The Company’s electronic mail system is equipped with protection mechanisms against threats (viruses and spam), and suspicious messages are kept in quarantine.
10. Partners undertake to comply with the security rules in force at the Company when transmitting messages to the Company by electronic means.
11. When communicating with the Company’s employees, Partners’ employees are required to:
    1) check whether transmitted attachments do not contain malware;
    2) refrain from distributing information via email to the Company’s employees that may pose a threat to the information system (such as spam, chain letters, etc.);
    3) refrain from transmitting content prohibited by law and information contrary to accepted principles of morality, e.g. racial discrimination, etc.
12. Rules for the secure use of the Company’s guest ICT network by Partners’ employees shall be agreed on an individual basis, following prior notification of the need for such access to the Company.
13. Access to the Company’s information system is possible exclusively by providing a valid identifier (login/user ID) and password granted to the user during the access rights provisioning process.
14. The password policy for Partner users accessing the Company’s information system shall be subject to the following rules:
    1) the password shall consist of a minimum of 8 characters;
    2) the password must meet the complexity requirement of containing: an uppercase letter, a lowercase letter, and a number or special character (e.g. !@#);
    3) the password must be changed no less frequently than once every 30 days;
    4) subsequent passwords must be distinct (a history of at least the last 6 passwords is maintained);
    5) passwords must be stored in a manner that guarantees their confidentiality;
    6) disclosing passwords to other persons is prohibited.
15. It is prohibited to create passwords based on:
    1) personal characteristics and numbers (e.g. dates of birth, first names, etc.);

2) keyboard sequences (e.g. qwerty, 12qwaszx);

3) user identifiers (logins) of the system user.

16. It is prohibited to create passwords that are easy to guess, and anonymous login by the Partner's employees is prohibited.

17. Authentication shall occur solely upon entering a matching password and its associated identifier (login).

18. Upon first login, each user is required to change the temporary password to a permanent one known only to themselves.

19. In the case of systems that do not automatically enforce periodic password changes and do not verify password complexity, each user is obliged to change their password in accordance with the rules set out above.

20. The user bears full responsibility for creating the password and storing it securely.

21. Passwords must not be disclosed either intentionally or accidentally and should be known exclusively to the user.

22. Passwords should not be stored in a form accessible to unauthorised persons:

1) in files;

2) on pieces of paper in places accessible to third parties;

3) in scripts;

4) in other electronic and paper records that would be accessible to third parties.

23. Where the Partner suspects that passwords have been disclosed to an unauthorised person, the passwords must be changed immediately by the user, and this fact must be reported to the Company's contact employee designated in the agreement or arrangement.

24. The password shall be kept secret even after its expiry.

25. The password change shall be performed by an employee or authorised representative of the Partner (where a password has been forgotten, the Partner shall report this fact to the Company's contact employee designated in the agreement or arrangement, who will return a configured temporary password to the user, enforcing its change upon first login).

§ 9.
Information Flow and Communication with Partners

1. Communication and information flow with Partners shall take place via the communication channels specified in agreements and arrangements with Partners, as well as via other communication and information flow channels approved for use by the Company.
2. The circulation of information between the Company and Partners must be carried out in compliance with the principle of accountability.
3. The circulation of protected information referred to in paragraph 2, transmitted by electronic mail (email), with particular regard to information constituting the Company's business secret and personal data, is permitted exclusively subject to compliance with the following rules:
   1) information must be transmitted in files, exclusively as email attachments (transmitting personal data or information constituting the Company's business secret as unprotected text within the body of an email message is prohibited);
   2) prior to being sent by electronic mail (email), files containing protected information shall be secured by compressing them into an archive and encrypting them using a 'strong' password;
   3) the password to decompress the file shall be transmitted to the recipient(s) of the material via a means of communication other than email (e.g. by telephone, SMS);
   4) prior to sending the message, the following settings must be mandatorily enabled:
      a) sensitivity – 'Confidential',
      b) delivery receipt request option,
      c) read receipt request option;
   5) the subject of the sent email should be preceded by a clear label, e.g. 'Information attached' (in this way, the recipient of the dispatch will be informed that a file—compressed with a password—containing secured protected information has been attached).
4. In the event that Partners are unable to apply the solution referred to in paragraph 3, or the methods of communication specified in the details of cooperation with the Company,

the circulation of information is permitted using encryption mechanisms previously accepted by the Company.

5. Partners should make every effort to apply cryptographic controls also:
   1) on computer hard drives, in particular laptops on which protected information of the Company is processed;
   2) on USB flash drives and other data storage media used to store information;
   3) on backup media;
   4) on mobile devices (where they have the technical capability to process protected information of the Company);
   5) within VPN tunnels.

§ 10.

Security Rules for Remote Access to the Company’s Information System Resources

1. Remote access to the resources of the Company’s information systems is only possible if the conditions set out in this document are met.
2. Two types of remote access are available to Partners:
   1) Personal VPN access – access via the public Internet. The VPN provides encrypted access to specific systems and business services from the Company's IT area, as specified in the request, excluding transit to the Internet. Access is granted through two-factor authentication using RSA tokens.
   2) Access via an IPSec Site-to-Site Tunnel – an encrypted tunnel established between the Company and the registered office of an external company for the purpose of exchanging traffic between strictly defined systems or devices indicated in the request.
3. Remote access is granted for a period specified in the provisions of the agreement, as well as under the terms and conditions contained therein.
4. The Company’s contact employee designated in the agreement or arrangement shall request remote access for the Partner’s employees and representatives.

5. The scope of remote access may be restricted or expanded following an analysis of the needs specified in the provisions of the agreement or arrangement with the Partner, subject also to additional consent from the owner of the requested system.
6. Remote access may be revoked where no use of the VPN access has been recorded for a period exceeding three months.
7. Up to 10 VPN accounts may be requested per single agreement. Where higher demand is anticipated, the quantity must be agreed with the IT Bureau of the Company’s Headquarters prior to signing the agreement. A list of consultants designated to perform the agreement must be attached to the application.
8. The Partner shall be responsible for the security of the workstation with access to the Company’s network and for the legality of the software installed on such workstation.
9. An employee of the Partner may apply for remote access only under an agreement with one Partner.
10. As part of remote access to the resources of the Company’s information system, Partners are prohibited from:
    1) permanently deleting data;
    2) performing any operations on drives/disks that could lead to their damage or the loss of data contained thereon, including formatting them,

    unless the provisions of the agreement or arrangement with the Partner provide otherwise.
11. The Partner is prohibited from undertaking any actions aimed at penetrating the Company's ICT resources, unless such actions relate to the performance of an agreement for security tests, penetration tests, etc.
12. It is prohibited to share the granted remote access with third parties, in particular authentication credentials, as well as physical access to devices with an established remote connection.
13. The Partner undertakes to use only the agreed information resources, even if resources other than those required to fulfil the order are available.
14. The person responsible for the performance of the Agreement shall provide the Partner with all instructions and attachments required to set up an account.

15. It is prohibited to perform remote access from computers and ICT networks that are publicly accessible, e.g. internet cafés, stations, restaurants, municipal wireless networks, etc.
16. In the event of the detection or suspicion of a security incident or a breach of the remote access rules, remote access may be revoked following verification of the logs.

§ 11.
Incident Response

1. Any event breaching the Company's information security, including the protection of personal data entrusted for processing and/or the protection of disclosed information constituting a Business Secret of PKP Polskie Linie Kolejowe S.A., must be reported to the Company without undue delay each time from the moment an information security breach incident is identified, in accordance with the provisions set out in the agreement.
2. In the event of a Company information security incident related to the performance of the concluded agreement:
    1) permissions/authorisations granted to the Partner's employees or representatives shall be immediately suspended/revoked, and the person designated on the Partner's part in the concluded agreement or arrangement shall be notified of this fact;
    2) the Partner's employees or representatives shall gather evidence as part of the incident proceedings, which includes:
        a) a general description of the incident (how the incident occurred, e.g. whether the incident was intentional or accidental),
        b) photographs, screenshots, and system logs, along with other information enabling identification and provision of evidence of the incident,
        c) a description of the nature of the incident (including, where possible, the categories and approximate number of data subjects concerned, data records affected by the incident, and the information security attributes that were breached: confidentiality, integrity, availability),

d) statements from witnesses to the incident, documented in the form of minutes of the interview of Company employees as well as Partner employees or representatives involved in the breach.

3) The Partner shall designate a point of contact from whom more information regarding the Company's information security incident may be obtained.

3. In specific cases of information security incidents, the Company shall inform the competent law enforcement authorities and other authorised bodies of the situation.

4. As part of corrective and/or preventive actions taken, the Company's employees together with the Partner's employees shall eliminate the root cause and remedy the consequences of the information security incident that occurred, including introducing additional ICT, physical, or organisational safeguards in order to minimise any potential adverse effects of the incident.

§ 12.
Information Security Audits

1. The Partner undertakes to provide the Company with all information necessary to demonstrate compliance with the provisions of the mandatory non-disclosure agreement (NDA) and the obligations set out in the current regulations on the protection of personal data, in particular in:

   1) Article 28 of the GDPR;

   2) Article 34 of the DODO;

   and also enable the Company, the Commander-in-Chief of the Railway Security Guard, or auditors authorised by them to conduct audits, including inspections.

2. The Partner shall promptly inform the Company if, in its opinion, an instruction issued to it as part of the activities referred to in paragraph 1 would constitute a breach of applicable regulations, and in particular, regulations on the protection of personal data.

§ 13.
Security in Agreements, Arrangements, and Cooperation (Including 'Non-Contractual' Cooperation)

1. The Partner is required to familiarise itself with document SZBI-Ibi-1a in accordance with the provisions of § 3(2), subject to the provisions of paragraph 2 of this Section.

2. The requirement for the Partner to familiarise itself with the provisions of document SZBI-Ibi-1a shall also apply to all persons assigned by the Partner to perform the agreement, arrangement, or cooperation, to the extent concerning such persons that ensures compliance with the provisions of SZBI-Ibi-1a during the performance of the agreement, arrangement, or cooperation.
3. The requirement to familiarise oneself with the provisions of document SZBI-Ibi-1a shall be stipulated in the concluded agreement or arrangement referred to in § 2(2)(1).
4. The concluded agreement or arrangement shall specify in detail, as appropriate:
   1) requirements towards the Partner regarding the protection of the Company's information;
   2) consequences and the scope of liability for failure by the Partner to comply with requirements related to the protection of the Company's information.
5. In the case of 'non-contractual' cooperation, the Partner shall confirm to the Company in writing that it has familiarised itself with SZBI-Ibi-1a within the meaning defined in paragraph 2.

§ 14.
Liability for Compliance with Information Security Rules in Connection with the Performed Agreement, Arrangement, or 'Non-Contractual' Cooperation

The Partner shall be directly liable to the Company for ensuring compliance with the information security rules concerning the Company, owned by the Company, and protected within the Company, by persons performing the agreement, arrangement, or cooperation on behalf of the Partner.

§ 15.
Vulnerability and Security Incident Management for Products with Digital Elements and Related Services

1. A Partner supplying the Company with products with digital elements or providing services related to their delivery, maintenance, integration, or operation (e.g. ICT resources, telecommunications resources) is required to notify the Company without undue delay of:
   1) detected vulnerabilities concerning the delivered products or provided services;

2) security incidents that may affect the security of products with digital elements used by the Company;

3) actively exploited vulnerabilities;

4) available security updates, patches, workarounds, or other mitigating measures reducing risks to the security of products with digital elements or services used by the Company, in particular the risk of breach of confidentiality, integrity, or availability of the Company’s data.

2. The obligation referred to in paragraph 1 also includes the provision of information on:

1) identification of the vulnerability or security incident, in particular the name of the vulnerability, the CVE identifier (if assigned), the product or component affected by the notification, and the version of the product or software;

2) assessment of the risk level or severity/criticality of the vulnerability;

3) potential impact on the security of products with digital elements or services used by the Company and on the functioning of the Company;

4) potential impact on the security of the Company’s data;

5) recommended remedial and corrective actions;

6) available mitigating measures pending the deployment of security patches.

3. The obligations referred to in paragraphs 1 and 2 shall be performed independently of the manufacturer's reporting obligations to the competent authorities arising under European Union legislation on the cybersecurity of products with digital elements, in accordance with the provisions of the Cyber Resilience Act.

4. The Partner is required to transmit information on detected vulnerabilities and security incidents concurrently to:

1) the contract coordinator or coordinators designated on the Company's part (persons specified in the agreement with the Partner);

2) the Security Operations Center (SOC) at the email address: soc@plk-sa.pl.

5. The notification referred to in paragraph 4 should contain at least:

1) identification of the product, service, or component affected by the notification;

2) a description of the vulnerability or security incident;

3) an initial assessment of the impact on the security of products with digital elements or services used by the Company;
4) an initial assessment of the impact on the security of the Company's data;
5) information on possible remedies (e.g. security patches, configuration changes, or workarounds);
6) recommended risk mitigation actions;
7) planned remedial actions on the part of the manufacturer or supplier of the product.

6. The Partner is required to submit the notification:
   1) in the case of critical vulnerabilities or actively exploited vulnerabilities, as well as security incidents that may cause a breach of confidentiality, integrity, or availability of data, or of the functioning of products with digital elements or services used by the Company – no later than within 24 hours from the moment of their detection or from obtaining information on their occurrence;
   2) in the case of other vulnerabilities or security incidents that may affect the security of products with digital elements or services used by the Company – no later than within 72 hours from the moment of their detection or from obtaining information on their occurrence.
7. Where full information is not available at the time of reporting, the Partner is required to submit an early warning/initial notification within the deadlines specified in paragraph 6, and subsequently provide supplementary information without undue delay after obtaining it.
8. The Partner is obliged to cooperate with the Company in the following areas:
   1) analysing the impact of a vulnerability or security incident on the Company's operations, including providing technical information and recommended risk mitigation measures;
   2) verifying and testing security patches prior to their deployment;
   3) providing support for the implementation of security updates or other remedial measures relating to products with digital elements or services used by the Company.

9. In the event of a high-risk vulnerability, the Partner is required to provide appropriate technical support to enable the implementation of remedial measures within the timeframe agreed upon by the Parties.
10. The Partner is obliged to ensure the availability of security updates for the supplied products with digital elements for the agreed support period corresponding to the expected useful life of the product.
11. Information on the availability of security updates must be provided to the Company, along with instructions for their secure implementation and, where possible, information on the potential impact of the updates on the functioning of products or services used by the Company.
12. The Partner is obliged to ensure that the obligations set out in this paragraph are also fulfilled by subcontractors and manufacturers of components used in the products or services provided.

§ 16.

Table of amendments

No.	No.: paragraph/section/point/letter/indent	Revision number after Change / Date of change	Description of change
1	Document heading §1(2) § 6(1)(2)	2 /2015-03-02	Correction of an error in the document's implementation date Incorporation of the amendment to the Personal Data Protection Act Clarification of the concept of trade secret
2	Entire document Annexes:	3/2016-08-01	Amendments consisting in clarifying the provisions; Withdrawn (template of the declaration of familiarisation with document SZBI-Ibi-1a)
3	Entire document	4/2018-05-25	Incorporation of the amendment to the

No.	No.: paragraph/section/point/letter/indent	Revision number after Change / Date of change	Description of change
			personal data protection regulations
4	Entire document	5/2018-11-30	Clarification of the provisions
5	Entire document	6/2019-03-20	Incorporation of the entry into force of the provisions on the protection of personal data processed in connection with the prevention and combating of crime
6	Entire document	7/2019-06-14	Amendments concerning the entry into force of the regulations on the National Cybersecurity System
7	Entire document	8/2020-07-01	Amendments consisting in providing more detail in the provisions
8	§ 4 1.	9/2021-10-15	Amendment consisting of clarifying the objectives of information security management within the Company The legal basis has been supplemented
9	§ 5	10/2022-03-22	Amendment consisting in clarifying the nature of information within the Company
10	Entire document	11/2024-10-31	Amendments consisting in providing more detail in the provisions
11	Article 1 § 15	12/2026-07-01	The legal basis has been supplemented Rules have been introduced for vulnerability and security incident management for products with digital elements and related

No.	No.: paragraph/section/point/letter/indent	Revision number after Change / Date of change	Description of change
			services.