PRODUCT CYBERSECURITY STANDARD

PRODUCT CYBERSECURITY STANDARD

Version 1.0

PRODUCT CYBERSECURITY STANDARD

Version 1.0

INTRODUCTION

Objective, history, addressees, application notes

Without sufficiently secure products, there can be no sufficiently secure processes: Cyber attackers regularly take advantage of the lack of IT security of networked products to successfully compromise IT systems and computer networks. As a result, companies are confronted with security gaps in their IT over which they often have no knowledge or control. To address this shortcoming, the European Union has introduced regulations such as the Cyber Resilience Act (CRA) to ensure higher security standards for all products with digital elements in the future.

The new „Product Cybersecurity Standard" (PCS) supports the implementation of „security by design" in IT products, i.e. the consideration of cybersecurity from the beginning of development to its discontinuation from the market. To this end, it defines basic requirements for what distinguishes data-secure and privacy-compliant digital and networked products, taking into account the current digital threat situation. The set of requirements provides concrete assistance for manufacturers of connected products in their timely preparation for the implementation standards of the Cyber Resilience Act and beyond. They are based on the proven EICAR standards, which have stood for additional security in networked products for years.

The PCS enables companies and providers of networked services to create the basis for higher IT security for their products by means of an initially voluntary public commitment, which in some cases goes beyond regulatory requirements: additional hurdles are imposed in particular for the use of data and information by third parties. In this way, PCS is meeting the increased manufacturer responsibility in the field of IT security and the growing need for trust in networked products.

PRODUCT CYBERSECURITY STANDARD

Version 1.0

A. TO CLAIM ADHERENCE TO THIS PRODUCT CYBERSECURITY STANDARD, AN IT PRODUCT SHALL FULFIL THE FOLLOWING REQUIREMENTS:

1. The requirements in this standard apply to all parts of the product including the whole digital supply-chain and product lifecycle:

- Code developed by the vendor (which includes the developer/manufacturer of the IT product)
- Code developed by external parties and included in the product by the vendor, including open source
- Code run on the user's device
- Any form of hardware necessary for the proper operation of the IT product
- Backend systems operated by the vendor or any subcontractor or third party to the extent they store, or process data received from the user's device or are relevant for the functionality of the user's device including cloud computing.

The term "code" is to be understood broadly in this context and refers to all instructions that are created for a computer program or part thereof as part of software development and that describe, represent and influence its functionality in a specific programming language. This includes not only the program code itself, but also its management governance, identity and rights con-

2. The product must comply with the principles of security by design. This requires threat modelling to take place from the start of development to the end of the product life cycle. Only a vendor with in depth knowledge of the system architecture, will be able to identify product-related risks and take risk-mitigating measures.

3. The vendor shall have a sufficient understanding of all code in the product, both internally and externally developed, to be able to ensure compliance with this standard. The vendor shall have implemented a governance process for third party code, which is defined, documented and strictly followed.

4. The vendor shall have sufficient control over all parts of the product's code, both, internally and externally developed, to make sure that any discovered faults that conflict with this standard can be mitigated promptly. This requires a timely patch management and coordinated vulnerability disclosure (CVD) policies which are made public for access of cybersecurity researchers and cybersecurity authorities. The vendor shall be especially aware of third-party risks and should choose third parties responsibly according to pre-defined standards.

5. The vendor shall have IT emergency plans in place enabling him to react appropriately to IT emergency situations, document them, minimize damage and restore functionality as quickly as possible. In case of a vulnerability, a security gap, a data breach or any other malfunction, the vendor shall inform his clients and, if applicable, the competent authorities immediately. The vendor shall develop, promote and support appropriate countermeasures

6. The vendor shall publish a privacy declaration covering the product and its ecosystem. This declaration is written in a clear and comprehensive way and does not obfuscate relevant information. It contains at least the items mentioned in this standard and is kept up to date when new versions of the product are released.

7. The product is designed to fulfil solely its claimed objectives; the claimed objectives are fully described in the product documentation and privacy declaration.

8. The vendor does not support any scheme that requires the non-detection of malicious activities concerning the product and its ecosystem that could be harmful to the user, its IT systems and the protection of any kind of data.

9. The product does not contain any hidden functionality or any other intended functionality that is not anticipated by the publicly claimed objectives, including the product documentation and privacy declaration.

10. More specifically, the product does not contain any back door, and the vendor does not support any third-party access (TPA) scheme. Back door means any, published or non-published access to the application, its code and user data other than the access described with the claimed objectives, which are clearly publicly stated according to the values of this standard, as well as in the product documentation and privacy declaration.

11. The product uses cryptographic methods to protect data that is transferred to and from the device and processed at any location under the control of the vendor, including the device itself, subcontractors and third parties. The vendor uses cryptographic methods to ensure the integrity of any code, updates or data installed on the user's devices as part of the product. Any used cryptographic method is based on algorithms and protocols that are considered to be of sufficient strength according to the current state of the art of technology also with regard to future technology developments. Code providing cryptographic algorithms and protocols is either based on widely accepted crypto libraries or otherwise engineered to provide sufficient security and be of sufficient quality to ensure a high level of data confidentiality according to the current state of the art of technology.

12. Information identifying the device owner, the product license owner or any other natural person using the device must not be transferred to the vendor unless there is a compelling reason as an exceptional case (privacy by design). The privacy declaration shall clearly and publicly state if such data is transferred, to what extent and for what (legal) reason. Where possible, the user's consent must be obtained in advance after giving sufficient information.

13. Where data is processed by the vendor, any subcontractor or third party, appropriate identity and access control management and system security should ensure that only authorized persons have access to the data necessary for the functioning of the product.

14. User-owned content, like contacts, passwords, messages, pictures, documents and any other personal files, must not be transferred to the vendor, a subcontractor or any other third party without the user's explicit consent, which is not automatically preselected (privacy by default). The privacy declaration shall clearly state in advance if such data can be transferred, to what extent, for what reason, when the transferred data will be deleted, and which measures are taken to secure the transferred datasets adequately.

15. Technical information, like device configuration, the application files, usage of features in the product, installed updates and other similar data, may be processed by the vendor only if this data is absolutely essential for fulfilling the product's intended purpose and security and is not in conflict with any significant user interest or the declarations in this general standard. The privacy declaration shall clearly and publicly state in advance if such data is transferred, to what extent, for what reason, when the transferred data will be deleted and which measures are taken to secure the transferred datasets adequately.

16. The product must comply with all general legal requirements of the law of the country in which it is used. If stricter legal requirements for cybersecurity and data privacy apply in certain countries than is the case in the country of origin of the product, the product must demonstrably comply with these stricter legal requirements.

17. If any type of product related data is transferred to a foreign country with a different definition of (digital) legal protection than the country of origin of the data, including the possible access by security authorities and/or intelligence agencies including lawful interception of user data, the user will be explicitly informed of this and of the associated risks before using the product. This can be done, for example, in the product documentation or the privacy declaration. Users must be aware of the potential risks of international data storage in advance so that they can make an informed decision. Wherever possible, the vendor must provide adequate technical and organizational protective measures to compensate for these risks and to inform the user as fast as possible of any kind of data access according to this provision.

B. THE VENDOR OF THE PRODUCT AGREES TO BE SUBJECT TO AN INDEPENDENT EVALUATION AND VERIFICATION OF THE ABOVE IDENTIFIED REQUIREMENTS. ALL THE AFORE MENTIONED MEASURES MUST BE DOCUMENTED ACCORDINGLY BY THE VENDOR SO THAT THEY CAN BE EASILY PRESENTED IN THE COURSE OF SUCH A VERIFICATION.

IMPRINT:

Product Cybersecurity Standard
Version 1.0 I January 2025

cyberintelligence.institute
Contact: Prof. Dr. Dennis-Kenji Kipker, Research Director
E-Mail: info@cyberintelligence.institute
Phone: +49 69 505034 602

Eicar e.V. - European Institute for Computer Anti-Virus Research
Contact: Rainer Fahrs, Chairmann
E-Mail: office@eicar.org
Phone: +49 8194 9985 01

ABOUT US:

CII: New times need a new form of research: the cyberintelligence.institute (CII) – a place where innovation, technology, strategy and resilience meet. At the interface of business and science, NGO and start-up, the CII in Frankfurt am Main develops new solutions for a secure digital future. The core idea is co-operation, dialogue and the interdisciplinary and global exchange of information and knowledge in order to make the state, economy and society more resilient. What is needed here are holistic concepts that understand cybersecurity not only as an abstract technical and organizational responsibility to ensure security, but as a task for society as a whole to protect common European values. In this way, the cyberintelligence.institute actively advocates for more digital security in an age of new digital challenges. Further information is available on the CII website at www.cyberintelligence.institute.

EICAR: EICAR was founded in 1991 as a registered association in Germany. Initially with the aim of bundling know-how in the field of antivirus research, EICAR is now considered a recognized IT security expert network. The institute sees itself as a platform for the exchange of information for all security experts who work in the areas of research and development, implementation and management. This is intended to promote global cooperation in the field of computer security. The aim of the institute is to develop solutions and preventive measures against all types of computer crime, such as the writing and dissemination of computer viruses, fraud and the spying on personal data. In doing so, the institute works very closely with companies, political organizations or university institutions as well as with the media, technology and legal experts. www.eicar.org