NASK

PC1 – Program oceny i certyfikacji bezpieczeństwa IT

PC1 – IT Security Evaluation and Certification Scheme

NASK-PIB Dokument Nr/Document No.: PC1/2.4

Egzemplarz dla Klienta (wyciąg z egzemplarza nadzorowanego)

Wersja/Version:	2.4
Data utworzenia/Creation date:	30.09.2019
Data aktualizacji/Updating date:	21.07.2022
Oznaczenie klasyfikacji/Classification:	Ogólnodostępne „O” / Public

Spis treści

Table of Contents

1. Odniesienia

CSA Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA i certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylające rozporządzenie (UE) nr 526/2013 (Cybersecurity Act).

PN-EN ISO/IEC 17065:2013-03 Ocena zgodności – Wymagania dla Jednostek Certyfikujących wyroby, procesy i usługi.

PN-EN ISO/IEC 17025:2018-02 Ogólne wymagania dotyczące kompetencji Laboratoriów badawczych i wzorcujących.

CC (Wspólne kryteria do oceny zabezpieczeń informatycznych), April 2017, Version 3.1, Revision 5.

CEM (Wspólna metodyka oceny zabezpieczeń teleinformatycznych), April 2017, Version 3.1, Revision 5.

PN-EN ISO/IEC 15408:2020-09 Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń;

PN-EN ISO/IEC 18045:2020-09 Technika informatyczna - Techniki bezpieczeństwa - Metodyka oceny zabezpieczeń informatycznych.

PN-EN ISO/IEC 19790:2020-09 Technika informatyczna - Techniki bezpieczeństwa - Wymagania bezpieczeństwa dla modułów kryptograficznych.

PN-EN ISO/IEC 27001:2017-06 Technika informatyczna – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

PN-EN ISO/IEC 27002:2017-06 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji.

ISO/IEC 27005:2018 (Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji).

PN-EN ISO 31000:2018-08 Zarządzanie ryzykiem - Zasady i wytyczne.

PN-EN ISO 19011:2018-08 Wytyczne dotyczące auditowania systemów zarządzania

1. References

CSA Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

ISO/IEC 17065:2012 Conformity assessment - Requirements for bodies certifying products, processes and services

ISO/IEC 17025:2017 General requirements for competence of calibration and testing laboratories

CC Common Criteria for Information Technology Security Evaluation April 2017, Version 3.1, Revision 5

CEM Common Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5

ISO/IEC 15408:2014-01 Information technology - Security techniques - Evaluation criteria for IT security;

ISO/IEC 18045:2008 Information technology — Security techniques — Methodology for IT security evaluation

ISO/IEC 19790:2012 Information Technology - Security Techniques - Security requirements for cryptographic modules

ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements

ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls

ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management

ISO 31000 :2018 Risk management - Guidelines

ISO 19011:2018 Guidelines for auditing management systems

SOG-IS MRA Porozumienie grupy SOG-IS o wzajemnym uznawaniu certyfikatów wydanych w oparciu o normę Common Criteria w zakresie bezpieczeństwa technologii informatycznych.	SOG-IS MRA Mutual Recognition Agreement of Information Technology Security Evaluation Certificates
CCRA Porozumienie o wzajemnym uznawaniu certyfikatów wydanych w oparciu o normę Common Criteria w zakresie bezpieczeństwa technologii informatycznych.	CCRA Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security

2.	Dokumenty Jednostki Certyfikującej*	2.	Certification Body documentation**
PC1	Program oceny i certyfikacji bezpieczeństwa IT	PC1	IT Security Evaluation and Certification Scheme
PC*nn*	Programy certyfikacji	PC*nn*	Certification Schemes
PT*nn*	Polityki NASK-PIB mające zastosowanie w działalności Jednostki Certyfikującej	PT*nn*	NASK-PIB's policies applicable to the activities of the Certification Body
P*nn*	Procedury NASK-PIB mające zastosowanie w działalności Jednostki Certyfikującej	P*nn*	NASK-PIB's operational procedures applicable to the activities of the Certification Body
Z*nn*	Zasady NASK-PIB mające zastosowanie w działalności Jednostki Certyfikującej (w tym podręczniki)	Z*nn*	NASK-PIB's rules applicable to the activities of the Certification Body (including manuals).
I*nn*	Instrukcje NASK-PIB mające zastosowanie w działalności Jednostki Certyfikującej	I*nn*	NASK-PIB's instructions applicable to the activities of the Certification Body.

* Spis obowiązujących programów certyfikacji, polityk, procedur, zasad/podręczników i instrukcji jest prowadzony w stosownych repozytoriach (rejestrach).

** List of applicable certification schemes, policies, procedures, rules/manuals and instructions is managed in appropriate repositories (registers).

3. Skróty

1 Oprócz zdefiniowanych poniżej skrótów wszystkie terminy używane w dokumentach wymienionych w pkt. 1. mają również zastosowanie do niniejszego programu.

3. Abbreviations

1 In addition to the abbreviations defined below, all the terminology used in the referenced documents listed in section 1 also apply to this scheme.

Skrót	Definicja
IT/ICT	Technologie informacyjne i komunikacyjne
ITSEF	Information Technology Security Evaluation Facility (skrót używany w SOG-IS i CCRA)

Tab. 1 – Skróty

Abbreviation	Definition
IT/ICT	Information and Communications Technology
ITSEF	Information Technology Security Evaluation Facility (as recognized in SOG-IS and CCRA)

Table 2 - Abbreviations

4. Słownik pojęć

2 W ramach niniejszego Programu oceny i certyfikacji bezpieczeństwa IT (dalej Programu Certyfikacji) następujące pojęcia będą rozumiane w sposób określony poniżej:

3 **Akredytacja** – atestacja przez stronę trzecią, dotycząca jednostki oceniającej zgodność, służąca formalnemu wykazaniu jej kompetencji do wykonywania określonych zadań w zakresie oceny zgodności.

4 **Laboratorium autoryzowane** – ocenione przez **Jednostkę Certyfikującą** jako posiadające potencjał techniczny w określonej dziedzinie IT i w obszarze badań bezpieczeństwa IT oraz formalnie upoważnione do wykonywania ewaluacji w Programie oceny i certyfikacji bezpieczeństwa IT jako podwykonawca działań związanych z oceną.

5 **Licencjonowane** – autoryzowane przez Jednostkę Certyfikującą na czas nieokreślony zgodnie z wymaganiami i procedurą licencjonowania.

6 **Aprobowane** – autoryzowane przez Jednostkę Certyfikującą do jednorazowego wykonania ewaluacji.

7 **Certyfikacja** – proces realizowany przez **Jednostkę Certyfikującą**, prowadzący do wydania certyfikatu.

8 **Specyfikacja Zabezpieczeń** – wymagania i specyfikacja właściwości cyberbezpieczeństwa produktu lub systemu IT.

9 **Ewaluacja (cyberbezpieczeństwa)** – ocena produktu IT lub profilu zabezpieczeń w odniesieniu do kryteriów oceny bezpieczeństwa IT z wykorzystaniem metod oceny bezpieczeństwa IT w celu określenia, czy złożone oświadczenia (o spełnieniu określonych wymagań) są uzasadnione.

Uwaga 1: Terminy równoważne: „ocena bezpieczeństwa IT".

4. Definitions

2 Within the framework of this IT Security Evaluation and Certification Scheme (hereinafter Certification Scheme) the following concepts will be understood as defined here:

3 **Accreditation -** third-party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks.

4 **Authorized laboratory** - assessed by a **Certification Body** as having technical potential in the specific IT field and in the area of IT security evaluation and formally authorized to carry out cybersecurity evaluations within the context of the IT Evaluation and Certification Scheme as a subcontractor for evaluation activities.

5 **Licensed -** authorized by the Certification Body for an indefinite period of time in accordance with the licensing requirements and procedure.

6 **Approved -** authorized by the Certification Body to perform one-time cybersecurity evaluation.

7 **Certification -** the process carried out by a **Certification Body** leading to the issuing of a certificate.

8 **Security Target -** requirements and specification of the cybersecurity properties of an IT product or system.

9 **Cybersecurity Evaluation** - the assessment of an IT product or a protection profile against the IT security evaluation criteria and with the use of IT security evaluation methods to determine whether or not the claims (on completion of specified requirements) are justified.

Note 1: Equivalent terms: 'IT security evaluation'.

Uwaga 2: Obejmuje wykonywanie przez laboratorium takich działań związanych z oceną jak badania, inspekcje i inne działania związane z określeniem oraz przedstawianie stwierdzeń zgodności, opinii lub interpretacji.

Note 2: It covers the performance by a laboratory of such evaluation activities as tests, inspections, and other determination activities and the reporting of statements of conformity, opinions or interpretations.

10 **Przedmiot Oceny** – produkt IT, system informatyczny lub profil zabezpieczeń, o którego certyfikację Klient zabiega oraz dokumentacja z nim związana.

10 **Product to Evaluate** – IT product, information system or protection profile for which a certification of its cybersecurity properties is solicited and related documentation.

Uwaga: Terminy równoważne: „produkt", „wyrób".

Note: Equivalent terms: 'product'.

11 **Laboratorium** – akredytowany podmiot wykonujący ewaluacje, licencjonowany lub zaaprobowany do przeprowadzania ewaluacji cyberbezpieczeństwa w Programie oceny i certyfikacji bezpieczeństwa IT.

11 **Laboratory** – an accredited evaluation facility, licensed or approved to perform cybersecurity evaluation within the context of the IT Security Evaluation and Certification Scheme.

Uwaga: Terminy równoważne: „ITSEF".

Note: Equivalent terms: 'ITSEF'.

12 **System teleinformatyczny** – zestaw elementów sprzętu (hardware), programów (software), danych i użytkowników, które w połączeniu zapewniają możliwość przechowywania, transmisji, przetwarzania i odtwarzania informacji.

12 **IT System** - set of elements of "hardware", "software", data and users, which when interconnected allow the storage, transmission, transformation and recovery of the information.

5. Definicja Programu Certyfikacji, role i funkcje

13 Niniejszy dokument określa zasady Programu Certyfikacji ustanowione przez **Jednostkę Certyfikującą** w celu utrzymania wysokich standardów w zakresie kompetencji i bezstronności oraz osiągnięcia spójności działań i wyników.

14 Niniejszy dokument określa wymagania, zasady i procedury, które składają się na program certyfikacji w odniesieniu do normy PN-EN ISO/IEC 17065.

15 Niniejszy program jest zgodny z założeniami przedstawionymi w „Akcie o Cyberbezpieczeństwie" (*ang. Cybersecurity Act*) poprzez zdefiniowanie kompleksowego zestawu zasad, wymagań technicznych, standardów i procedur dotyczących certyfikacji lub oceny zgodności produktów IT.

16 Program Certyfikacji jest zarządzany przez NASK i jest jego własnością.

17 Proces certyfikacji ma zapewnić, że została potwierdzona przez niezależną stronę trzecią zgodność produktu IT z określonymi wymaganiami.

18 W Programie Certyfikacji zdefiniowane są następujące role:

a) **Jednostka Certyfikująca**, która autoryzuje **Laboratoria** i certyfikuje produkty IT;

b) **Laboratoria**, prowadzące ewaluacje i testy produktu IT oraz tworzące raport będący podstawą do wydania decyzji w sprawie certyfikacji (decyzja certyfikacyjna) przez **Jednostkę Certyfikującą**;

c) **Klienci**, którzy wnioskują do **Jednostki Certyfikującej** o certyfikację produktu IT i przedkładają produkt do ewaluacji do autoryzowanego **Laboratorium** oraz ponoszą koszty z nimi związane. Klient to osoba lub organizacja, która zapewnia, że wymagania

5. Certification Scheme definition, roles and functions

13 This document specifies rules of the Certification Scheme established by the **Certification Body** in order to maintain high standards of competence and impartiality and to achieve consistency of activities and results.

14 This document specifies the requirements, rules and procedures that define the certification scheme in reference to ISO/IEC 17065.

15 This scheme complies with the concept laid out by the "Cybersecurity Act" as it includes a comprehensive set of rules, technical requirements, standards and procedures that apply to the certification or conformity assessment of IT products.

16 The Certification Scheme is owned and managed by NASK.

17 The certification process is designed to ensure that the IT product has been validated for compliance with specified requirements by an independent third party.

18 The Certification Scheme distinguishes the following roles:

a) A **Certification Body**, that authorize **Laboratories** and certifies the IT products;

b) **Laboratories** that perform the cybersecurity evaluation and testing of an IT product, and who produce a report that is to be used to form the decision relating to certification (certification decision) by the **Certification Body**;

c) **Clients**, who request the certification of the cybersecurity of IT product to the **Certification Body** and submit the product to an authorized **Laboratory** for the cybersecurity evaluation and cover the associated costs. A Client is a person or an organization that ensures

certyfikacyjne są spełnione.

that certification requirements are fulfilled.

Uwaga: Termin równoważny: „sponsor”.

Note: Equivalent term: ‘sponsor’.

19 Program Certyfikacji jest zdefiniowany w uniwersalny sposób względem dokumentów normatywnych dotyczących cyberbezpieczeństwa, co pozwala na jego rozwój poprzez potencjalne rozszerzanie go o nowe standardy lub w przypadku pojawienia się nowych kryteriów oceny.

19 The Certification Scheme is designed to be agnostic in terms of the cybersecurity evaluation standard that is to apply, so the proper scheme may evolve with the evolution of such standards, or the appearance of new evaluation criteria.

20 Stworzony mechanizm jest na tyle elastyczny, że pozwala na inkorporację nowych lub wycofanie istniejących norm (standardów) z technicznego zakresu Programu Certyfikacji.

20 The mechanism established is flexible to allow for the incorporation of new or withdrawal of existing standards from the technical scope of the Certification Scheme.

6. Prawa i obowiązki uczestników Programu Certyfikacji

21 Program Certyfikacji oferuje certyfikację bezpieczeństwa produktów IT. Usługi te są dostępne dla wszystkich podmiotów w sposób niedyskryminujący kogokolwiek, zgodnie z normą PN-EN ISO/IEC 17065.

22 Produkty będą akceptowane do certyfikacji pod warunkiem, że zakres wnioskowanej certyfikacji jest zgodny z możliwościami Programu Certyfikacji i charakterem produktu IT oraz z zatwierdzonymi wymaganiami certyfikacyjnymi.

23 Program Certyfikacji jest otwarty dla podmiotów, które chciałyby do niego przystąpić w roli **Laboratorium**.

24 Warunkiem wykonywania ewaluacji cyberbezpieczeństwa w Programie Certyfikacji jest spełnieniem wymagań zdefiniowanych w niniejszym programie, potwierdzone przez autoryzację.

25 Program Certyfikacji obejmuje ogólne wymagania i opis procesów dotyczących autoryzacji **Laboratoriów**. Szczegóły licencjonowania lub aprobaty laboratoriów, w tym wymagania techniczne i organizacyjne oraz procedury certyfikacji są opisane w odpowiednich procedurach operacyjnych (P34, P33).

26 NASK-PIB zobowiązuje się do zachowania poufności wszystkich informacji uzyskanych od klientów w procesie certyfikacji. Usługi na każdym etapie są świadczone w sposób bezstronny, obiektywny i etyczny. Personel własny oraz podwykonawcy zostali zobowiązani do zachowania zasad poufności w zakresie wszystkich informacji uzyskanych w procesie certyfikacji i nadzoru.

27 NASK-PIB zapewnia, że działania certyfikujące realizowane są w sposób bezstronny i posiada zasoby niezbędne do działania w zakresie certyfikacji.

6. Rights and obligations of the Certification Scheme actors

21 The Certification Scheme provides IT product security certification. These services are to be provided in an open, non-discriminatory manner, as mandated by ISO/IEC 17065.

22 IT products will be accepted for certification as long as the requested certification scope is consistent with the Certification Scheme capabilities and the IT product nature, and with the approved certification criteria.

23 The Certification Scheme is open to entities that would like to participate as a **Laboratory**.

24 In order to perform cybersecurity evaluation in the Certification Scheme, it is required to meet the requirements defined in this scheme, confirmed by an authorization.

25 The Certification Scheme includes the general requirements and description of the processes for the authorization of **Laboratories**. Details of laboratory licensing or approval, including technical and organizational requirements and certification procedures, are described in the appropriate operating procedures (P34, P33).

26 NASK-PIB commits to keeping confidential all information obtained from clients during the certification process. Services at each stage are provided in an impartial, objective and ethical manner. Our own staff and subcontractors have been obliged to maintain confidentiality of all information obtained during the certification and monitoring process.

27 NASK-PIB shall ensure that certification activities are conducted in an unbiased manner and has the resources necessary to operate within the scope of certification.

28 Certyfikacja produktów jest dobrowolna. Usługi te są otwarte dla wszystkich podmiotów w sposób niedyskryminujący kogokolwiek.

28 Product certification is voluntary. These services are open to all entities in a non-discriminatory manner.

29 Wszelkie prawa własności intelektualnej zawarte w dokumentach certyfikacyjnych pozostają własnością Jednostki Certyfikującej. Klient ma prawo do korzystania z dokumentów certyfikacyjnych bez żadnych ograniczeń, pod warunkiem, że będą one wykorzystywane w całości, bez żadnych skrótów lub modyfikacji.

29 All intellectual property rights contained in certification documents shall remain the property of the Certification Body. The Client has the right to use certification documents without any restrictions, provided that they are used in their whole, without any abridgements or modifications.

30 **Uwaga:** Do dokumentów certyfikacyjnych należą np. raport certyfikacyjny, certyfikat.

30 **Note:** Certification documents include e.g., certification report, certificate.

7. Wymagania w zakresie autoryzacji Laboratoriów

7.1. Wymagania ogólne

31 **Jednostka Certyfikująca** wymaga, aby **Autoryzowane Laboratoria** spełniały następujące wymagania:

a) Posiadanie kompetencji do wykonywania ewaluacji cyberbezpieczeństwa produktów IT. Wymaganie to będzie uznane za spełnione, jeśli podmiot przedłoży akredytację według normy PN-EN-ISO/IEC 17025, której zakres będzie obejmował kryteria oceny, metody oraz normy i specyfikacje techniczne właściwe dla Przedmiotu Oceny.

b) Spełnienie wymagań dotyczących zarządzania bezpieczeństwem informacji określonych przez **Jednostkę Certyfikującą**;

c) Zdolność prowadzenia ewaluacji zgodnie z procedurami zdefiniowanymi przez **Jednostką Certyfikującą**.

32 W każdym przypadku zakres autoryzacji udzielonej przez **Jednostkę Certyfikującą** musi być ograniczony do zakresu akredytacji **Laboratorium**.

7.2. Wymagania dotyczące zarządzania bezpieczeństwem

33 **Laboratorium** powinno posiadać system zarządzania bezpieczeństwem informacji zgodny z normą PN-EN ISO/IEC 27001 do celów tworzenia, zabezpieczenia i zarządzania informacją w procesie ewaluacji.

34 System zarządzania bezpieczeństwem informacji **Laboratorium** powinien obejmować:

a) System zarządzania ryzykiem jako podstawę struktury systemu zarządzania bezpieczeństwem informacji;

b) Procedurę szacowania ryzyka zgodną z powszechnie znaną i powszechnie

7. Requirements for the authorization of Laboratories

7.1 General requirements

31 The **Certification Body** requires the following requirements to be fulfilled by the **Authorized Laboratories**:

a) Competence to perform cybersecurity evaluations of IT products. This requirement shall be considered fulfilled when the entity provides accreditation to ISO/IEC 17025, the scope of which shall include the assessment criteria, methods and technical standards and specifications referred to Product to Evaluate;

b) Fulfilment of the requirements of security information management established by the **Certification Body**;

c) Capability to perform the cybersecurity evaluation according to procedures defined by the **Certification Body**.

32 In any case, the scope of the authorization granted by the **Certification Body** shall be limited by the scope of accreditation of the **Laboratory**.

7.2 Security management requirements

33 **Laboratories** shall define and operate an information security management system conformant with ISO/IEC 27001 to define, protect and manage the information within the cybersecurity evaluation process.

34 The **Laboratory** information security management system shall include:

a) Risk management system as a basis of the information security management system framework;

b) A risk assessment procedure according to a well-known and widely recognized

uznawaną metodyką, taką jak normy PN-EN ISO 31000 lub PN-EN ISO/IEC 27005;

c) Politykę bezpieczeństwa informacji zgodną z normą PN-EN ISO/IEC 27002;

d) Plan ciągłości działania, ograniczający pozostałe ryzyko, które nie jest objęte środkami bezpieczeństwa wprowadzonymi za pośrednictwem systemu zarządzania bezpieczeństwem informacji.

methodology, such as ISO 31000 or ISO/IEC 27005 standards;

c) An information security policy conformant to ISO/IEC 27002;

d) A business continuity plan mitigating the residual risks not covered by the security controls implemented in the information security management system.

7.3. Wymagania dotyczące prowadzenia ewaluacji

7.3 Requirements to the cybersecurity evaluation procedures

35 Procedury ewaluacji, obowiązujące w **Laboratorium** wnioskującym o autoryzację, muszą obejmować zasady współpracy i wymiany informacji z **Jednostką Certyfikującą**.

35 The cybersecurity evaluation procedures of the **Laboratory** requesting authorization must take into account the obligations of coordination and communication with the **Certification Body.**

36 **Jednostka Certyfikująca** przekazuje **Laboratorium** zobowiązania wymagane w odniesieniu do procedury ewaluacji i **Laboratoriów** zwarte w porozumieniach, uzgodnieniach lub umowach dotyczących wzajemnego uznawania certyfikatów.

36 The **Certification Body** transfers to the **Laboratory** the obligations in relation to the cybersecurity evaluation procedure and to the **Laboratory's** required by the agreements, arrangements or contracts concerning mutual recognition certificates.

7.3.1 Zasady współpracy i wymiany informacji

7.3.1 Coordination and Communication Obligations

37 **Jednostka Certyfikująca** uznaje jedynie te działania, które zostały wykonane przez **Laboratorium** w całości pod jej nadzorem i za jej wiedzą.

37 The **Certification Body**, shall only recognize the actions of the **Laboratory** that are performed completely under its knowledge and monitoring.

38 Procedury ewaluacyjne **Laboratorium** muszą zawierać:

38 The **Laboratory** cybersecurity evaluation procedures shall include:

a) Zakaz rozpoczynania ewaluacji bez uprzedniej pisemnej zgody **Jednostki Certyfikującej**. O zgodę **Laboratorium** wnioskuje na piśmie, z załączonymi dokumentami:

1) Plan ewaluacji zawierający etapy, zadania i odpowiadające im jednostki pracy oraz identyfikację, alokację i obowiązki personelu;

2) Kopia umowy lub innego równoważnego dokumentu, który

a) The prohibition of starting a cybersecurity evaluation without obtaining a previous approval in writing from the **Certification Body**. Approval is requested by the **Laboratory** in writing, accompanied by documents:

1) The plan of the cybersecurity evaluation, with phases, tasks and units of corresponding work, allocation and identification of personnel involved and their responsibilities;

2) A copy of the contract or similar document that regulates the relationship

reguluje relacje pomiędzy **Laboratorium** a Klientem wnioskującym o certyfikację;

between the **Laboratory** and the Client applying for certification;

b) Obowiązek powiadamiania **Jednostki Certyfikującej** o rozpoczęciu oraz zakończeniu każdego etapu, zadania i jednostki pracy związanej z ewaluacjami;

b) The obligation to notify the **Certification Body** of the start and finish of each phase, activity, action and unit of work of the cybersecurity evaluation;

c) Obowiązek powiadamiania Jednostki Certyfikującej o odstępstwach od założonego planu ewaluacji;

c) The obligation to notify the **Certification Body** of deviations regarding the cybersecurity evaluation plan;

d) Obowiązek powiadamiania **Jednostki Certyfikującej** o wszelkich zaistniałych trudnościach mających wpływ na realizację ewaluacji;

d) The obligation to notify the **Certification Body** of any arisen difficulty that affects the normal course of a cybersecurity evaluation;

e) Obowiązek powiadamiania **Jednostki Certyfikującej** o wszelkich wydanych raportach obserwacyjnych i raportach o niezgodnościach;

e) The obligation to notify the **Certification Body** of all the observation and nonconformity reports issued;

f) Obowiązek przekazywania wszelkich dodatkowych informacji technicznych – niezbędnych do analizy informacji z ewaluacji przez **Jednostkę Certyfikującą**;

f) The obligation to provide all additional technical information that is necessary for the analysis by the **Certification Body** cybersecurity evaluation information;

g) Obowiązek powiadamiania i zapraszania przedstawicieli **Jednostki Certyfikującej** na każde spotkanie, jakie **Laboratorium** organizuje z Klientem;

g) The obligation to notify and invite **Certification Body** representatives to whichever meetings the **Laboratory** holds with the Client;

h) Zobowiązanie **Laboratorium** do uczestnictwa we wszystkich spotkaniach monitorujących organizowanych przez **Jednostkę Certyfikującą**;

h) The obligation of the **Laboratory** to attend whichever monitoring meetings the **Certification Body** calls;

i) Zobowiązanie **Laboratorium** do udostępnienia swoich systemów i stanowisk badawczych do wglądu **Jednostki Certyfikującej**.

i) The obligation of the **Laboratory** to place its tests systems and premises at the disposal of the **Certification Body**.

39 **Laboratorium** zapewnia **Jednostce Certyfikującej** pełny dostęp do wszystkich informacji dotyczących przeprowadzanych przez siebie ewaluacji, jeśli są wykonywane w trybie nadzoru **Jednostki Certyfikującej.**

39 The **Laboratory** shall facilitate the **Certification Body** full access to all the information concerning the cybersecurity evaluation it performs, if they are performed under the surveillance of the **Certification Body**.

40 W przypadku certyfikacji nadzorowanych **Laboratorium** jest zobowiązane uzyskać pisemne upoważnienie od **Jednostki**

40 In the case of surveillance certification the **Laboratory** shall obtain written authorisation from the **Certification Body**

	Certyfikującej przed udzieleniem jakiejkolwiek osobie trzeciej, w tym twórcy Przedmiotu Oceny, dostępu do informacji pochodzących z oceny, takich jak plany, testy, analizy lub wyniki ewaluacji. **Uwaga:** Zapis nie dotyczy uzgodnień pomiędzy laboratorium oraz klientem przed rozpoczęciem procesu certyfikacji, które umożliwiają przygotowanie do ewaluacji, w tym opracowanie jej planu i oszacowanie pracochłonności.		before granting to any third party, including the developer of the Product to Evaluate, access to information from the evaluation such as plans, cybersecurity evaluation, **analysis or test findings.** **Note:** This does not refer to arrangements between laboratory and the client prior to beginning the certification process, which enable preparation for the evaluation, including planning and estimation of the work involved.
41	**Jednostka Certyfikująca** może zakazać rozpowszechniania informacji opracowanych przez **Laboratorium**. wykonywanych pod nadzorem **Jednostki Certyfikującej.**	41	The **Certification Body** may forbid the distribution of information produced by the **Laboratory** performed under the surveillance of the **Certification Body.**
42	Szczegółowe wymagania dotyczące zobowiązań **Laboratorium** w zakresie komunikacji z **Jednostką Certyfikującą** są określone w procedurze autoryzacji laboratorium.	42	Detailed requirements for the **Laboratory** obligations to communicate with the **Certification Body** are specified in the laboratory authorization procedure.

8. Certyfikacja produktu

43 **Jednostka Certyfikująca** przeprowadza proces certyfikacji produktu IT zgodnie z niniejszym Programem Certyfikacji i procedurami certyfikacji produktu określonymi w dokumencie P33.

44 Certyfikacja bezpieczeństwa produktu rozpoczyna się od złożenia wniosku o certyfikację przez Klienta do **Jednostki Certyfikującej**.

45 Klient wnioskujący o certyfikację (Wnioskodawca) wskazuje **Laboratorium**, które przeprowadzi ewaluację zgodnie z kryteriami, metodami i normami oceny bezpieczeństwa IT wskazanymi (jak w pkt 10) przez **Jednostkę Certyfikującą**. Przeprowadzenie ewaluacji przez laboratorium nie posiadające licencji wymaga aprobaty **Jednostki Certyfikującej**.

46 Procedura autoryzacji laboratoriów jako podwykonawców w procesie oceny produktu IT obejmuje licencjonowanie lub aprobatę. Licencjonowane laboratoria są upoważnione do przeprowadzania ewaluacji w procesie certyfikacji na czas nieokreślony, natomiast aprobata dotyczy jednorazowego zezwolenia na wykonanie ewaluacji.

47 Warunki ogólne do wykonywania ewaluacji zostały opisane w niniejszym programie a ich uszczegółowienie następuje w procedurach dotyczących autoryzacji laboratoriów.

48 Certyfikacja produktu lub systemu IT zakłada wiarygodność oświadczeń dotyczących właściwości cyberbezpieczeństwa wyłożonych w odnośnej Specyfikacji Zabezpieczeń.

49 Niezależnie od powyższego, certyfikacji produktu nie należy rozumieć jako deklaracji słuszności zastosowania certyfikowanego produktu w dowolnym przypadku lub obszarze zastosowań. W celu dokonania poprawnej oceny zasadności certyfikatu muszą być wzięte pod uwagę dodatkowe czynniki, w tym

8. Product Certification

43 The **Certification Body** conducts the certification process of IT products according to this Certification Scheme and product certification procedures as laid down in P33 document.

44 The certification of product cybersecurity starts with the certification application form submission by the Client to the **Certification Body**.

45 When applying for certification, the Client (Applicant) indicates a **Laboratory** that will conduct cybersecurity evaluation in accordance with the criteria, methods, and standards for IT security evaluation indicated (see point 10) by the **Certification Body**. Cybersecurity evaluation by a non-licensed laboratory requires approval of the **Certification Body**.

46 The procedure for authorizing laboratories as subcontractors in the IT product evaluation process includes licensing or approval. Licensed laboratories are authorized to perform cybersecurity evaluation in the certification process for an indefinite period of time, while approval refers to a one-off authorisation to carry out cybersecurity evaluation.

47 The general requirements for performing cybersecurity evaluations are described in this scheme and are laid down in detail within procedures for laboratory authorization.

48 The cybersecurity certification of an IT product or system presumes the recognition of the veracity of the cybersecurity properties of the corresponding Security Target.

49 Nevertheless, the cybersecurity certification of a product or system does not presuppose a declaration of suitability of the certified product for use in any scenario or field of application. For assessing the suitability other factors must be considered, including the restrictions established in the Security Target for the correct interpretation of the certificate.

ograniczenia określone w Specyfikacji Zabezpieczeń.

8.1. Zakres certyfikacji

50 Certyfikacja jest ograniczona przez zakres, który definiuje Przedmiot Oceny oraz normy i poziomy oceny.

51 **Jednostka Certyfikująca** wymaga precyzyjnego określenia zakresu, tak aby uniknąć utożsamiania produktu komercyjnego z Przedmiotem Oceny w sytuacji, gdy ten ostatni jest częścią pierwszego, lecz nie jest z nim tożsamy.

8.1.1. Odniesienia do ocenianego produktu

52 Certyfikacja odnosi się do danego produktu i jego Specyfikacji Zabezpieczeń.

53 Specyfikacja Zabezpieczeń musi zawierać precyzyjne określenie Przedmiotu Oceny, specyfikacji środowiska użytkowego, w tym przewidywanych zagrożeń, stosowanych polityk i założeń dotyczących bezpieczeństwa, szczegółów zabezpieczeń produktu lub systemu i listę niezbędnych wymagań bezpieczeństwa. Poziom szczegółowości deklaracji może różnić się w zależności od stosowanej w ocenie normy, jednak deklaracja ta musi w jasny i prawdziwy sposób oddawać właściwości bezpieczeństwa produktu lub systemu.

8.1.2. Odniesienia do norm i poziomów oceny

54 Zakres certyfikacji musi określać kryteria, metody i normy zastosowane w ocenie produktu lub systemu, jak również określać poziom, jaki został osiągnięty w odniesieniu do każdej z norm wraz z wykazem zastosowanych interpretacji oraz wytycznych.

8.2. Dowody zgodności – kryteria certyfikacji

8.2.1. Techniczny Raport Ewaluacyjny

55 Głównym materiałem dowodowym wykorzystywanym w procesie certyfikacji jest Techniczny Raport Ewaluacyjny (*ang. ETR*), wydany przez autoryzowane

8.1 Certification Scope

50 The certification is limited by the scope, which includes the definition of the Product to Evaluate and of the evaluation standards and levels.

51 The **Certification Body** shall only allow a precise definition of the scope, so as to avoid confusion between a commercial product and the Product to Evaluate in cases where the latter is part of, but not equal to the former.

8.1.1 Reference to the Evaluated Product

52 The certification shall relate to the evaluated product, as well as its Security Target.

53 This Security Target must contain the precise identification of the Product to Evaluate the specification of the environment of use, including the predicted threats, applicable security policies and assumptions, further details of the security objectives of the product or system, and the list of its necessary security requirements. The details of the declaration may vary conforming to the standards applied in the evaluation, but such a declaration must be a true and clear reflection of the security properties of the product or system.

8.1.2 Reference to the Standards and Levels of Evaluation

54 The certification shall include in its scope the criteria, methods and standards of evaluation used in the evaluation of the product or system, as well as the level that has been reached in accordance with each standard and the list of interpretations and guidance applied.

8.2 Evidence of conformity - certification criteria

8.2.1 Evaluation Technical Report

55 The principal evidence in the carrying out of the certification process is the Evaluation Technical Report (ETR), issued by the authorized **Laboratory** and created

Laboratorium zgodnie z procedurami certyfikacji produktu.

Uwaga: Techniczny Raport Ewaluacyjny stanowi sprawozdanie z ewaluacji zawierające stwierdzenia zgodności ze specyfikacją lub normami.

in accordance with product certification procedures.

Note: The Technical Evaluation Report is a cybersecurity evaluation report containing statements of conformity with a specification or standards.

8.2.2. Kryteria uzupełniające

56 **Jednostka Certyfikująca** może według własnego uznania przeprowadzać analizy, badania, inspekcje i audyty w odniesieniu do:

a) **Laboratorium**, dotyczące ewaluacji produktu;

b) **Wnioskodawcy**, w zakresie uzasadnienia zaufania w stosowanych metodach i kryteriach oceny;

c) **Przedmiotu Oceny** w zakresie spełnienia wymagań certyfikacyjnych.

8.2.2 Complementary criteria

56 The **Certification Body** can, at its discretion, perform analyses, tests, inspections and audits of the:

a) **Laboratory**; in the exercise of its cybersecurity evaluation of the product;

b) **Applicant**, in the aspects of security assurance applied in the applicable evaluation methods and criteria;

c) **Product to Evaluate** - in respect of compliance with certification requirements.

8.2.3. Nadzór nad ewaluacją

57 Nadzór nad ewaluacją musi pozwolić **Jednostce Certyfikującej** na potwierdzenie zgodności prowadzonych ewaluacji i w konsekwencji walidację Technicznego Raportu Ewaluacyjnego z mającymi zastosowanie normami.

8.2.3 Monitoring of evaluation

57 The monitoring of the evaluations shall allow the **Certification Body** to determine the compliance of the cybersecurity evaluation and consequently to validate the Evaluation Technical Report with the applicable standards.

8.3. Proces certyfikacji

58 Wnioskodawcę i **Laboratorium** obowiązuje poniższy sposób działania:

8.3 Certification Process

58 The Applicant and the **Laboratory** are required to act as follows:

8.3.1. Wniosek o certyfikację

59 Wniosek o certyfikację musi być przesłany do **Jednostki Certyfikującej** wraz z właściwie udokumentowanymi informacjami. Należy dołączyć co najmniej:

a) dane identyfikacyjne Wnioskodawcy, wraz z numerem identyfikacji podatkowej lub innym ekwiwalentnym numerem;

b) dane personalne osoby/osób umocowanych do złożenia wniosku o certyfikację, które będą sygnatariuszami wniosku i w związku z tym będą odpowiedzialne

8.3.1 Certification Application

59 The application of the certification must be sent to the **Certification Body**, along with, at the minimum, the following properly documented information:

a) Identification data of the Applicant, with the fiscal identification number, or whatever figure is applicable;

b) The name of the person(s) with sufficient authority to submit the application, who shall be signatories, and as such responsible, for the veracity of the proofs and documentary evidence supplied;

za wiarygodność przedstawionego materiału dowodowego;

c) oświadczenie o zapoznaniu się i akceptacji mających zastosowanie warunków i wymagań wnioskowanej certyfikacji, w tym praw dostępu, oraz ograniczeń dotyczących publikacji informacji dotyczących działań związanych z oceną przez **Jednostkę Certyfikującą;**

c) Liability declaration of knowing and accepting the applicable terms and requirements to the certification requested, including the access rights, publication and limitation of the evaluation activities information by the **Certification Body**;

d) wskazanie **Laboratorium**, które przeprowadzi ewaluacje bezpieczeństwa produktu lub systemu, o którego certyfikację się wnosi;

d) Identification of the **Laboratory** who shall carry out the cybersecurity evaluation of the product or system security whose certification is requested;

e) listę siedzib, oddziałów i obiektów, wraz z ich lokalizacjami, gdzie prowadzone są prace nad rozwojem i integracją Przedmiotu Ewaluacji;

e) List and location of the premises, branches and facilities where the activity of development or integration of the Product to Evaluate takes place;

f) zakres wnioskowanej certyfikacji, wskazujący:

f) Scope of the requested certification, indicating:

1) Przedmiot Oceny z dołączoną szczegółową Specyfikacją Zabezpieczeń i jeśli ma to zastosowanie, Profilem Zabezpieczeń;

1) Product to Evaluate with a sufficiently detailed Security Target attached, and (if applicable) a Protection Profile;

2) normy i poziomy oceny, względem których ma być przeprowadzona ocena;

2) Applicable standards and levels of evaluation;

g) pisemny dowód uiszczenia opłaty za przegląd wniosku.

g) Written proof of the payment of the review application fee.

60 Wnioskodawca na wniosek **Jednostki Certyfikującej** jest zobowiązany do przeprowadzenia demonstracji Przedmiotu Oceny i szczegółowej prezentacji zakresu certyfikacji.

60 The Applicant upon request of the **Certification Body** is obliged to perform a demonstration of the Product to Evaluate and a detailed presentation concerning the certification scope.

61 Wnioskodawca jest zobowiązany do udostępnienia Przedmiotu Oceny **Jednostce Certyfikującej** w uzgodniony sposób:

61 The Applicant is obliged to make the Product to Evaluate available to the **Certification Body** in the agreed manner:

a) Wnioskodawca dostarcza do **Jednostki Certyfikującej** egzemplarz, kopię lub przykład Przedmiotu Oceny. W uzasadnionym przypadku, gdy produkt jest w fazie rozwoju, dostarczenie może być przełożone nie dłużej niż do momentu podjęcia decyzji certyfikacyjnej, lub

a) The Applicant delivers a unit, copy or sample of the Product to Evaluate to the **Certification Body**. In justified cases, when the product is still under development, delivery can be postponed to the date of the decision of the certification request, or

b) w uzasadnionym przypadku Przedmiot Oceny jest dostępny dla **Jednostki Certyfikującej** w **Laboratorium** w okresie prowadzenia ewaluacji.

b) In justified cases, the Product to Evaluate shall be available to the **Certification Body** only on the premises of the **Laboratory** while under cybersecurity evaluation.

62 Powyższe rozstrzygnięcia są zawarte w Umowie o świadczenie usług certyfikacyjnych.

62 The above settlements are included in the Certification Agreement.

63 Wnioskodawca ma obowiązek przechowywania certyfikowanego Przedmiotu Oceny i dokumentacji procesu certyfikacji z nim związanej oraz udostępniania ich na żądanie **Jednostki Certyfikującej** w trakcie obowiązywania certyfikatu oraz przez okres co najmniej 3 lat po jego wygaśnięciu.

63 The Applicant is obliged to store the certificated Product to Evaluate associated certification documentation and made available on its request to the **Certification Body** during the validity of the certificate and for a period of at least three years after the expiration date of the certificate.

64 Wnioskodawca ustala z wybranym **Laboratorium** szczegółowy plan ewaluacji oraz podpisuje umowę lub inny równoważny dokument regulujący zobowiązania pomiędzy Wnioskodawcą a **Laboratorium**.

64 The Applicant shall agree with the chosen **Laboratory** on the detailed cybersecurity evaluation plan, as well as the contract or similar document that regulates the relations between the **Laboratory** and the Applicant.

8.3.2 Przegląd wniosku o certyfikację

8.3.2 Review of the Certification Application

65 Po otrzymaniu wniosku o certyfikację, **Jednostka Certyfikująca** przeprowadza wstępną weryfikację otrzymanych informacji. Wzór wniosku jest dostępny w **Jednostce Certyfikującej** na życzenie.

65 On reception of the certification application, the **Certification Body** shall perform an initial verification of the received information. An application form is available from the **Certification Body** on request.

66 Wnioskodawca jest zobowiązany do usunięcia wskazanych uchybień we wniosku. W przypadku nieuzupełniania braków wniosek zostaje odrzucony.

66 The Applicant shall be required to remediate indicated deficiencies in the request. Otherwise, the certification request shall be rejected.

67 Wnioskodawca może być również zobowiązany do dostarczenia dodatkowych egzemplarzy, kopii lub próbek produktu poddawanego ocenie w zależności od jego charakteru i zgodnie z potrzebami kryteriów uzupełniających certyfikacji.

67 The Applicant can equally be required to provide additional units, copies or samples of the product to evaluate, according to its nature and to the needs of the complementary certification criteria.

68 Wnioskodawca jest zobowiązany do aktualizacji dokumentacji i materiału zawartego we wniosku o certyfikację przekazanych **Jednostce Certyfikującej**, jeśli występują w nich zmiany wynikające z procesu oceny.

68 The Applicant shall be obliged to keep the documentation and material included in the certification application held by the **Certification Body** up-to-date, where there are modifications resulting from the evaluation process.

8.3.3. Powiadomienie Wnioskodawcy

69 **Jednostka Certyfikująca** powiadamia Wnioskodawcę o rozpoczęciu procesu certyfikacji, w tym o danych kontaktowych osoby odpowiedzialnej za proces certyfikacji.

8.3.4 Zgoda na rozpoczęcie ewaluacji

70 **Laboratorium** wnioskuje do **Jednostki Certyfikującej** o zgodę na rozpoczęcie ewaluacji. Do wniosku dołączyć należy:

a) plan ewaluacji, zawierający fazy, zadania i jednostki pracy oraz przydzielony personel zaangażowany w ewaluacje wraz z przypisanymi do personelu odpowiedzialnościami;

b) kopię umowy lub innego równoważnego dokumentu regulującego relacje pomiędzy **Laboratorium** a Wnioskodawcą, w której **Laboratorium** obowiązkowo zawrze klauzule dotyczące spełnienia wymagań bezpieczeństwa.

71 **Laboratorium** musi wykazać zgodność i adekwatność fizycznych i osobowych zasobów przydzielonych do procesu ewaluacji, w szczególności w kwestii przeszkolenia personelu w zakresie szczegółów zakresu certyfikacji.

72 **Jednostka Certyfikująca** wydaje decyzję o zgodzie na rozpoczęcie ewaluacji na piśmie.

8.3.5. Procedury oceny

73 Ocena[1] jest prowadzona zgodnie z następującymi zasadami:

a) **Jednostka Certyfikująca** dokonuje wyboru działań związanych z oceną poprzez zaplanowanie procesu oceny, określenie wymagań oraz zebranie

8.3.3 Notification to the Applicant

69 The **Certification Body** shall notify the Applicant of the start of the certification process, including in this notification the name and contact details of the person in charge of the certification process.

8.3.4 Approval of the Start of the Tests

70 **Laboratory** shall request from the **Certification Body** the authorization to start the cybersecurity evaluation. The application shall be accompanied by:

a) The cybersecurity evaluation plan, with the phases, tasks and units of corresponding work, the appointment and identification of the personnel involved in the cybersecurity evaluation and their responsibilities;

b) A copy of the contract or similar document that regulates the relationship between the **Laboratory** and the Applicant, in which the **Laboratory** shall obligatorily include the necessary clauses for the fulfilment of the security requirements.

71 **Laboratory** must demonstrate the correspondence and adequacy of the physical and human resources allocated to the cybersecurity evaluation, in particular regarding the training of the evaluator personnel in the details of the certification scope.

72 The **Certification Body** shall make a decision on the authorization of the start of the cybersecurity evaluation activities in writing.

8.3.5 Evaluation Procedures

73 The evaluation[2] shall be performed conforming to the following:

a) The **Certification Body** shall make the selection by planning the process, defining the requirements and collecting

[1] Rozumiana zgodnie z normą PN-EN ISO/IEC 17065 jako połączenie funkcji wyboru i określenia działań związanych z oceną zgodności.

[2] Understood in accordance with EN ISO/IEC 17065 as a combination of the selection and determination functions of conformity assessment activities.

danych wejściowych do oceny zgodności;

b) **Jednostka Certyfikująca** określa właściwości poprzez ewaluację produktów IT, audyty, inspekcje oraz weryfikację dokumentacji, w tym:

1) w trakcie przeprowadzania przez **Laboratorium** ewaluacji produktu lub systemu **Jednostka Certyfikująca** prowadzi nadzór nad czynnościami ewaluacyjnymi. W ramach realizacji tego nadzoru **Laboratorium** przekazuje **Jednostce Certyfikującej**, informacje z ewaluacji, na podstawie których będą zwoływane niezbędne spotkania monitorujące;

2) **Laboratorium** przekazuje Techniczny Raport Ewaluacyjny w następujących przypadkach:

i. po zakończeniu każdego etapu ewaluacji;

ii. na żądanie **Jednostki Certyfikującej**.

the input data for conformity assessment.

b) The **Certification Body** shall determine of characteristics by cybersecurity evaluation of IT products, audits, inspections, and verification of documentation, including:

1) During the cybersecurity evaluation of the product or system performed by the **Laboratory**, monitoring of the cybersecurity evaluation activities by the **Certification Body** shall take place. For the fulfilment of this monitoring, the **Certification Body** shall receive cybersecurity evaluation information from the **Laboratory** in view of which it shall call monitoring meetings as necessary;

2) The Evaluation Technical Report shall be sent by the **Laboratory** in the following cases:

i. at the end of the cybersecurity evaluation phase;

ii. upon request by the **Certification Body**.

8.3.6 Raport Certyfikacyjny

74 Po otrzymaniu Technicznego Raportu Ewaluacyjnego, **Jednostka Certyfikująca** przygotowuje Raport Certyfikacyjny z wynikami i wnioskami wynikającymi z oceny i działań nadzorujących, który jest przesyłany do wiadomości Wnioskodawcy.

8.3.6 Certification Report

74 After receipt of the Technical Evaluation Report, the **Certification Body** prepares a Certification Report with the results and conclusions of the evaluation and monitoring activities, which is sent to the applicant informatively.

8.3.7. Spotkanie podsumowujące ocenę

75 Po otrzymaniu raportu **Jednostki Certyfikującej** Wnioskodawca jest wzywany na spotkanie podsumowujące ocenę.

76 Na spotkaniu przedstawiciele **Jednostki Certyfikującej** przedstawiają przedmiot, wagę i konsekwencje spostrzeżeń i niezgodności zidentyfikowanych podczas oceny i nadzoru nad nią, wraz z ich wpływem na decyzję certyfikacyjną.

8.3.7 Evaluation summary meeting

75 After receiving the report from the **Certification Body**, the Applicant shall be summoned to evaluation summary meeting.

76 In this meeting the **Certification Body** shall indicate the nature, seriousness and consequences of the observations and nonconformities identified during the evaluation and its monitoring, with their implications on the certification decision.

8.3.8. Przegląd i decyzja certyfikacyjna

77 **Jednostka Certyfikująca** wyznacza osobę lub osoby, które dokonują przeglądu dokumentacji zebranej w trakcie procesu certyfikacji.

78 Przegląd wszystkich informacji i wyników dotyczących oceny pod względem merytorycznym i formalnym ma na celu przedstawienie rekomendacji dotyczącej decyzji w sprawie certyfikacji.

79 Po dokonaniu przeglądu wyników procesu certyfikacji podejmowana jest **decyzja** o wydaniu lub odmowie wydania certyfikatu.

Uwaga: Wnioskodawca w przypadku decyzji o wydaniu certyfikatu jest zobowiązany do podpisania **kontraktu** określającego wymagania certyfikacyjne. Wzór kontraktu jest dostępny w **Jednostce Certyfikującej**.

80 Pozytywna decyzja certyfikacyjna zawiera w sobie przynajmniej następujące informacje:

a) zakres przyznanego certyfikatu;

b) datę wejścia w życie certyfikatu i datę jego wygaśnięcia.

81 Decyzja odmowna zawiera uzasadnienie odmowy.

82 W przypadku wydania decyzji odmownej Klient ma prawo w ciągu 14 dni od doręczenia decyzji złożyć odwołanie od decyzji do **Jednostki Certyfikującej** wraz z uzasadnieniem.

8.4. Warunki obowiązywania certyfikatu

83 Certyfikat przyznawany jest na okres do 5 lat, z wyjątkiem wprowadzenia zmian w warunkach przyznawania certyfikatów, naruszania warunków korzystania z certyfikatu lub wyraźnej rezygnacji z certyfikacji wyrażonej przez Klienta.

Uwaga 1: Warunkiem wydania certyfikatu jest podpisanie kontraktu certyfikacyjnego. Wzór kontraktu

8.3.8 Review and Certification Decision

77 The **Certification Body** designates a person or persons to review the documentation collected during the certification process.

78 The review of all information and results relating to the evaluation in terms of content and form is intended to provide a recommendation for a certification decision.

79 After reviewing the results of the certification process, a **decision** is made to issue or refuse to issue a certificate.

Note: In the case of a decision to issue a certificate, the Applicant is required to sign a **contract** specifying the certification requirements. A template of the contract is available in the **Certification Body**.

80 The positive decision of certification shall additionally contain at least the following points:

a) Scope of the certification awarded;

b) The effective and expiry date of the certificate.

81 The rejection decision shall include a rejection rationale.

82 In case of issuing a refusal decision, the Client has the right, within 14 days from the delivery of the decision, to appeal to the **Certification Body** with justification.

8.4 Certification Validity Terms

83 The certificate shall be awarded for up to five years, except for changes in the conditions the award is based on, nonfulfillment of these conditions, or explicit resignation by the Client.

Note 1: The prerequisite for issuing a certificate is signing a certification contract. A template of the contract specifying the

określający prawa i obowiązki stron jest dostępny w **Jednostce Certyfikującej**.

Uwaga 2: W przypadku zakończenia ważności certyfikatu **Jednostka Certyfikująca** wymaga zaprzestania powoływania się na certyfikat i zwrotu certyfikatu.

rights and obligations of the participants is available at the **Certification Body.**

Note 2: In the event of termination of the certificate, the **Certification Body** requires that the certificate be discontinued and returned.

84 W celu utrzymania certyfikatu **Jednostka Certyfikująca** przeprowadza niezbędne przeglądy ważności certyfikatu i działania w zakresie nadzoru jego wykorzystania, zgodnie z poniższymi zasadami.

84 For the maintenance of the certification, the **Certification Body** shall carry out the necessary reviews of its validity and monitoring activities of the use of the certificate, conforming to the following.

Uwaga 1: W przypadku zmiany wymagań norm lub interpretacji ich wymagań, klienci zostaną poinformowani poprzez stronę internetową **Jednostki Certyfikującej** oraz pisemnie.

Note 1: When the requirements of the standards change or their requirements are interpreted, clients will be informed via the **Certification Body's** web site and in writing.

Uwaga 2: Uzyskany przez Klienta certyfikat bezpieczeństwa produktu IT nie zwalnia go z odpowiedzialności za ten produkt ani nie może powodować przeniesienia części tej odpowiedzialności na **Jednostkę Certyfikującą**.

Note 2: The security certification of an IT product achieved by a Client does not relieve the customer of responsibility for that product, nor can it assign part of that responsibility to the **Certification Body.**

8.4.1. Przegląd ważności certyfikatu

8.4.1 Validity Review

85 Każdy certyfikat podlega przeglądowi co 2 lata. Celem przeglądu jest weryfikacja czy środowisko użytkowania certyfikowanego produktu nie uległo zmianie, np. w wyniku zmian technologicznych, pojawienia się nowych podatności lub innych aspektów podważających założenia, hipotezy, analizy ryzyka i polityki bezpieczeństwa dotyczące tego środowiska użytkowania.

85 Every two years a review of the validity of each certificate issued shall be performed. The aim of this review is to check that the environment of use of the product certificate has not undergone variations, such as technological changes, appearance of new vulnerabilities or any other aspect that could invalidate the hypotheses, risk analyses and security policies reflected in this environment of use.

86 Przegląd ważności certyfikatu może spowodować zawieszenie, ograniczenie lub cofnięcie certyfikatu.

86 The validity review of the certificate may result in suspension, reduction, or withdrawal of the certificate.

8.4.2. Nadzór nad wykorzystaniem certyfikatu

8.4.2 Monitoring of Certificate Use

87 **Jednostka Certyfikująca** prowadzi ciągły nadzór nad wykorzystywaniem wydanych certyfikatów poprzez analizę oraz rejestrację wszelkich znanych **Jednostce Certyfikującej** technicznych i handlowych informacji odnoszących się do wydanego certyfikatu.

87 The **Certification Body** shall perform a continuous monitoring of the use of the certificates issued, by means of analyses and record of all any information available to the **Certification Body** commercial or technical information that makes reference to the certification issued.

88 Naruszenie warunków użytkowania certyfikatu może spowodować cofnięcie, zawieszenie lub ograniczenie certyfikatu.

88 The nonfulfillment of the conditions of use of the certificate can give rise to the withdrawal, suspension or reduction of the certificate.

8.5. Zmiana zakresu certyfikatu

8.5 Change of Certificate Scope

89 W celu zmiany zakresu certyfikatu produktu lub systemu Klient składa formalny wniosek w tej sprawie. Procedura jest dopasowywana do zakresu i charakteru zmiany. i może powodować ograniczenie lub rozszerzenie zakresu certyfikatu. Ograniczenie zakresu certyfikatu może nastąpić również w wyniku prowadzenia nadzoru nad certyfikatem.

89 When change of the scope of a product or system certification is desired, the Client shall formally request this extension. The procedure shall be adjusted to the scope and nature of the change and may result in a reduction or extension of the scope of the certificate. A reduction in the scope of the certificate may also result from the monitoring use of the certificate.

8.6. Powiadamianie o zmianach

8.6 Change Notification

90 Wnioskodawca jest zobowiązany do informowania **Jednostki Certyfikującej** o zidentyfikowanych zmianach dotyczących bezpieczeństwa środowiska certyfikowanego produktu, jak również o wszelkich innych istotnych zmianach dotyczących warunków wstępnych, na jakich certyfikat został przyznany.

90 The applicant must inform the **Certification Body** of the changes that it identifies regarding the security environment of the product certified, as well as any other fundamental change in the initial conditions under which certification was awarded.

8.7. Publikowanie informacji o certyfikacie

8.7 Publishing information about the certificate

91 **Jednostka Certyfikująca** publikuje listę produktów poddawanych ocenie oraz listę certyfikowanych produktów ze wskazaniem ich Specyfikacji Zabezpieczeń lub Profilu Zabezpieczeń, a także informacje z raportu certyfikacyjnego. Lista produktów identyfikuje nazwę i adres klienta, produkt, datę wydania certyfikatu, datę ważności certyfikatu oraz normę, na podstawie której produkt jest certyfikowany.

91 The **Certification Body** publishes the list of products in process of evaluation, as well as of certified products, including in this respect, their Security Target or Protection Profile, as well as information from the certification report. The product list identifies the name and address of the customer, the product, the date of issue of the certificate, the expiry date of the certificate and the standard under which the product is certified.

8.8. Spostrzeżenia, zawieszenie lub cofnięcie certyfikatu

8.8 Observations, Suspension and Withdrawal of the Certificate

92 Niewypełnianie przez Wnioskodawcę warunków użytkowania certyfikatu, nieprawidłowe powołanie się na program certyfikacji lub wprowadzającego w błąd wykorzystanie certyfikatu, w zależności od wagi zidentyfikowanej niezgodności, może skutkować poniższymi konsekwencjami.

92 The non-fulfilment by an applicant of the certification obligations, incorrect reference to a certification scheme or misleading use of a certificate shall cause the following measures to be adopted depending on the seriousness of the nonconformity.

8.8.1. Spostrzeżenia

93 Spostrzeżenie jest stwierdzeniem faktu, wskazującego na możliwość doskonalenia istniejącego stanu, w tym możliwość usunięcia potencjalnych źródeł problemów, mogących w przyszłości spowodować niezgodność.

8.8.2. Cofnięcie lub zawieszenie

94 Cofnięcie lub zawieszenie certyfikatu jest skutkiem utrzymującej się niezgodności względem ograniczeń bądź warunków wykorzystania certyfikatu, wymagań certyfikacyjnych lub w wyniku niewdrażania działań korygujących względem formułowanych spostrzeżeń.

95 Cofnięcie certyfikatu obliguje Wnioskodawcę do niezwłocznego zaprzestania używania statusu certyfikowanego produktu we wszystkich dokumentach i miejscach, w których dotychczas informacja ta była udostępniona oraz zwrotu dokumentów certyfikacyjnych.

8.9. Termin wydania decyzji

96 Termin na wydanie decyzji certyfikacyjnej wynosi do 60 dni kalendarzowych od daty otrzymania Technicznego Raportu Ewaluacyjnego z **Laboratorium**.

97 W przypadku wniosku o zmianę zakresu certyfikatu, co do którego nie jest wymagany Techniczny Raport Ewaluacyjny, decyzja jest wydawana również w terminie 60 dni od daty złożenia wniosku.

98 Termin na rozpatrzenie wniosku o wyrażenie zgody na rozpoczęcie ewaluacji wynosi 14 dni kalendarzowych od daty złożenia do **Jednostki Certyfikującej**.

8.10. Odwołania i skargi

99 Klient ma prawo odwołać się od decyzji w sprawie certyfikacji lub złożyć skargę do **Jednostki Certyfikującej**.

99 **Jednostka Certyfikująca** posiada zdefiniowany i udostępniony publicznie proces obsługi odwołań i skarg, zgodny

8.8.1 Observations

93 Observation is a recognition of fact indicating an opportunity to improve the existing status, including an opportunity to remove potential sources of problems that may cause future nonconformance.

8.8.2 Withdrawal or Suspension

94 Withdrawal or suspension of the certificate is the result of persistent non-compliance with the restrictions or conditions for the use of the certificate, certification requirements or as a result of failure to implement corrective actions against the formulated observations.

95 The withdrawal of the certification shall oblige the applicant to immediately cease using the product certificate status, in all documents or information in which it was used, including withdrawing from the market of the products so labelled and return of certification documents.

8.9 Term for Decisions

96 The term to issue a certification decision, shall be up to 60 days from the reception date of the Evaluation Technical Report from **Laboratory**.

97 The decision concerning the change of the certification scope for which there is no need for an Evaluation Technical Report shall be issued also within sixty days from the reception of the request.

98 The term to issue a decision for approval to start the evaluation shall be 14 calendar days from the submission date of the request to the **Certification Body**.

8.10 Appeals and Complaints

98 The Client has the right to appeal the certification decision or complain to the **Certification Body**.

99 The **Certification Body** shall have, and make publicly available, defined a process to handle appeals and complaints that

z wymaganiami normy PN-EN ISO/IEC 17065.

complies with the requirements from ISO/IEC 17065.

100 **Laboratorium** posiada zdefiniowany udostępniony publicznie proces obsługi odwołań i skarg, zgodny z wymaganiami normy PN EN ISO/IEC 17025.

100 **Laboratory** shall have, and make publicly available, a defined process to handle appeals and complaints that complies with the ISO/IEC 17025.

101 Sposób postępowania określony w odpowiednich procedurach odwołań i skarg stanowi podstawę do rozpatrywania sporów pomiędzy rolami określonymi w Programie Certyfikacji.

102 The approach set out in the relevant procedures for appeals and complaints is the basis for resolving disputes between the roles defined in the Certification Scheme.

8.11. Opłaty

8.11 Charges

103 Klient jest zobowiązany pokryć koszty certyfikacji zgodnie z zawartą umową, niezależnie od jej wyników. Opłaty są ustalane indywidulanie z uwzględnieniem zakresu wnioskowanej przez Klienta certyfikacji. Informacja o wysokości opłat jest przekazywana Klientowi przed podpisaniem umowy. Opłata wstępna za rozpatrzenie wniosku jest stała – aktualna jej wysokość jest określona na stronie internetowej NASK-PIB.

103 The Client is obliged to finance the certificate in accordance with the concluded agreement, independently of its results. Fees are set individually taking into account the scope of certification requested by the Client. Information on the amount of fees is provided to the Client before signing the agreement. Initial fee for application review is fixed - its current amount is specified on NASK-PIB website.

8.12 Język

8.12 Language

104 W przypadku rozbieżności co do interpretacji zapisów niniejszego dokumentu pierwszeństwo ma wersja polska.

104 In case of divergences in the interpretation of the wording of this document, the Polish version shall have precedence.

9. Warunki korzystania ze statusu certyfikowanego produktu

9.1. Warunki używania statusu certyfikowanego produktu

105 Używanie odniesienia do stanu statusu certyfikowanego produktu jest środkiem, za pomocą którego Wnioskodawcy oświadczają publicznie, że spełniają wszystkie przewidziane wymagania, które mogą obejmować certyfikację zgodności z profilem zabezpieczeń i mającymi zastosowanie przepisami prawnymi.

106 Każde użycie certyfikatu, które nie jest wyraźnie dozwolone w niniejszym programie, musi być najpierw skonsultowane z **Jednostką Certyfikującą**.

9.1.1. Produkt i dołączona dokumentacja

107 Odwołanie do statusu certyfikowanego produktu musi być stosowane we wszelkiej dokumentacji administratora i użytkownika, która została wykorzystana jako materiał dowodowy producenta podczas ewaluacji.

108 Odniesienie do statusu certyfikowanego produktu powinno być zgodne z zasadami identyfikacji certyfikowanych produktów określonymi przez **Jednostkę Certyfikującą**.

9.1.2 Pozostałe dokumenty

109 W materiałach reklamowych lub broszurach związanych z certyfikowanym produktem Klienci mogą stosować odniesienia do statusu certyfikowanego produktu z ograniczeniami określonymi w Programie Certyfikacji.

9.2. Ograniczenia dotyczące używania statusu certyfikowanego produktu

110 Odwołania do statusu certyfikowanego produktu nie mogą być stosowane w następujących okolicznościach:

a) Bez pełnych i jednoznacznych odniesień do zakresu certyfikatu. Informacja powinna zawierać jako minimum:

9. Conditions on the Use of Certified Product Status

9.1 Conditions of Use of the Certified Product Status

105 The use of the reference to the condition of certified product status is the means by which the certification applicants publicly declare the fulfilment of all the stipulated requirements, which may include the certification of conformity of protection profiles and applicable legal dispositions.

106 Any use of the certificate not explicitly permitted in the current scheme must first be consulted with the **Certification Body**.

9.1.1 Product and Attached Documentation

107 The reference to the certified product status must be used in all the administrator and user documentation that was used as developer evidence in the evaluation.

108 The certified product status reference shall follow the rules of identification for certified products indicated by **Certification Body**.

9.1.2 Other Documents

109 In advertising documents or brochures related to the certified product, the certification Client can use the certified product status reference with the restrictions mentioned in Certification Scheme.

9.2 Restrictions Related to the Use of the Certified Product Status

110 The reference to the certified product status must not be used in the following circumstances:

a) Without a complete and unique references of the scope of the certificate. The information should include as a minimum:

i. nazwę i wersję Przedmiotu Oceny;

ii. normę i poziom oceny bezpieczeństwa;

iii. odniesienie do Specyfikacji Zabezpieczeń;

b) w sposób, który może sugerować, że certyfikat jest przyznany do całego systemu lub produktu, gdy ocenie podlegała jedynie jego część;

c) w sposób, który może sugerować istnienie właściwości cyberbezpieczeństwa produktu, które nie zostały odzwierciedlone w Specyfikacji Zabezpieczeń;

d) jeżeli certyfikat został cofnięty.

i. Name and version of the Product to Evaluate;

ii. The standard and the evaluation assurance level;

iii. Reference to the Security Target;

b) In a way that may suggest that the certificate is applied to an entire system or product, when the evaluated product is only a part;

c) In a way that may suggest the presence of cybersecurity properties of the product certificate not reflected in the Security Target;

d) When the certificate has been withdrawn.

9.3. Pozostałe warunki wykorzystania certyfikatu

111 Odwoływanie się do statusu certyfikowanego produktu zobowiązuje Wnioskodawcę do spełnienia następujących warunków:

a) prowadzenia ewidencji wszystkich skarg i reklamacji zgłaszanych Wnioskodawcy w zakresie cyberbezpieczeństwa certyfikowanego produktu oraz udostępnianie tej ewidencji na żądanie **Jednostki Certyfikującej**;

b) podejmowania odpowiednich działań korygujących w odniesieniu do skarg lub reklamacji oraz w odniesieniu do wszelkich wykrytych nieprawidłowości w produktach, które mają wpływ na zgodność z wymogami certyfikacji;

c) dokumentowania podjętych działań.

9.3 Other Obligations of the Use of the Certificates

111 The reference to the certified product status shall oblige the certification applicant to fulfil the following:

a) maintain records of all complaints and claim reported to the Client regarding the cybersecurity of the certified product and make such records available to the **Certification Body** upon request;

b) take appropriate corrective action with respect to complaints or claims, and any product deficiencies discovered that affect compliance with certification requirements;

c) document the actions taken.

9.4. Oznaczenie certyfikowanego produktu

112 Identyfikacja certyfikowanego produktu powinna być zgodna z zasadami określonymi przez **Jednostkę Certyfikującą**.

9.4 Labelling of the Certified Product

112 The identification of the certified product shall comply with the rules laid down by the **Certification Body**.

10. Kryteria i metodyki oceny

113 **Jednostka Certyfikująca** prowadzi certyfikacje bezpieczeństwa produktów i systemów IT zgodnie z aktualnym stanem wiedzy i dobrymi praktykami w zakresie oceny cyberbezpieczeństwa.

10.1. Normy dotyczące oceny

114 **Jednostka Certyfikująca,** w celu wykorzystania i wypełniania przez **Laboratoria** może publikować własne dokumenty normatywne do stosowania w Programie Certyfikacji.

115 Aktualny wykaz norm, metodyk, dokumentów normatywnych oraz zakres ich stosowania jest dostępny na stronie internetowej Programu Certyfikacji.

10.1.1. Kryteria oceny

a) CC Common Criteria (Wspólne kryteria do oceny zabezpieczeń informatycznych;) April 2017, Version 3.1, Revision 5;

b) PN-EN ISO/IEC 15408:2020-09 Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń;

c) PN-EN ISO/IEC 19790:2020-09 - Technika Informatyczna - Techniki Bezpieczeństwa - Wymagania zabezpieczeń dla modułów kryptograficznych.

10.1.2. Metodyki oceny

a) CEM (Wspólna metodyka oceny zabezpieczeń informatycznych); April 2017, Version 3.1, Revision 5;

b) PN-EN ISO/IEC 18045:2020-09 Technika informatyczna - Techniki bezpieczeństwa - Metodyka oceny zabezpieczeń informatycznych;

c) ISO/IEC 24759:2017 Test requirements for cryptographic module.

10. Evaluation Criteria and Methodologies

113 The **Certification Body** conducts security certifications of the IT products and systems according to the current knowledge and good practices in cyber security assessment.

10.1 Evaluation Standards

114 The **Certification Body**, for the purposes of use and fulfilment by the **Laboratories**, may publish its own normative documents for use in the Certification Scheme.

115 The current list of standards, methodologies, normative documents and its applicability can be consulted at the Certification Scheme's web site.

10.1.1 Evaluation Criteria

a) CC Common Criteria for Information Technology Security Evaluation; April 2017, Version 3.1, Revision 5;

b) ISO/IEC 15408:2014-01 Information technology - Security techniques - Evaluation criteria for IT security;

c) ISO/IEC 19790:2012 Information technology - Security techniques - Security requirements for cryptographic modules.

10.1.2 Evaluation Methodologies

a) CEM Common Methodology for Information Technology Security Evaluation; April 2017, Version 3.1, Revision 5;

b) ISO/IEC 18045:2008 Information technology - Security techniques - Methodology for IT security evaluation;

c) ISO/IEC 24759:2017 Test requirements for cryptographic module.

10.1.3. Wytyczne i interpretacje

116 Wytyczne i interpretacje (norm) mają charakter ogólny i dotyczą określonego zakresu stosowania.

117 Wykaz właściwych wytycznych i interpretacji (jeśli zostały wydane) jest udostępniany na stronie internetowej Programu Certyfikacji.

10.1.3 Guidance and interpretations

116 Guidance and interpretations (of standards) are of a general nature and apply to a specified scope of operation.

117 A list of relevant guidance and interpretations (if issued) is available on the Certification Scheme website.

Spis tabel

List of tabels