

Załącznik nr 15 do WZ



Wymagania ENEA Operator sp. z o. o. w zakresie bezpieczeństwa dla dostawców produktów i usług związanych z systemem informacyjnym Usługi Kluczowej

Zatwierdzone Uchwałą nr^{348/2021} Zarządu ENEA Operator Sp. z o.o. z dnia
.....^{23.11.2021} r. Obowiązuje od dnia^{01.12.2021} r.

SPIS TREŚCI

1	WPROWADZENIE	3
2	CEL I ZAKRES STOSOWANIA.....	3
3	PRZEPISY I NORMY	3
4	SŁOWNIK PODSTAWOWYCH POJĘĆ.....	5
5	DOKUMENTY POWIĄZANE.....	6
6	WERYFIKACJA SPEŁNIANIA WYMAGAŃ PRZEZ DOSTAWCĘ	6
7	BEZPIECZEŃSTWO REALIZACJI ZADAŃ	7
8	BEZPIECZEŃSTWO PROCESU PROJEKTOWEGO DOSTAWCY	10
9	BEZPIECZEŃSTWO BUDOWY ŚRODOWISK ROZWOJOWYCH I TESTOWYCH.....	11
10	AUDYTY BEZPIECZEŃSTWA DOSTAWCÓW	13
11	ZAKOŃCZENIE WSPÓŁPRACY	14
12	METRYKA DOKUMENTU	15

1 WPROWADZENIE

Dokument zawiera podstawowe wymagania w zakresie bezpieczeństwa jakie powinni spełniać Dostawcy usług, urządzeń lub oprogramowania związanego z systemem informacyjnym wykorzystywanym przez ENEA Operator Sp. z o. o. do świadczenia Usługi Kluczowej.

2 CEL I ZAKRES STOSOWANIA

Celem niniejszego dokumentu jest zapewnienie bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia Usługi Kluczowej przez Spółkę (zarówno już eksploatowanych, jak i planowanych do wdrożenia).

Dokument stosuje się dla dostawców oprogramowania oraz urządzeń działających w oparciu o procesor/mikroprocesor wykonujący program, którego kod znajduje się w pamięci tego urządzenia lub jest temu urządzeniu udostępniany w jakiegokolwiek sposób.

Opracowanie określa mechanizmy ochrony cyberbezpieczeństwa, w zakresie organizacji funkcjonowania bezpieczeństwa wewnętrznego Dostawcy oraz dostarczanych produktów (urządzeń, systemów, oprogramowania).

Wymagania sprawdzane są na etapie:

- wyboru Dostawcy w postępowaniu zakupowym,
- oraz w trakcie realizacji usługi / dostawy.

Zakres opracowania obejmuje:

- wymagania ogólne (organizacyjne) w zakresie bezpieczeństwa informacji,
- wykaz certyfikatów wymaganych dla organizacji,
- wymagania dla linii wytwórczej systemów lub oprogramowania,
- wymagania funkcjonalne dla dostarczanych systemów,
- wymagane certyfikaty dla dostarczanych urządzeń.

Szczegółowe wymagania techniczne dla urządzeń stosowanych w sieci dystrybucyjnej Enea Operator Sp. z o. o. określają Standardy wydane przez Radę Techniczną.

Niniejszy dokument obowiązuje w ENEA Operator Sp. z o.o.

Niniejszy dokument obowiązuje od dnia opublikowania.

Najnowsza wersja niniejszego dokumentu opublikowana jest na stronach internetowych ENEA Operator Sp. z o. o.

3 PRZEPISY I NORMY

Dokument uwzględnia, w szczególności następujące podstawowe materiały normatywne i regulacje:

- [1] DYREKTYWĘ PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.
- [2] Ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
- [3] ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ.
- [4] ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie).
- [5] Rodzinę norm Systemu Zarządzania Bezpieczeństwem Informacji:
 - ISO/IEC 27000, Information security management systems - Overview and vocabulary
 - ISO/IEC 27001, Information security management systems - Requirements
 - ISO/IEC 27002, Code of practice for information security controls

- ISO/IEC 27003, *Information security management system implementation guidance*
- ISO/IEC 27004, *Information security management - Measurement*
- ISO/IEC 27005, *Information security risk management*
- ISO/IEC 27006, *Requirements for bodies providing audit and certification of Information security management systems*
- ISO/IEC 27007, *Guidelines for Information security management systems auditing*
- ISO/IEC TR 27008, *Guidelines for auditors on Information security controls*
- ISO/IEC 27019, *Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry*
- [6]** Rodzinę norm IEC 62351 Zarządzanie systemem elektroenergetycznym i związana z tym wymiana informacji – Ochrona danych komunikacji:
- [7]** Rodzinę norm IEC 61970 Interfejs programu aplikacyjnego systemu zarządzania energią (EMS-API)
- [8]** Rodzinę norm IEC 61968 Integracja aplikacji w przedsiębiorstwach elektroenergetycznych – Interfejsy systemowe do zarządzania dystrybucją
- [9]** Rodzinę norm IEC 62325-351:2017 Struktura komunikacji dla rynku energii – Część 351: Profil CIM wymiany informacji dla europejskiego modelu rynku

Korzystając z niniejszego dokumentu należy każdorazowo sprawdzić aktualność przepisów i norm oraz uwzględnić postanowienia zawarte w najnowszych ich wydaniach. W przypadku przywołanych powyżej dokumentów zawierających datę, należy każdorazowo uwzględniać postanowienia w nich zawarte. Jeżeli w jakimkolwiek punkcie wymagania niniejszego dokumentu są ostrzejsze, aniżeli wymagania zawarte w najnowszych wydaniach przytoczonych powyżej przepisów i norm lub w ich zastąpieniach, to należy stosować się do wymagań określonych w „Wymaganiach ENEA Operator sp. z o. o. w zakresie bezpieczeństwa dla dostawców produktów i usług związanych z systemem informacyjnym Usługi Kluczowej”

Poprzez słowa „powinien”, „ma być” lub „należy” użyte w niniejszym dokumencie należy rozumieć „musi” lub „wymaga się”.

4 SŁOWNIK PODSTAWOWYCH POJĘĆ

Autentyczność	Właściwość Informacji polegająca na tym, że istnieje pewność co do jej pochodzenia (autor lub nadawca Informacji jest tym, za kogo się podaje).
Bezpieczeństwo Informacji	Zachowanie Poufności, Integralności, Dostępności i Autentyczności Informacji.
Bezpieczeństwo Teleinformatyczne	Cyberbezpieczeństwo w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa.
Cyberbezpieczeństwo	Odporność Systemów Informatycznych na działanie naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.
Dostawca Zewnętrzny	Osoba fizyczna niebędąca Pracownikiem, osoba prawna niewchodząca w skład Grupy ENEA lub jednostka organizacyjna niebędąca osobą prawną, której ustawa przyznaje zdolność prawną, którą łączy ze spółką Grupy ENEA umowa, na mocy której przekazywane są Informacje Chronione.
Dostępność	Właściwość Informacji polegająca na tym, że osoby lub podmioty upoważnione mogą korzystać z Informacji w danym miejscu i czasie.
Incydent	Zdarzenie, które ma lub może mieć niekorzystny wpływ na Cyberbezpieczeństwo.
Incydent Bezpieczeństwa Informacji	Niepożądane lub niespodziewane zdarzenie, stanowiące zagrożenie naruszenia zasad ochrony informacji, w tym naruszenie ochrony danych osobowych.
Incydent poważny	Incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej.
Informacja chroniona (klasyfikacja)	<ul style="list-style-type: none"> Informacja powzięta w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, dotycząca bezpośrednio lub pośrednio Spółki, gdy jej nieuprawnione ujawnienie poza Grupę ENEA może spowodować szkodę dla interesów Grupy ENEA i nie jest podana do wiadomości publicznej (Informacja klasy B); informacja powzięta w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, dotycząca bezpośrednio lub pośrednio Spółki, gdy jej nieuprawnione ujawnienie poza Spółkę może spowodować szkodę dla interesów Spółki i nie jest podana do wiadomości publicznej (Informacja klasy C); informacje spełniające kryteria dla klasy C, a dodatkowo o zasadniczym znaczeniu dla Spółki, dla której zachodzi uzasadniona potrzeba identyfikacji osób, które miały do niej dostęp (Informacja klasy D).
Integralność	Właściwość Informacji polegająca na tym, że nie podlega ona przypadkowej lub nieautoryzowanej zmianie, czyli jest dokładna, niezafałszowana i kompletna.
Poufność	Właściwość informacji polegająca na tym, że nie jest ona udostępniana na potrzeby nieupoważnionych osób, podmiotów oraz procesów.
Przepisy KSC	Ustawa z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa i jej przepisy wykonawcze.
Sieć OT ENEA Operator Sp. z o.o.	Sieć telekomunikacyjna (urządzenia aktywne i pasywne), umożliwiająca wymianę danych oraz sygnałów pomiędzy systemami, sterownikami, urządzeniami wykonawczymi oraz czujnikami uczestniczącymi w procesie sterowania i kontroli pracy elektroenergetycznej sieci dystrybucyjnej ENEA Operator Sp. z o.o.

Spółka	ENEA Operator Sp. z o.o.
SZBI	System Zarządzania Bezpieczeństwem Informacji według normy PN-EN ISO/IEC 27001.
System	Elektroenergetyczny system dystrybucyjny zarządzany przez Spółkę.
System informacyjny	System teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne ¹), wraz z przetwarzanymi w nim danymi w postaci elektronicznej
System teleinformatyczny	Zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego.
Urządzenie IED	Ang. Intelligent Electronic Device – Inteligentne urządzenia elektroniczne wykorzystywane w obszarze telemechaniki na stacjach elektroenergetycznych
Usługa kluczowa	Usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienionej w wykazie usług kluczowych. W przypadku ENEA Operator sp. z o.o. jest to dystrybucja energii elektrycznej

Pozostałe użyte w dokumencie definicje są zgodne z obowiązującymi w tym zakresie regulacjami wewnętrznymi ENEA Operator Sp. z o. o., w tym ze Standardami Rady Technicznej.

5 DOKUMENTY POWIĄZANE

Dokumentami powiązanymi z niniejszym opracowaniem są:

- Zasady Przetwarzania Informacji w Grupie Enea.
- Zasady Bezpieczeństwa Teleinformatycznego w Grupie Enea.
- Standardy Rady Technicznej.

6 WERYFIKACJA SPEŁNIANIA WYMAGAŃ PRZEZ DOSTAWCĘ

6.1 Weryfikacja spełnienia wymagań przez Dostawcę na etapie wyboru wykonawcy w procesie zamówienia.

W procesie wyboru Wykonawcy/Dostawcy w ramach postępowania zakupowego dokonywana jest weryfikacja spełnienia wymagań stawianych Dostawcy oraz dostarczonym produktom.

Potwierdzeniem spełnienia niżej opisanych wymagań w zakresie organizacji jest:

1. Posiadanie przez Dostawcę ważnego Certyfikatu dla Systemu Zarządzania wg. PN-EN ISO/IEC 27001:2017 wydanego przez akredytowaną jednostkę certyfikującą, albo
2. Oświadczenie Dostawcy o stosowaniu rozwiązań organizacyjnych Systemu Zarządzania Bezpieczeństwem Informacji opartych o system zarządzania wg. PN-EN ISO/IEC 27001:2017 wraz ze zgodą na weryfikację wymagań przez Zamawiającego.

Potwierdzeniem spełnienia niżej opisanych wymagań w odniesieniu do dostarczanych produktów jest:

¹ Dz. U. z 2017 r. poz. 570 oraz z 2018 r. poz. 1000 i 1544

1. Dla urządzeń IED i sterowników Telemekhaniki i Zabezpieczeń przedstawienie deklaracji zgodności urządzenia z normami określonymi w Standardach sieci dystrybucyjnej ENEA Operator Sp. z o.o., które dostępne są na stronach Spółki pod linkiem: <https://www.operator.enea.pl/infoosieci/instrukcje/standardysieci/standardwysiecidystribucyjnejieop>
2. Dla oprogramowania specjalistycznego i systemów sterowania typu SCADA przedstawienie ważnego Certyfikatu dla Systemu Zarządzania wg PN-EN ISO/IEC 27001:2017 wydanego przez akredytowaną jednostkę certyfikującą dla wytwórcy oprogramowania lub systemu.

6.2 Weryfikacja wymagań w trakcie realizacji zamówienia.

W trakcie realizacji zamówienia Dostawca umożliwia Zamawiającemu w procesie audytu sprawdzenie spełniania wymogów określonych w wymaganiach albo przedstawia ważny Certyfikat dla Systemu Zarządzania wg. PN-EN ISO/IEC 27001:2017.

7 BEZPIECZEŃSTWO REALIZACJI ZADAŃ

7.1 Wymagania ogólne

Dostawca POWINIEN zapewnić, że zadania realizowane na rzecz ENEA Operator Sp. z o.o. będą zarządzane zgodnie z najlepszymi praktykami określonymi w rozdz. 6.1. normy PN-EN ISO/IEC 27002:2017.

W szczególności MUSI zostać zapewnione, aby:

- a) Dostawca zidentyfikował cele bezpieczeństwa realizowanego przedsięwzięcia,
- b) Dostawca zidentyfikował i oszacował ryzyka związane z realizacją przedsięwzięcia,
- c) Dostawca zdefiniował i zastosował zabezpieczenia adekwatne do zidentyfikowanych ryzyk.

7.2 Klasyfikacja informacji

Dostawca POWINIEN stosować klasyfikację informacji przesyłanej, przechowywanej i przetwarzanej w kontekście realizacji zadań na rzecz Enea Operator Sp. z o.o., zgodnie z zasadami klasyfikacji określonymi w niniejszym dokumencie oraz najlepszymi praktykami określonymi w rozdz. 8.2 normy PN-EN ISO/IEC 27002:2017.

7.3 Bezpieczeństwo informacji

Dostawca POWINIEN zapewnić bezpieczeństwo informacji przesyłanej, przechowywanej i przetwarzanej w związku z realizacją zadań na rzecz ENEA Operator Sp. z o.o. zgodnie z wymaganiami określonymi w rozdz. 13 normy PN-EN ISO/IEC 27002:2017.

W szczególności Dostawca MUSI:

- a) Zapewnić ochronę poufności oraz integralności informacji przechowywanej przez Dostawcę oraz przesyłanej przez niego publicznymi kanałami transmisyjnymi, odpowiednio do jej klasy bezpieczeństwa,
- b) Zapewnić, że wszystkie osoby mające dostęp do informacji chronionych lub szczególnie chronionych podpisały klauzule poufności oraz posiadają wydane upoważnienie do przetwarzania danych osobowych.

7.4 Bezpieczeństwo powierzonych aktywów

Dostawca POWINIEN zapewnić właściwe użycie aktywów, powierzonych przez ENEA Operator Sp. z o.o., wykorzystywanych w pracach na rzecz Spółki, zgodnie z najlepszymi praktykami określonymi w rozdz. 8.1.3 i 8.1.4 normy PN-EN ISO/IEC 27002:2017.

W szczególności WYMAGANYM jest aby:

- a) Użytkownicy tych aktywów posiadali wiedzę i umiejętności odnośnie bezpiecznego korzystania z udostępnionych aktywów.

- b) Po zakończeniu realizacji zleconych zadań użytkownicy zwrócili aktywa lub, w przypadku gdy są to dane, usunęli je w skuteczny sposób.

7.5 Bezpieczeństwo personelu

Dostawca POWINIEN zapewnić bezpieczeństwo wykorzystywanego personelu zgodnie z najlepszymi praktykami określonymi w rozdz. 7.2.1, 7.2.2 oraz 7.3.1 normy PN-EN ISO/IEC 27002:2017, adekwatnie do zadań realizowanych na rzecz ENEA Operator Sp. z o.o.

W szczególności Dostawca MUSI posiadać i realizować udokumentowane polityki dotyczące jego personelu, które obejmują:

- a) przekazanie swojemu personelowi, realizującemu zadania na rzecz Spółki, informacji o wymaganiach bezpieczeństwa dotyczących współpracy z ENEA Operator Sp. z o.o.,
- b) zapewnienie, poprzez adekwatne szkolenia, odpowiedniego poziomu wiedzy o wymaganiach bezpieczeństwa oraz sposobach ich realizacji,
- c) podpisanie przez pracowników realizujących zadania na rzecz Spółki oświadczeń o zapoznaniu się z wymaganiami bezpieczeństwa i odpowiednimi politykami ich realizacji; podpisane oświadczenie winno także zawierać klauzulę o zachowaniu poufności pozyskanych informacji.

7.6 Bezpieczeństwo fizyczne i środowiskowe, w tym kontrola dostępu

Dostawca POWINIEN zapewnić bezpieczeństwo informacji i środowisk przetwarzania informacji, zgodnie z najlepszymi praktykami określonymi w rozdz. 9 oraz 11 normy PN-EN ISO/IEC 27002:2017.

W szczególności Dostawca MUSI:

- a) posiadać zabezpieczenia środowiska, w którym realizowane jest zlecenie na rzecz ENEA Operator Sp. z o.o. adekwatne do oceny poziomu ryzyka związanego z wykorzystaniem przetwarzanych informacji,
- b) zapewnić bezpieczeństwo fizyczne obszaru, w którym przetwarzane są informacje udostępniane przez lub dotyczące ENEA Operator Sp. z o.o.,
- c) zapewnić bezpieczeństwo danych udostępnionych przez lub dotyczących ENEA Operator Sp. z o.o. w przypadku wnoszenia zasobów poza obszar chroniony,
- d) zapewnić minimalizację ryzyk związanych z nieuprawnionym dostępem, poprzez co najmniej:
 - określenie zasad kontroli dostępu do pomieszczeń w których przetwarzane są informacje na rzecz ENEA Operator Sp. z o.o.,
 - ustanowienie i stosowanie zasad dostępu pracowników do systemów i aplikacji, w których przetwarzane są informacje na rzecz ENEA Operator Sp. z o.o., a także zasad ich odbierania i dostosowywania,
 - wdrożenie i stosowanie procedury bezpiecznego logowania do systemów i aplikacji.

7.7 Bezpieczeństwo urządzeń mobilnych

Dostawca POWINIEN zapewnić bezpieczeństwo wykonywania na rzecz ENEA Operator Sp. z o.o. pracy zdalnej oraz wykorzystywanych urządzeń mobilnych zgodnie z najlepszymi praktykami określonymi w rozdz. 6.2.1 normy PN-EN ISO/IEC 27002:2017.

W szczególności Dostawca MUSI posiadać i realizować udokumentowaną politykę korzystania z urządzeń mobilnych, która zapewnia:

- a) ochronę fizyczną urządzeń przenośnych (komórki/tablety/notebooki),
- b) nadzór nad oprogramowaniem instalowanym na urządzeniach mobilnych,
- c) zarządzanie uprawnieniami dostępu do urządzeń mobilnych,
- d) ochronę urządzeń mobilnych przed szkodliwym oprogramowaniem,
- e) zarządzanie technikami kryptograficznymi, które zapewnią bezpieczeństwo przechowywanych danych,

- f) ograniczenia w połączeniach do usług informacyjnych i tym samym minimalizacja pobierania oraz gromadzenia informacji na urządzeniach mobilnych,
- g) bezpieczną realizację kopii bezpieczeństwa,
- h) zabezpieczenie przed ingerencją zewnętrzną, np. firewall lokalny,
- i) bezpieczeństwo zdalnego zarządzania urządzeniami.

7.8 Bezpieczeństwo łańcucha dostaw

Dostawca MUSI zidentyfikować i udokumentować łańcuch dostaw związany z realizacją projektu. Dostawca MUSI zapewnić, że jego poddostawcy zapewniają co najmniej taki sam poziom bezpieczeństwa jaki spełnia on sam w odniesieniu do ENEA Operator Sp. z o.o. Dostawca odpowiada za zapewnienie bezpieczeństwa w całym łańcuchu dostaw produktów i usług, za który jest odpowiedzialny zgodnie z zawartą umową. Wytyczne do realizacji tego wymagania określają najlepsze praktyki zawarte w rozdz. 14.2.7 i 15.1.3 normy PN-EN ISO/IEC 27002:2017.

7.9 Bezpieczeństwo wymiennych nośników danych

Dostawca POWINIEN zapewnić bezpieczeństwo wymiennych nośników danych wykorzystywanych w związku z realizacją zadań na rzecz ENEA Operator Sp. z o.o. zgodnie z najlepszymi praktykami określonymi w rozdz. 8.3 normy PN-EN ISO/IEC 27002:2017.

W szczególności Dostawca MUSI:

- a) posiadać i realizować polityki dotyczące bezpiecznego usuwania danych z nośników zawierających dane związane z realizacją zadań na rzecz Spółki, zapewniając ich skuteczne usuwanie uniemożliwiające odzyskanie danych przez osoby nieuprawnione,
- b) posiadać i realizować polityki bezpiecznego przekazywania nośników zawierających dane związane z realizacją zadań na rzecz Spółki, zapewniając skuteczną ochronę tych danych.

7.10 Bezpieczeństwo pracy zdalnej

Dostawca POWINIEN zapewnić bezpieczeństwo zdalnej pracy na systemach Grupy ENEA, w szczególności systemach Spółki, zgodnie z najlepszymi praktykami określonymi w rozdz. 6.2.2 normy PN-EN ISO/IEC 27002:2017.

W szczególności:

- a) zdalny- dostęp do zasobów Zleceniodawcy MUSI być realizowany wyłącznie z wykorzystaniem zasobów i informacji udostępnionych przez Zleceniodawcę,
- b) zdalny dostęp do zasobów Zleceniodawcy MUSI być wykorzystywany tylko w celach i zakresie określonym przez Zleceniodawcę,
- c) nadawany zdalny dostęp jest imienny i udzielany każdemu pracownikowi Dostawcy indywidualnie,
- d) osoby korzystające ze zdalnego dostępu są ZOBOWIĄZANE do zapewnienia ochrony fizycznej zasobów oraz zachowania poufności informacji niezbędnych do korzystania ze zdalnego dostępu,
- e) osoby korzystające z zasobów oraz informacji niezbędnych do korzystania ze zdalnego dostępu NIE MOGĄ ich udostępniać ani ujawniać innym osobom,
- f) wykorzystanie zdalnego dostępu MUSI być realizowane w warunkach, które będą zabezpieczały przed ujawnieniem informacji związanych z realizowanym zleceniem oraz zabezpieczały przed dostępem zdalnym osób nieuprawnionych,
- g) ZABRONIONE jest wykorzystywanie podatności zidentyfikowanych w mechanizmach zdalnego dostępu Spółki,
- h) wszelkie wykryte podatności MUSZĄ być niezwłocznie zgłoszone do Zleceniodawcy, dalsze korzystanie ze zdalnego dostępu po zidentyfikowaniu podatności winno być realizowane wyłącznie po wyrażeniu zgody przez Zleceniodawcę,
- i) osoby korzystające ze zdalnego dostępu MUSZĄ zapewnić, że komputer lub urządzenie mobilne nie jest jednocześnie podłączony do innej sieci komputerowej, ewentualnie za wyjątkiem sieci komputerowej Dostawcy,
- j) osoby korzystające ze zdalnego dostępu MUSZĄ zapewnić, że używany dla jego realizacji komputer jest odpowiednio zabezpieczony przed złośliwym oprogramowaniem,

- w szczególności dla systemów marki Microsoft posiada aktualne oprogramowanie antywirusowe,
- k) zleciodawca ma prawo do nagrywania, przechowywania i wykorzystania w celach dowodowych nagrań oraz zapisów wszelkich zdarzeń dotyczących sesji zdalnego dostępu realizowanych przez Dostawcę.

8 BEZPIECZEŃSTWO PROCESU PROJEKTOWEGO DOSTAWCY

8.1 Bezpieczeństwo projektu

Dostawca POWINIEN wykorzystywać w procesach projektowych, realizowanych na rzecz ENEA Operator Sp. z o.o., najlepsze praktyki określone w rozdz. 14.2.1, 14.2.2, 14.2.5 normy PN-EN ISO/IEC 27002:2017.

W szczególności Dostawca MUSI:

- a) zapewnić istnienie i realizację udokumentowanych punktów kontrolnych z realizowanych na rzecz ENEA Operator Sp. z o.o. wymagań bezpieczeństwa,
- b) zapewnić kontrolę wersji wytwarzanego kodu oraz dokumentacji,
- c) zapewnić spełnienie udokumentowanych standardów programowania, przekazanych w ramach realizacji prac,
- d) zapewnić realizację udokumentowanych procedur zarządzania zmianami w wytwarzanych aplikacjach, systemach.

8.2 Ochrona dokumentacji projektowej i eksploatacyjnej

Dostawca POWINIEN zapewnić ochronę dokumentacji projektowej oraz eksploatacyjnej, tworzonej i przetwarzanej na rzecz ENEA Operator Sp. z o.o., zgodnie z najlepszymi praktykami określonymi w rozdz. 8.1.3 oraz 8.2.3 normy PN-EN ISO/IEC 27002:2017.

W szczególności:

- a) dokumentacja może być udostępniona wyłącznie osobom mającym upoważnienie do dostępu do takiej informacji w oparciu o umowę z ENEA Operator Sp. z o.o.,
- b) dostawca jest ZOBOWIĄZANY do oznaczania dokumentacji projektowej klasą bezpieczeństwa według klasyfikacji Grupy ENEA,
- c) dokumentacja MUSI być przechowywana w repozytorium zapewniającym ochronę poufności oraz integralności przechowywanej dokumentacji,
- d) dostawca MUSI rejestrować zdarzenia związane z dostępem do bezpiecznego repozytorium i przechowywać bezpiecznie zapisy nie krócej niż 3 lata.

8.3 Incydynty bezpieczeństwa

Dostawca MUSI zapewnić identyfikowanie i obsługę incydentów bezpieczeństwa we własnych systemach informatycznych i produkcyjnych, zgodnie z najlepszymi praktykami określonymi w rozdz. 16.1 normy PN-EN ISO/IEC 27002:2017.

W szczególności Dostawca MUSI:

- a) zgłaszać w formie pisemnej i elektronicznej do ENEA Operator Sp. z o.o. wszelkie incydynty bezpieczeństwa, które mają jakikolwiek związek z zadaniami realizowanymi na rzecz Spółki lub z produktami wytwarzanymi na rzecz ENEA Operator Sp. z o.o.,
- b) w przypadku zaistnienia incydentu bezpieczeństwa w jego systemach, podjąć wszelkie niezbędne środki, aby zminimalizować wpływ incydentu na działanie Spółki i jej systemy informatyczne i systemy automatyki,

- c) posiadać odpowiednie procedury umożliwiające gromadzenie wszelkich dowodów związanych z zaistnieniem incydentu bezpieczeństwa, zgodnie z najlepszymi praktykami określonymi w rozdz. 16.1.7 normy PN-EN ISO/IEC 27002:2017.

8.4 Incydenty Bezpieczeństwa związane z dostarczaniem produktami lub usługami

W przypadku zaistnienia incydentu bezpieczeństwa w systemach informacyjnych Spółki, Dostawca zapewnia wsparcie Spółce w zakresie bezpieczeństwa dostarczanych produktów i usług, w szczególności w zakresie:

- a) weryfikacji oryginalności oprogramowania,
- b) przywróceniu oryginalnego oprogramowania,
- c) przywrócenia poprawnej konfiguracji baz danych, aplikacji i systemów,
- d) weryfikacji poprawności wniosków z analizy funkcjonalności zidentyfikowanego przez służby EOP złośliwego oprogramowania w zakresie jego potencjalnego wpływu na dostarczane produkty/usługi,
- e) wsparcia innych działań ENEA Operator Sp. z o.o. w trakcie obsługi Incydentu poważnego.

9 BEZPIECZEŃSTWO BUDOWY ŚRODOWISK ROZWOJOWYCH I TESTOWYCH

9.1 Bezpieczne środowisko rozwojowe

Dostawca POWINIEN realizować prace rozwojowe z wykorzystaniem bezpiecznego środowiska rozwojowego, dla którego najlepsze praktyki określono w rozdz. 14.2.6 normy PN-EN ISO/IEC 27002:2017.

W szczególności Dostawca MUSI zapewnić:

- a) zabezpieczenia środowiska rozwojowego i testowego adekwatne do poziomu ryzyka związanego z wykorzystaniem danych o określonym poziomie ochrony,
- b) kontrolę przepływu danych od i do środowiska rozwojowego i testowego, zapewniając brak wpływu danych testowych oraz brak nieuprawnionego dostępu do systemów.

9.2 Bezpieczeństwo środowisk rozwojowych i testowych

Dostawca POWINIEN zapewnić bezpieczeństwo fizyczne środowisk rozwojowych i testowych zgodnie z najlepszymi praktykami określonymi w rozdz. 11.1 i 11.2 normy PN-EN ISO/IEC 27002:2017.

W szczególności Dostawca MUSI:

- a) zapewnić bezpieczeństwo fizyczne obszaru, w którym znajdują się środowiska rozwojowe i testowe,
- b) zapewnić ochronę fizyczną środowisk rozwojowych i testowych,
- c) zapewnić minimalizację ryzyk dotyczących środowisk rozwojowych i testowych związanych z nieuprawnionym dostępem i modyfikacją danych, w szczególności kodu binarnego oraz źródłowego oprogramowania,
- d) zapewnić bezpieczeństwo danych udostępnionych przez ENEA Operator Sp. z o.o. lub dotyczących Spółki w przypadku wynoszenia zasobów poza obszar chroniony.

9.3 Zarządzanie uprawnieniami środowisk rozwojowych i testowych

Dostawca POWINIEN zarządzać uprawnieniami dostępu do środowisk rozwojowych i testowych zgodnie z najlepszymi praktykami określonymi w rozdz. 9.2, 9.3, 9.4 normy PN-EN ISO/IEC 27002:2017.

W szczególności dostawca MUSI spełniać następujące wymagania:

- a) przyznawanie uprawnień dostępu do systemów rozwojowych i testowych MUSI być dokumentowane i kontrolowane,

- b) przyznawanie uprawnień do systemów rozwojowych i testowych MUSI być oparte o zasadę minimum koniecznego,
- c) procedura i mechanizmy przyznawania uprawnień MUSZĄ zapewnić, że dostęp do danych chronionych i szczególnie chronionych uzyskają tylko te osoby, które są do tego upoważnione,
- d) zapewnić możliwość rozliczalności użytkowników z przyznanych uprawnień,
- e) uprawnienia niewykorzystywane MUSZĄ być niezwłocznie odbierane,
- f) przyznane uprawnienia dostępu MUSZĄ podlegać kontroli nie rzadziej niż co 6 miesięcy, zaś wyniki przeglądów MUSZĄ być udokumentowane i przechowywane w bezpieczny sposób nie krócej niż 3 lata,

9.4 Separacja środowisk rozwojowych i testowych

Dostawca POWINIEN zapewnić (co najmniej na poziomie maszyny wirtualnej lub fizycznej) odseparowanie środowisk rozwojowych i testowych przeznaczonych do realizacji zadań na rzecz ENEA Operator Sp. z o.o. od środowisk realizujących zadania dla innych klientów, zgodnie z najlepszymi praktykami określonymi w rozdz. 12.1.4 normy PN-EN ISO/IEC 27002:2017.

9.5 Rejestracja zdarzeń

Dostawca MUSI zapewnić rejestrowanie zdarzeń związanych z dostępem użytkowników oraz administratorów do systemów rozwojowych i testowych oraz zapewnić ich bezpieczne przechowywanie przez okres nie krótszy niż 3 lata.

Dostawca MUSI udostępnić, przechowywane rejestry związane ze świadczeniem usług dla Spółki, na życzenie Spółki. Najlepsze praktyki w tym zakresie są określone w rozdz. 12.4 normy PN-EN ISO/IEC 27002:2017.

9.6 Ochrona kopii bezpieczeństwa

Dostawca POWINIEN zapewnić ochronę kopii zapasowych informacji przetwarzanej w trakcie realizacji zadań na rzecz ENEA Operator Sp. z o.o., zgodnie z najlepszymi praktykami określonymi w rozdz. 12.3 normy PN-EN ISO/IEC 27002:2017.

W szczególności Dostawca MUSI zapewnić fizyczne zabezpieczenie kopii bezpieczeństwa, a także gdy jest to właściwe dla wymaganego poziomu ochrony informacji, szyfrowanie kopii bezpieczeństwa.

9.7 Ochrona danych testowych

Dostawca MUSI zapewnić:

- a) bezpieczeństwo danych testowych adekwatnie do rodzaju danych oraz klasy poufności tych danych, zgodnie z klasyfikacją informacji GK Enea,
- b) aby dostęp do danych testowych posiadały tylko osoby upoważnione,
- c) rejestrowanie wykorzystania danych testowych, z oznaczeniem co najmniej osób które miały dostęp do danych, w jakim okresie i w jakim celu, oraz na czyje zlecenie,
- d) przechowywanie rejestru wykorzystania danych przez okres co najmniej 3 lat.

9.8 Bezpieczeństwo kodów źródłowych

Wszelkie kody źródłowe oprogramowania muszą być przechowywane przez Dostawcę w bezpiecznym repozytorium kodów źródłowych, zgodnie z wymaganiami określonymi w rozdz. 9.4.5 normy PN-EN ISO/IEC 27002:2017.

Dostawca ma obowiązek zapewnić, że dostęp do repozytorium kodów źródłowych umożliwiający ich modyfikację będzie kontrolowany, zaś korzystać z repozytorium z możliwością modyfikacji jego zawartości będą wyłącznie osoby upoważnione. Dostęp do repozytorium musi być rejestrowany, zaś rejestry przechowywane nie krócej niż 3 lata od daty zdarzenia. W trakcie transferu kodów źródłowych Dostawca MUSI zapewnić ich integralność, poufność oraz autentyczność, zgodnie z wymaganiami określonymi w rozdz. 13.2.2 normy PN-EN ISO/IEC 27002:2017.

Dostawca ma obowiązek zapewnić, że wytworzone przez niego oprogramowanie spełnia co najmniej wymagania standardu Application Security Verification Standard dla poziomu 2², chyba że w umowie wskazano inny poziom.

9.9 Korzystanie z usług w chmurze

Dostawca korzystając z technologii przetwarzania danych w chmurze MUSI:

- a) Posiadać plan awaryjnego dostępu do chmury oraz plan awaryjnego wyjścia z chmury,
- b) Dane dotyczące usługi kluczowej Spółki mogą być przechowywane w zasobach chmurowych wyłącznie w postaci zaszyfrowanej. Klucze szyfrujące i deszyfrujące nie mogą znajdować się w zasobach chmurowych na żadnym etapie szyfrowania.

Dostawca korzystając z usług w chmurze do realizacji zadań oraz budowy systemów na potrzeby ENEA Operator Sp. z o.o. jest ZOBOWIĄZANY do zawarcia formalnej umowy prawnej z dostawcą tych usług.

Dostawca jest zobowiązany do zapewnienia bezpieczeństwa w korzystaniu z usług w chmurze na co najmniej takim samym poziomie, jak jest zobowiązany wobec ENEA Operator Sp. z o.o.,

Dostawca jest zobowiązany do powiadomienia ENEA Operator Sp. z o.o. o wszelkich incydentach bezpieczeństwa związanych z korzystaniem z usług w chmurze.

10 AUDYTY BEZPIECZEŃSTWA DOSTAWCÓW

10.1 Prawo do audytu

Dostawca MUSI zapewnić przedstawicielom Spółki możliwość przeprowadzenia audytu bezpieczeństwa w zakresie własnych środowisk rozwojowych i testowych wykorzystywanych do współpracy z ENEA Operator Sp. z o.o., a także analogicznych środowisk własnych poddostawców.

ENEA Operator Sp. z o.o. może odstąpić od audytu w przypadku przedstawienia ważnego Certyfikatu dla Systemu Zarządzania wg. PN-EN ISO/IEC 27001:2017 wydanego przez akredytowaną jednostkę certyfikującą.

10.2 Zakres audytu

Zakres audytu bezpieczeństwa POWINIEN być adekwatny do projektu, którego dotyczy.

10.3 Termin audytu

Termin audytu POWINIEN być uzgodniony z Dostawcą minimum na 3 dni robocze przed planowanym audytem.

10.4 Wyniki audytu

Wyniki audytu WINNY być omówione z przedstawicielami Dostawcy, a w przypadku zidentyfikowania niezgodności, z przeglądu MUSI zostać sporządzony udokumentowany plan działania.

10.5 Ochrona informacji audytowej

Wyniki audytu są klasyfikowane jako informacja o klasie C.

2 ASVS Poziom 1 jest przeznaczony dla wszystkich programów.

ASVS Poziom 2 jest przeznaczony dla aplikacji, które zawierają dane wymagające ochrony.

ASVS Poziom 3 jest przeznaczony dla najbardziej krytycznych aplikacji - takich, które wykonują transakcje znacznej wartości, zawierają wrażliwe dane medyczne, a także innych aplikacji, które wymagają najwyższego poziomu zaufania.

11 ZAKOŃCZENIE WSPÓŁPRACY

11.1 Zwrot aktywów

Dostawca JEST ZOBOWIĄZANY do zwrotu wszystkich aktywów powierzonych mu przez Spółkę.

11.2 Ochrona informacji

Dostawca JEST ZOBOWIĄZANY do zapewnienia bezpieczeństwa wszystkich informacji chronionych w czasie określonym przez umowę, a także po zakończeniu współpracy.

11.3 Niszczenie powierzonych aktywów

Dostawca JEST ZOBOWIĄZANY do skutecznego zniszczenia informacji, które winny zostać zniszczone po zakończeniu umowy, oraz do przedstawienia protokołu przeprowadzenia zniszczenia tych informacji.