

### ZAŁĄCZNIK NR 3 DO OPZ - WYMAGANIA W ZAKRESIE BEZPIECZEŃSTWA SYSTEMU

1. Wymagania dotyczące cyberbezpieczeństwa muszą być uwzględnione we wszystkich modułach i usługach Systemu, a funkcje związane z bezpieczeństwem, muszą być zarządzalne, w ramach wszystkich komponentów składowych Systemu.
2. Wykonawca dostarczy dokumentację opisującą wszystkie wdrożone fizyczne, proceduralne i inne środki bezpieczeństwa, które mają na celu ochronę:
  - 1) poufności i integralności danych w dostarczonym Systemie, oraz
  - 2) niezawodność dostarczonego Systemu.
3. Wykonawca dostarczy dokumentację do oprogramowania Systemu. W przypadku produktów dostarczanych przez strony trzecie, należy dostarczyć oryginalną dokumentację OEM, a także dokument opisujący wszelkie zmiany oraz ich konfiguracje (jeśli dotyczy). Dodatkowo, wymagana jest dokumentacja w odniesieniu do:
  - 1) skryptów i/lub makr (opis źródła z komentarzem),
  - 2) plików konfiguracyjnych czasu wykonywania i składni wymaganej przez interpretery (jeśli istnieją),
  - 3) baz danych i tabel oraz wszelkiego innego dołączonego oprogramowania (identyfikacja wersji, rewizji i/lub poziomów poprawek, zgodnie z dostawą).

Lista powinna zawierać wszystkie porty i autoryzowane usługi aktywne w Systemie lub te, które mogą być aktywowane wyłącznie poprzez konfigurację.
4. Wykonawca musi posiadać System Zarządzania Bezpieczeństwem Informacji SZBI, w celu ochrony wszelkich informacji i tworzonych systemów.

SZBI Wykonawcy musi posiadać certyfikat ISO/IEC 27001, a zakres certyfikacji musi obejmować rozwój i wsparcie aplikacji przemysłowych i powiązanego oprogramowania.
5. W kwestiach technicznych związanych z bezpieczeństwem, Wykonawca będzie komunikować się z jednym wskazanym punktem kontaktowym Zamawiającego (dane kontaktowe zostaną wskazane przez Zamawiającego).
6. Wykonawca zutylizuje wszelki sprzęt, dokumentację lub inne materiały wymienione podczas rozwoju lub konserwacji Systemu w taki sposób, aby chronić wrażliwe informacje. Wykonawca przedstawi procedurę bezpiecznej utylizacji.
  - 1) Nośniki, takie jak dokumenty papierowe oraz nośniki magnetyczne, elektroniczne i optyczne zawierające lub potencjalnie zawierające informacje sklasyfikowane przez Zamawiającego jako wrażliwe, zostaną zniszczone przez Wykonawcę, gdy nie będą już potrzebne, a najpóźniej na koniec projektu (tj. nie później niż przed upływem terminu Odbioru Końcowego wdrożenia Systemu) – z wyłączeniem dokumentacji niezbędnej do realizacji gwarancji i usług serwisowych.
  - 2) Dokumenty papierowe powinny być zniszczone przy użyciu niszczarki typu crosscut (lub równoważnej). Nośniki magnetyczne mogą być ponownie użyte, ale przed ponownym użyciem muszą zostać wyczyszczone w taki sposób, aby odzyskanie lub odtworzenie danych było niemożliwe.
  - 3) Dyski DVD i CD-ROM muszą zostać fizycznie zniszczone, aby nie było możliwości odzyskania z nich danych.
  - 4) Wykonawca przekaże Zamawiającemu dokumentację zniszczenia, bezpiecznego usunięcia lub zabezpieczenia nośników informacji przed przystąpieniem do procedury Odbioru Końcowego wdrożenia Systemu.

7. Wykonawca dostarczy dokumentację Systemu obejmującą funkcje bezpieczeństwa oraz instrukcje dotyczące konserwacji produktu, wsparcia i rekonfiguracji ustawień domyślnych.  
Dokumentacja powinna obejmować co najmniej:
- 1) hardening: w przypadku produktów stron trzecich należy dostarczyć przewodniki hardeningu oprogramowania OEM wraz z oświadczeniem, które ze środków zostały wdrożone.
  - 2) podręcznik administratora w języku polskim, obejmujący co najmniej:
    - zarządzanie kontami użytkowników,
    - zasady dotyczące haseł,
    - włączanie środków uwierzytelniania,
    - konfigurowanie środków kryptograficznych,
    - konfigurowanie zarządzania kluczami,
    - konfigurowanie kopii zapasowych oraz ich testowanie,
    - instalowanie ochrony punktów końcowych na stanowiskach operatorskich,
    - konfigurowanie monitoringu wydajności,
    - konfigurowanie rejestrowania zabezpieczeń.
8. Na etapie opracowania Projektu Technicznego Systemu, Wykonawca skonsultuje z Zamawiającym, zasady konfigurowania zabezpieczeń i ustawień dotyczących bezpieczeństwa Systemu, zgodnie z politykami bezpieczeństwa i procedurami obowiązującymi u Zamawiającego.
9. Wykonawca przeprowadzi niezależny audyt bezpieczeństwa Systemu w fazie testów akceptacyjnych w miejscu instalacji. Zakłada się, że audyt bezpieczeństwa będzie obejmował co najmniej:
- 1) sprawdzenie zgodności z wymaganiami przedstawionymi w niniejszym dokumencie,
  - 2) skanowanie podatności i testy penetracyjne zainstalowanego Systemu.
- Wykonawca przedstawi Zamawiającemu proces przeprowadzania skanowania, biorąc pod uwagę specyfikę i ograniczenie potencjalnego wpływu skanowania na normalną pracę całego Systemu, przy jednoczesnym zapewnieniu wymaganej funkcji celu skanowania.
10. Wykonawca zapewni Zamawiającemu niezbędne wsparcie w przeprowadzaniu audytów i testów bezpieczeństwa w okresie po zakończeniu wdrożenia tj. po dokonaniu Odbioru końcowego - w czasie trwania gwarancji i umowy serwisowej Systemu.
11. W przypadku stwierdzenia zagrożeń bezpieczeństwa w ramach przeprowadzonych audytów bezpieczeństwa, Wykonawca będzie zobowiązany do ich usunięcia lub obniżenia ryzyka do uzgodnionego poziomu.
12. W trakcie wdrożenia Systemu, Wykonawca wyeliminuje zagrożenia bezpieczeństwa stwierdzone w wyniku audytu cyberbezpieczeństwa przed dokonaniem Odbioru Końcowego i przekazaniem Systemu do eksploatacji. Ewentualne odstępstwa lub wyjątki muszą być wyraźnie zaakceptowane i zatwierdzone przez Zamawiającego. W przypadku zagrożeń o mniejszym wpływie, przed przekazaniem do eksploatacji Systemu, Zamawiający i Wykonawca uzgodnią plan postępowania w odniesieniu do ewentualnych zagrożeń.
13. Wykonawca udokumentuje wszystkie procesy lub programy (ang. "daemon"), które muszą być aktywne dla prawidłowego działania Systemu.
14. System musi zapewniać konfigurowalność wymagań dotyczących haseł dla lokalnych kont użytkowników, umożliwiającą ustawienie, co najmniej następujących parametrów:
- 1) zmiana hasła na żądanie dla pojedynczego użytkownika (w tym wymagana zmiana hasła domyślnego/początkowego),



NARODOWY FUNDUSZ  
OCHRONY ŚRODOWISKA  
I GOSPODARKI WODNEJ

„Kwalifikowane z całego systemu środki ograniczające do emisji (Fundacja Modernizacji)”



- 2) długość hasła,
  - 3) częstotliwość regularnej zmiany hasła,
  - 4) złożoność hasła,
  - 5) liczba nieudanych logowań przed zablokowaniem konta,
  - 6) metoda odblokowania zablokowanego konta,
  - 7) porównanie z biblioteką zabronionych ciągów znaków, dostarczona przez Wykonawcę z możliwością edycji przez Zamawiającego,
  - 8) pochodne użycie nazwy użytkownika,
  - 9) odmowa wielokrotnego lub ponownego użycia tego samego hasła.
15. Konta usług służące do integracji z systemami zewnętrznymi muszą używać unikatowych haseł.  
Konta serwisowe używane w sytuacjach awaryjnych, muszą używać co najmniej unikalnych haseł dla każdego zakresu, takiego jak stacje w tej samej strefie z tą samą funkcją (np. dwa serwery Systemu z tą samą funkcją lub grupa przełączników w tej samej strefie mogą mieć to samo hasło). Wykonawca może korzystać z narzędzi Privileged Access Management w celu zapewnienia unikalnych haseł dla wszystkich kont wymaganych usług.
16. System musi wymuszać kontrolę dostępu opartą na rolach dla wszystkich użytkowników:
- 1) użytkownicy logują się za pomocą indywidualnych kont,
  - 2) centralny serwer kontroli dostępu określa ich rolę,
  - 3) punkt końcowy, do którego uzyskano dostęp, egzekwuje prawa dostępu tej roli.
- System rozdziela różne role, tak aby każda rola mogła otrzymać tylko uprawnienia potrzebne do uzyskania wymaganego dostępu.  
Administratorzy Systemu, muszą mieć możliwość zarządzania kontami i rolami.
17. Interfejs zarządzania dostępem do Systemu musi spełniać następujące wymagania:
- 1) dla każdej roli musi zapewniać możliwość skonfigurowania dozwolonych działań,
  - 2) musi zapewniać użytkownikowi o odpowiednich uprawnieniach możliwość definiowania nowych lub usuwania ról,
  - 3) musi zapewniać użytkownikowi o odpowiednich uprawnieniach możliwość przyznawania uprawnień do ról,
  - 4) musi zapewniać użytkownikowi o odpowiednich uprawnieniach możliwość wskazania, które prawa są przyznawane poszczególnym rolom i którzy użytkownicy mają przyznane określone role (np. macierz autoryzacji).
18. W celu ograniczenia wpływu zagrożeń, takich jak błąd użytkownika, naruszenie bezpieczeństwa konta i złośliwe działania wewnętrzne, następujące role powinny być od siebie oddzielone:
- 1) administratorzy bazy danych,
  - 2) administratorzy sieci,
  - 3) administratorzy bezpieczeństwa,
  - 4) administratorzy Systemu,
  - 5) zaawansowani użytkownicy Systemu,
  - 6) użytkownicy Systemu.
19. System musi wykorzystywać standardowe protokoły uwierzytelniania, przy czym wymagana jest obsługa co najmniej protokołu LDAP.
20. Niedopuszczalne jest przechowywanie w Systemie danych uwierzytelniających jak np. haseł w postaci niezaszyfrowanej.



21. Dopuszczalne są wyłącznie protokoły szyfrujące i bezpiecznie przesyłające dane logowania (np. Secure Shell [SSH]) lub szyfrujące komunikację (np. za pomocą Transport Layer Security [TLS]).
22. Jeśli uwierzytelnianie nie powiedzie się, System nie będzie przekazywać żadnych informacji zwrotnych o tym, czy konto istnieje, czy nie, lub że podano nieprawidłowe hasło.
23. Wykonawca przekaże Zamawiającemu ewentualne istnienie wszystkich znanych metod obejścia udokumentowanych kontroli uwierzytelniania lub autoryzacji we wszystkich warstwach Systemu, które zostały utworzone podczas procesu konfiguracji.  
Wykonawca zapewni usunięcie z Systemu wszystkich takich istniejących obejść przed przystąpieniem do Odbioru końcowego.
24. Wykonawca skonfiguruje każdy komponent Systemu tak, aby działał zgodnie z zasadą najniższych uprawnień. Obejmuje to uprawnienia systemu operacyjnego, dostępu do plików, uprawnienia kont użytkowników, komunikację między aplikacjami oraz dostęp do usług Systemu.
25. Działania uprzywilejowane powinny być wykonywane za pośrednictwem spersonalizowanych kont administracyjnych lub przy użyciu narzędzi dostępu uprzywilejowanego, w celu zapewnienia identyfikowalności operacji uprzywilejowanych. Konta ogólne uprzywilejowane lub awaryjne nie powinny być używane w scenariuszach innych niż awaryjne.
26. Wykonawca przekaże dane uwierzytelniające kont, które są niezbędne do inicjalizacji Systemu przy użyciu bezpiecznych metod.  
Obejmuje to konta użytkowników, konta uprzywilejowane i konta awaryjne.  
Wykonawca skonfiguruje System tak, aby wymagał zmiany hasła po pierwszym użyciu dostarczonych danych uwierzytelniających inicjalizacji lub, jeśli nie jest to możliwe, Wykonawca opracuje wytyczne dotyczące resetowania wszystkich fabrycznie ustawionych danych uwierzytelniających danego konta.
27. Jeśli System używa certyfikatów do uwierzytelniania użytkownika, należy zastosować walidację certyfikatu. Obejmuje to weryfikację tożsamości użytkownika, okresu ważności certyfikatu, podpisu, pełnego łańcucha certyfikatów i statusu odwołania.
28. W ramach opieki serwisowej Wykonawca wykonana zmianę wersji protokołu szyfrowania i zestawów szyfrów, jeśli jest to wymagane ze względu na zidentyfikowane luki w zabezpieczeniach lub z uwagi na zakończenie okresu wsparcia.
29. W przypadku, gdy System składa się z rozproszonych modułów / komponentów składowych, w których różne składniki komunikują się ze sobą, komunikacja między różnymi komponentami składowymi Systemu musi być zabezpieczona (zapewniać ochronę poufności i integralności). Do zabezpieczenia komunikacji wymagane są bezpieczne protokoły. Użycie niezabezpieczonych protokołów np. z uwagi na wymaganą wydajność, musi zostać zatwierdzone przez Zamawiającego.
30. Wykonawca stosuje istniejące i ogólnie przyjęte najlepsze praktyki i wytyczne w zakresie hardeningu systemów operacyjnych, systemów zarządzania bazami danych i aplikacji.
31. Wykonawca usunie wszystkie komponenty oprogramowania, które nie są wymagane do obsługi i/lub konserwacji Systemu.



Jeśli usunięcie nie jest technicznie wykonalne, Wykonawca wyłączy oprogramowanie, które nie jest wymagane do obsługi i/lub konserwacji Systemu. Wykonawca usunie lub wyłączy co najmniej następujące oprogramowanie z systemu produkcyjnego, w tym serwerów i stacji roboczych:

- 1) gry,
- 2) sterowniki urządzeń dla komponentów produktu, które nie zostały zamówione lub dostarczone,
- 3) usługi przesyłania wiadomości (np. poczta elektroniczna, komunikatory internetowe, udostępnianie plików peer-to-peer),
- 4) kod źródłowy,
- 5) kompilatory oprogramowania na stacjach roboczych użytkowników i serwerach,
- 6) kompilatory oprogramowania dla języków programowania, które nie są używane w produkcji,
- 7) nieużywane protokoły sieciowe i komunikacyjne,
- 8) nieużywane narzędzia administracyjne, diagnostyka, zarządzanie siecią i funkcje zarządzania Systemem,
- 9) kopie zapasowe plików, baz danych i programów używanych wyłącznie w trakcie wdrożenia Systemu,
- 10) wszystkie nieużywane dane i pliki konfiguracyjne.

Jeśli oprogramowanie, które nie jest wymagane, nie może zostać usunięte lub wyłączone, Wykonawca udokumentuje konkretne przypadki i przedstawi zalecenia ograniczające ryzyko.

Wykonawca dostarczy dokumentację w której zostaną zawarte informacje o usuniętych lub wyłączonych składnikach.

32. Przed przekazaniem Systemu do eksploatacji, Wykonawca usunie lub wyłączy wszelkie konta użytkowników, które nie są potrzebne do normalnego działania Systemu lub jego konserwacji.
33. Wykonawca usunie lub wyłączy, za pomocą oprogramowania, fizycznego odłączenia lub barier technicznych, wszystkie usługi lub porty w Systemie, które nie są wymagane do normalnej pracy, operacji awaryjnych lub rozwiązywania problemów. Dotyczy to w szczególności:
  - 1) portów komunikacyjnych i fizyczne porty wejścia/wyjścia (np. porty dokujące USB, napędy CD/DVD, porty wideo i porty szeregowy),
  - 2) nieużywane porty Ethernet na zaporach sieciowych, przełącznikach i routerach,
  - 3) dostęp do sieci dla systemów składowych będzie dozwolony w oparciu o uwierzytelnianie portów 802.1X.Wykonawca dostarczy dokumentację wyłączonych portów, złączy i interfejsów, w tym opis metody zastosowanej w celu spełnienia tego wymogu.
34. Wykonawca skonfiguruje System, tak aby umożliwić Zamawiającemu ponowne włączenie wyłączonych portów i/lub usług. Zamawiający będzie konsultował z Wykonawcą możliwość włączenia wyłączonych portów.
35. Wykonawca zweryfikuje, czy nie zostały wprowadzone do Systemu nieautoryzowane urządzenia rejestrujące (np. rejestratory kluczy, kamery i mikrofony).
36. Pliki systemowe powinny być wyraźnie oddzielone od plików aplikacji i danych aplikacji. Dostęp do plików i danych powinien być zgodny z predefiniowanymi prawami dostępu (zarówno na poziomie systemu operacyjnego, jak i aplikacji).
37. Wykonawca zapewni schemat aktualizacji narzędzia ochrony przed złośliwym oprogramowaniem oraz aktualizacji definicji/sygnatur. Aktualizacje będą wykonywane bez bezpośrednich połączeń z zewnętrznymi serwerami, przy użyciu bezpiecznej architektury wykorzystującej serwery proxy lub pośrednie repozytorium.
38. Wykonawca przetestuje i potwierdzi kompatybilność poprawek i aktualizacji aplikacji do ochrony przed złośliwym oprogramowaniem i wykrywania włamań.



NARODOWY FUNDUSZ  
OCHRONY ŚRODOWISKA  
I GOSPODARKI WODNEJ

„Kwalifikowane z oryginalnego systemu funduszu opierającego się na projekcie Modernizacja”



39. Wykonawca zweryfikuje, czy usługi ochrony przed złośliwym oprogramowaniem oddziałujące na System nie kolidują z innymi usługami mającymi wpływ na prawidłowe działanie Systemu. Wykonawca przedstawi listę wyjątków, w tym plików, które nie są skanowane lub funkcji narzędzi ochrony przed złośliwym oprogramowaniem, które są wyłączone, wraz z uzasadnieniem dla każdego wyjątku.
40. Dzienniki zdarzeń bezpieczeństwa z narzędzia do ochrony przed złośliwym oprogramowaniem i wykrywania włamań opartego na hoście, muszą być gromadzone i przechowywane w centralnym repozytorium dzienników bezpieczeństwa.
41. System musi mieć możliwość korzystania z zapory opartej na hoście. Taka zaporę sieciową powinna być skonfigurowana w taki sposób, aby zezwalać wyłącznie na niezbędną i autoryzowaną komunikację do i z systemów/aplikacji. Wykonawca dostarczy szablon zestawu reguł zapory, który może być bezpośrednio wdrożony i modyfikowany przez Zamawiającego bez wsparcia Wykonawcy.
42. Wykonawca zapewni przy pomocy funkcji footprinting lub whitelistach, mechanizm okresowego skanowania integralności zawartości dysków Systemu w celu ustalenia, czy dokonano nieautoryzowanych modyfikacji. Takie modyfikacje mogą obejmować między innymi oprogramowanie, pliki konfiguracyjne, uprawnienia do plików, konta systemowe i konta użytkowników.
43. Narzędzia skanujące muszą być skonfigurowane zgodnie z planem skanowania uzgodnionym z Zamawiającym aby nie zakłócać wydajności i działania Systemu.
44. Wykonawca zapewni skonfigurowanie zabezpieczeń i rejestrowania ścieżki audytowej na wszystkich zasobach ICT Systemu.
45. System musi zapewnić ochronę zapisów dziennika zdarzeń i ustawienia konfiguracji ścieżki audytowej przed nieautoryzowanym dostępem, modyfikacją i usunięciem.
46. Wykonawca musi dostarczyć listę wszystkich funkcji rejestrowania zdarzeń obsługiwanych przez System oraz format tych dzienników. Lista ta musi określać, które z tych dzienników są domyślnie włączone.
47. Każdy z komponentów składowych Systemu powinien znajdować się w jednoznacznie zdefiniowanej strefie bezpieczeństwa.
- 1) Wszystkie systemy i urządzenia znajdujące się w obrębie danej strefy bezpieczeństwa, a także urządzenia, które definiują strefę bezpieczeństwa, należy traktować i konfigurować jako systemy krytyczne.
  - 2) Punktem dostępu do danej strefy musi być firewall.
  - 3) Wszystkie inne punkty dostępu, takie jak obsługa dostępu zdalnego, powinny być wyłączone lub zabezpieczone w taki sposób, aby ich włączenie wymagało wyraźnej manualnej interwencji.
  - 4) Instalacja lub korzystanie z sieci bezprzewodowych w komponentach składowych Systemu lub pomiędzy nimi jest zabronione.
48. Wykonawca dostarczy dokumentację przedstawiającą podział Systemu na strefy bezpieczeństwa, zawierającą wszystkie połączone elementy Systemu w danej strefie bezpieczeństwa, wszystkie punkty dostępu przez firewalle oraz wszystkie skonfigurowane do kontrolowania i monitorowania dostępu do określonych punktów dostępowych.
49. Wykonawca musi skonfigurować strukturalne strefy zdemilitaryzowane w taki sposób aby systemy w danej strefie DMZ były od siebie odizolowane. Atak cybernetyczny, który zakłóca lub narusza serwery lub urządzenia sieciowe składające się na jedną strefę zdemilitaryzowaną, nie może mieć wpływu na serwery lub urządzenia sieciowe



składające się na inną strefę zdemilitaryzowaną. Wykonawca zapewni wystarczającą redundancję sprzętu i separację architektoniczną, aby osiągnąć ten cel.

50. Wykonawca dostarczy informacje na temat całej komunikacji (np. protokołów) wymaganej między strefami bezpieczeństwa sieciowego, zarówno przychodzącej, jak i wychodzącej, oraz zidentyfikuje każdy komponent sieciowy Systemu inicjujący komunikację.
51. W przypadku uszkodzenia danego komponentu Systemu lub w przypadku gdy jego wydajność ulegnie pogorszeniu w wyniku incydentu cyberbezpieczeństwa, musi istnieć możliwość szybkiego odizolowania dotkniętego komponentu od reszty Systemu. W przypadku komponentu Systemu umieszczonego w strefie DMZ musi istnieć możliwość natychmiastowego zamknięcia połączenia i wyłączenia komponentu. W przypadku komponentu umieszczonego w strefie głównej musi istnieć możliwość wyłączenia tego komponentu i przeniesienia wszystkich jego usług na komponent redundantny umieszczony w innej lokalizacji.
52. Cała komunikacja pomiędzy Systemem z systemami trzecimi musi przechodzić przez strefę DMZ, gdy w komunikację są zaangażowane inne sieci lub domeny. Wyjątki od tej reguły wymagają wyraźnej zgody Zamawiającego.
53. Wykonawca zapewni ograniczanie ruchu sieciowego pomiędzy różnymi strefami bezpieczeństwa sieci, stosując co najmniej ograniczenia w warstwie 3 OSI. Wykonawca dostarczy dokumentację dotyczącą wszelkich metod lub urządzeń wykorzystywanych do ograniczania ruchu sieciowego. Wykonawca umieści i skonfiguruje serwery front-end Systemu w wyznaczonych i odpowiednich strefach zdemilitaryzowanych. Połączenia między serwerami aplikacji/baz danych, stacjami roboczymi i serwerami front-end obsługującymi proces będą ograniczone przez zaporę sieciową, która wymusza ograniczenia IP i protokołów.
54. W celu umożliwienia skutecznej aktualizacji składników Systemu, np. aktualizacji systemu operacyjnego, serwery te powinny znajdować się w oddzielnej strefie. Serwery Systemu nie mogą otrzymywać aktualizacji bezpośrednio z Internetu.
55. Wykonawca zweryfikuje i dostarczy dokumentację, wskazującą że interfejsy zarządzania konfiguracją sieci są zabezpieczone.
56. Wykonawca usunie lub wyłączy nieużywane funkcje konfiguracji i zarządzania siecią na urządzeniach sieciowych.
57. Wykonawca zapewni reguły zapory sieciowej dla ruchu przychodzącego i wychodzącego w oparciu o zestawy reguł odmowy. Regułom zapory sieciowej powinny towarzyszyć komentarze opisujące ich cel, datę utworzenia i twórcę.
58. Wykonawca zapewni metodę zarządzania komponentami sieciowymi Systemu i zmiany konfiguracji, w tym konfiguracji sprzętu i oprogramowania (np. schematów adresacji).
59. Wykonawca zapewni listy kontroli dostępu (ACL) do monitorowania komponentów sieciowych Systemu.
60. Wykonawca zainstaluje zapory sieciowe w segmentach sieci Systemu. Zapory ogniowe powinny obsługiwać zaawansowane funkcje filtrowania, takie jak głęboka inspekcja pakietów, inspekcja antywirusowa i obsługa inspekcji ruchu szyfrowanego. Firewallle na wszystkich strefach powinny obsługiwać ograniczanie ruchu w przypadku ataku typu denial-of-service poprzez flooding.
61. Wykonawca udokumentuje wszystkie ścieżki zdalnego dostępu i zapewni, że mogą one zostać włączone lub wyłączone przez Zamawiającego w razie potrzeby.



62. Domyślnie, cały dostęp zdalny będzie zablokowany. Zdalny dostęp będzie włączany na żądanie, zgodnie z obowiązującą polityką bezpieczeństwa Zamawiającego.
63. Rozwiązanie dostępu zdalnego powinno umożliwiać stosowanie dostępu warunkowego w oparciu o zasady zgodności, które uwzględniają parametry uwierzytelniania lub bezpieczeństwa, w tym:
- 1) certyfikaty klucza publicznego,
  - 2) członkostwo w domenie.
64. Zamawiający poinformuje Wykonawcę po zawarciu umowy o szczegółach technicznych połączenia i organizacyjnych w celu uzyskania zdalnego dostępu przez Wykonawcę do realizacji wdrożenia i serwisu Systemu.
65. Wykonawca skonfiguruje komponenty tunelowania komunikacji z Systemem, aby zapewnić kompleksową ochronę (np. szyfrowanie end-to-end) przesyłanych danych.
66. Wykonawca zastosuje środki bezpieczeństwa do stacji roboczych i serwerów wykorzystywanych (zwanym łącznie systemem zdalnego wsparcia) do świadczenia zdalnego wsparcia. Wykonawca przedstawi opis takich środków i procesów, które zostały ustanowione w celu utrzymania takich środków w działaniu i ich ciągłego doskonalenia.
67. Wykonawca zapewni bezpieczeństwo fizycznego dostępu do zasobów IT, które są wykorzystywane w systemie zdalnego wsparcia Wykonawcy.
68. Wykonawca będzie egzekwował ściśle fizyczne i elektroniczne procedury bezpieczeństwa dostępu do systemu zdalnego wsparcia Wykonawcy. System musi być co najmniej umieszczony w bezpiecznym miejscu i wymagać uwierzytelniania wieloskładnikowego w celu uzyskania dostępu.
69. Wykonawca wystąpi o zgodę na każde połączenie zdalnego dostępu, które zostanie autoryzowane przez Zamawiającego przed połączeniem, zgodnie z obowiązującymi u Zamawiającego regulacjami w tym zakresie.
70. Wykonawca będzie prowadzić listę pracowników upoważnionych do dostępu do Systemu Zamawiającego, identyfikując każdego z nich imieniem i nazwiskiem, tytułem, telefonem służbowym oraz listą systemów lub funkcji aplikacji, do których mają dostęp. Wykonawca będzie przechowywał historię zmian na tej liście do celów reagowania na incydenty.
71. Zamawiający będzie miał prawo i możliwość wyłączenia zdalnego dostępu udzielonego Wykonawcy bez uprzedniej konsultacji, jeśli zajdzie taka potrzeba. Aby zapewnić, że ten przypadek użycia nie zakłóci zadań instalacyjnych i konfiguracyjnych, Wykonawca będzie miał zapewnioną możliwość realizacji tych zadań za pośrednictwem komponentów lokalnych.
72. Wykonawca w ramach Projektu Technicznego Systemu lub odrębnego opracowania w ramach uzupełnienia istniejącej dokumentacji zawrze informacje o kierunkach przepływu informacji w Systemie, w tym o ich źródłach, miejscach docelowych, protokołach, itp.
73. Sprzęt sieciowy użyty do ułatwienia tworzenia kopii lustrzanych portów (ang. Switched Port Analyzer) musi być odpowiednio zwymiarowany. Porty lustrzane muszą być w stanie przekazywać cały ruch przechodzący przez urządzenie sieciowe, bez przerywania ruchu z powodu ograniczeń przepustowości.
74. Wykonawca dostarczy Zamawiającemu dokumentację projektową obejmującą:
- 1) zastosowane odpowiednie standardy i praktyki,
  - 2) środowisko programistyczne,



NARODOWY FUNDUSZ  
OCHRONY ŚRODOWISKA  
I GOSPODARKI WODNEJ

„Kofinansowane z oryginalnego systemu funduszu opartego na dotacji (Funduszu Modernizacyjnym)”



- 3) stosowane bezpieczne praktyki kodowania,
- 4) kontrolę wersji kodu źródłowego,
- 5) wewnętrzne przeglądy kodu,
- 6) bezpieczeństwo łańcucha dostaw.

Zakres dokumentacji powinien obejmować dostarczone rozwiązania sprzętowe, oprogramowanie i oprogramowanie sprzętowe Systemu.

75. Wykonawca zapewni program zapewnienia jakości i potwierdzi, że oprogramowanie Systemu przeszły testy kontroli jakości w celu zidentyfikowania i skorygowania potencjalnych słabości i luk w cyberbezpieczeństwie.

Testy te powinny obejmować:

- 1) testy fuzz,
- 2) testy statyczne,
- 3) testy dynamiczne,
- 4) testy penetracyjne.

Wykonawca wykorzysta pozytywne i odpowiednie negatywne testy w celu zweryfikowania, czy System działa zgodnie z wymaganiami, a także będzie monitorował nieoczekiwane lub niepożądane zachowanie podczas tych testów. Testy te mogą zostać przeprowadzone przez Wykonawcę lub niezależny podmiot. Wykonawca dostarczy dokumentację podsumowującą wyniki testów, która obejmuje nierozwiązane luki w zabezpieczeniach i zalecane środki zaradcze.

76. Wykonawca przedstawi Zamawiającemu w terminie 30 dni od daty podpisania Umowy zarys stosowanego programu cyberbezpieczeństwa, z wyłączeniem informacji poufnych stanowiących tajemnicę przedsiębiorstwa Wykonawcy.

77. Wykonawca zapewni bezpieczną sieć na potrzeby rozwoju Systemu Zamawiającego i określi elektroniczne (logiczne) zabezpieczenia zapewnione dla Systemu Zamawiającego, znajdujących się pod kontrolą Wykonawcy, w miejscu rozwoju Systemu.

Obejmuje to opis implementacji kontroli dostępu do sieci (np. zestawów reguł zapory sieciowej) wdrożonych w celu ograniczenia nieautoryzowanego dostępu elektronicznego do Systemu Zamawiającego lub do informacji i dokumentacji dotyczącej Systemu Zamawiającego lub systemu elektroenergetycznego Zamawiającego a także w celu ochrony Systemu przed nieumyślnym, niewłaściwym użyciem.

78. Wykonawca dostarczy Zamawiającemu w ciągu 3 (trzech) miesięcy od udzielenia zamówienia udokumentowaną procedurę dostępu do danych Systemu Zamawiającego, w przypadku gdy dane te będą znajdować się w siedzibie Wykonawcy. Procedura powinna spełniać następujące wymagania:

- 1) Procedura ta powinna obejmować proces przeglądu i zatwierdzania przez Strony realizowanego projektu w celu zapewnienia, że tylko upoważniony personel (tj. personel Wykonawcy) ma dostęp do Systemu i informacji Zamawiającego.
- 2) Zamawiający może zażądać przeglądu procedury w trakcie trwania projektu, w dowolnym rozsądnym czasie, powiadamiając Wykonawcę o planowanym przeglądzie na co najmniej jeden miesiąc przed planowanym przeglądem.
- 3) Wykonawca będzie stale udostępniać Zamawiającemu listę upoważnionych pracowników mających dostęp do środowiska programistycznego Systemu Zamawiającego.
- 4) Logiczny lub elektroniczny dostęp personelu Wykonawcy do Systemu będzie ograniczony do zakresu wymaganego do wykonywania przez personel obowiązków służbowych, w oparciu o odpowiednie role i obowiązki udokumentowane w ramach zatwierdzenia dostępu.



79. Wykonawca przekaże Zamawiającemu zasady i procedury jakie stosuje w celu odpowiedzialnego ujawniania informacji i zgłaszania zagrożeń, które będą obejmować zabezpieczenia przed publicznym ujawnianiem informacji.
80. Wykonawca przedłoży dokumentację swojego programu zarządzania poprawkami i procesu aktualizacji oprogramowania. Dokumentacja ta powinna zawierać:
- 1) zasoby techniczne do utrzymania tego programu i procesu,
  - 2) metodę lub zalecenia Wykonawcy dotyczące sposobu walidacji integralności poprawki przez Zamawiającego,
  - 3) podejście Wykonawcy i jego zdolność do naprawy nowo zgłoszonych luk typu zero-day.
81. Wykonawca zweryfikuje i dostarczy oświadczenie zawierające informację, że wszystkie istotne poprawki do prawidłowego funkcjonowania i konfiguracji komponentów Systemu zostały zainstalowane przed przystąpieniem do Odbioru Końcowego.
82. Wykonawca podejmie działania w celu zapewnienia integralności Systemu nawet podczas instalacji poprawek lub aktualizacji do nowej wersji oprogramowania.
- 1) Wykonawca zapewni procedurę weryfikacji integralności i autentyczności poprawek i nowych wersji oprogramowania przed ich zainstalowaniem.
  - 2) poprawki oraz nowe wersje oprogramowania powinny być podpisane cyfrowo (podpisywanie kodu), aby można było zweryfikować autentyczność oprogramowania.
83. Za każdym razem, gdy Wykonawca Systemu, dostawca systemu operacyjnego i dostawcy oprogramowania stron trzecich, wyda zmianę oprogramowania ("uaktualnienie", "aktualizację", "modyfikację", "wydanie" lub "poprawkę") w celu poprawienia błędu związanego z bezpieczeństwem w kodzie lub usunięcia luki w zabezpieczeniach, Wykonawca podejmie kroki, lecz nie rzadziej niż jeden raz na 6 miesięcy, w celu przetestowania, potwierdzenia i zainstalowania zmiany oprogramowania w Systemie.
- Wykonawca opracuje i przetestuje zmiany oprogramowania związane z bezpieczeństwem w środowisku oprogramowania "linii bazowej" w celu zminimalizowania czasu testowania wymaganego w Systemie Zamawiającego.
- Wykonawca powiadomi Zamawiającego tak szybko, jak to możliwe, że zbliża się zmiana oprogramowania zabezpieczającego, aby umożliwić Zamawiającemu przydzielenie odpowiednich zasobów do wdrożenia zmiany oprogramowania, gdy zostanie ona wydana.
84. Wstępne testy konfiguracji Systemu Zamawiającego zostaną przeprowadzone w środowisku testowym operacyjnie podobnym do środowiska produkcyjnego Systemu. Testowanie powinno mieć na celu potwierdzenie, że poprawka koryguje opublikowany błąd i nie wprowadza nowych błędów, tj. testy regresji.
85. Kierownik projektu Wykonawcy we współpracy z Kierownikiem projektu Zamawiającego będzie odpowiedzialny za realizację projektu i spełnienie określonych standardów i kryteriów jakości określonych w Projekcie Technicznym oraz zapewnienie, że Wykonawca i jego personel będą przestrzegać wszystkich wymaganych wymogów i przepisów bezpieczeństwa przez czas wdrożenia Systemu.
86. Zamawiający i Wykonawca będą wymieniać wszystkie informacje poufne za pośrednictwem kanałów komunikacji zatwierdzonych przez Zamawiającego.
- Poczta elektroniczna nie będzie używana do wymiany informacji poufnych, chyba że informacje są dodatkowo szyfrowane przy użyciu najnowocześniejszych metod, a klucze szyfrowania są bezpiecznie wymieniane.
87. Wykonawca przedstawi ogólny opis zasad i procedur zakazujących nieuprawnionego ujawniania wiedzy, informacji o architekturze lub konfiguracji istotnych dla Systemu Zamawiającego.

88. Wykonawca przedstawi Zamawiającemu procedurę bezpieczeństwa fizycznego, która będzie stosowana w odniesieniu do Systemu Zamawiającego znajdującego się pod kontrolą Wykonawcy, w miejscu realizacji Projektu przez Wykonawcę.  
Opis winien obejmować opis kontroli, kontroli "piętra testowego" oraz przepisów dotyczących zabezpieczenia dostępu do Systemów Zamawiającego w środowisku piętra testowego.  
Opisane zabezpieczenia fizyczne powinny obejmować ograniczenie dostępu do informacji i dokumentacji dotyczącej Systemu lub systemu elektroenergetycznego Zamawiającego oraz ochronę Systemu Zamawiającego przed nieumyślnym, niewłaściwym użyciem, a także przed uszkodzeniem lub kradzieżą.
89. Zamawiający przedstawi Wykonawcy najnowszą wersję Polityki bezpieczeństwa Zamawiającego na początkowym etapie realizacji projektu.  
Wykonawca dokona przeglądu i zaakceptuje wymagania Polityki bezpieczeństwa Zamawiającego.  
Personel Wykonawcy będzie przestrzegać wymogów Polityki bezpieczeństwa Zamawiającego podczas przebywania w lokalizacji Zamawiającego lub zdalnego połączenia z Systemem Zamawiającego w celu rozwoju lub konserwacji Systemu.
90. Wykonawca określi, w jaki sposób cyfrowe dostarczanie oprogramowania Systemu będzie walidowane i monitorowane w celu zapewnienia, że dostawa cyfrowa pozostaje zgodna ze specyfikacją. Wykonawca zastosuje kryptograficzne funkcje skrótu i szyfrowanie w celu ochrony integralności i poufności dostarczanego oprogramowania w trakcie realizacji Projektu.
91. Wykonawca dostarczy Zamawiającemu plany odtwarzania po awarii w celu przywrócenia:
- 1) podstawowych funkcji Systemu,  
oraz
  - 2) pełnej funkcjonalności Systemu, po awarii oprogramowania lub sprzętu Systemu.
- Plany muszą obejmować zidentyfikowane scenariusze odbudowy po awarii (ang. disaster recovery).  
Dodatkowo Wykonawca dostarczy Zamawiającemu plan odtworzenia środowiska na nowych zasobach sprzętowych.
92. Funkcje bezpieczeństwa cybernetycznego muszą być spójne we wszystkich aplikacjach i usługach Systemu, a zarządzanie bezpieczeństwem musi być realizowane dla wszystkich modułów składowych Systemu.
93. Wykonawca sporządzi dokumentację opisującą wszystkie fizyczne, proceduralne, personalne i inne środki bezpieczeństwa, które są niezbędne do zapewnienia ochrony:
- poufności i integralność danych w dostarczonym Systemie,
  - niezawodności dostarczonego Systemu.
94. Wykonawca uzgodni z Zamawiającym zakres, a następnie zleci do zewnętrznego wyspecjalizowanego podmiotu przeprowadzenie audytu bezpieczeństwa Systemu i uwzględni wyniki audytu wskazujące na luki w zabezpieczeniach Systemu, wyeliminuje je w ramach wdrożenia przed podpisaniem protokołu odbioru końcowego. Wykonawca dostarczy dokumentację podsumowującą wyniki testów.
95. System musi zapewniać identyfikację użytkowników zalogowanych do Systemu. Logowanie za pomocą dwuskładnikowego systemu opartego na AD Zamawiającego i karcie lub kluczu U2F. W przypadku awarii AD lokalnego systemu autoryzacyjnego i karty, System musi rejestrować i przechowywać wszystkie czynności zalogowanego użytkownika.
96. W Systemie musi być dostępne maskowanie hasła podczas jego wpisywania.



97. Wszystkie komponenty Systemu muszą zapewniać synchronizację swojego wewnętrznego zegara systemowego z zewnętrznym źródłem czasu z minimum dwóch wzorców czasu dostarczonych przez Wykonawcę w ramach wdrożenia, wykorzystujących różne technologie z wyłączeniem GLONASS.
98. System musi umożliwiać monitorowanie środowiska w trybie ciągłym, bez negatywnego wpływu na pracę Systemu.



NARODOWY FUNDUSZ  
OCHRONY ŚRODOWISKA  
I GOSPODARKI WODNEJ

„Kierowca finansowania z oryginalnego systemu funduszu opierającego się na (Funduszu Modernizacyjnym)”

