Projekt, 28.05.2026 r.

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia …….. 2026 r.

w sprawie minimalnych wymagań w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania infrastruktury krytycznej

Na podstawie art. 6ze ust. 4 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2026 r. poz. 574 oraz …) zarządza się, co następuje:

§ 1. Minimalne wymagania w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania, niezbędne do wdrażania rozwiązań w zakresie ochrony infrastruktury krytycznej, zwane dalej minimalnymi wymaganiami", są określone w załączniku do rozporządzenia.

§ 2. Minimalne wymagania mają charakter funkcjonalny i są wdrażane przez operatora infrastruktury krytycznej (zwanego dalej operatorem) w sposób zapewniający osiągnięcie celu ochrony infrastruktury krytycznej, adekwatnie do wyników analizy zagrożeń, o której mowa w art. 6ze ust. 1 pkt 2 ustawy o zarządzaniu kryzysowym.

§ 3. Minimalne wymagania stosuje się z uwzględnieniem lokalizacji oraz charakterystyki infrastruktury krytycznej, w szczególności:

1) rodzaju realizowanych funkcji infrastruktury krytycznej;
2) uwarunkowań przestrzennych, środowiskowych, technicznych i prawnych;
3) wzajemnych zależności z innymi elementami infrastruktury krytycznej, w tym zależności ciągłości działania infrastruktury krytycznej oraz funkcjonowania infrastruktury krytycznej w innych sektorach lub podsektorach;
4) charakterystyki sieci powiązań funkcjonalnych i organizacyjnych z innymi sektorami infrastruktury krytycznej, w tym z podmiotami krytycznymi oraz organami właściwymi w sprawach zarządzania kryzysowego.

§ 4. Rozporządzenie wchodzi w życie po upływie 14 dni od ogłoszenia.

Załącznik

do rozporządzenia Rady Ministrów z dnia ….

MINIMALNE WYMAGANIA W ZAKRESIE BEZPIECZEŃSTWA FIZYCZNEGO, TECHNICZNEGO, OSOBOWEGO, CYBERBEZPIECZEŃSTWA, PRAWNEGO ORAZ CIĄGŁOŚCI DZIAŁANIA INFRASTRUKTURY KRYTYCZNEJ

I. Bezpieczeństwo fizyczne obiektów lądowych

1. Bezpieczeństwo fizyczne obiektów lądowych obejmuje:
   1) opracowanie założeń systemu bezpieczeństwa fizycznego;
   2) wdrażanie rozwiązań proceduralnych;
   3) kontrolę osób oraz ładunków przekraczających granice stref ochrony infrastruktury krytycznej;
   4) bezpośrednią ochronę fizyczną (osobową);
   5) zapewnienie bariery fizycznej oddzielającej strefę zewnętrzną od pozostałych stref ochrony;
   6) instalowanie i utrzymywanie systemów zabezpieczeń technicznych rozumianych jako elektroniczne urządzenia i rozwiązania obejmujące co najmniej System Kontroli Dostępu (SKD), System Sygnalizacji Włamania i Napadu (SSWiN), System Dozoru Wizyjnego (VSS), zewnętrzne systemy zabezpieczeń oraz wszystkie kombinacje tych systemów instalowane w strefach ochrony (dalej SZT) zintegrowane z systemem bezpośredniej ochrony fizycznej;
   7) zabezpieczenia mechaniczne i budowlane.
2. Opracowanie, wdrażanie oraz okresowe aktualizacje procedur eskalacji środków bezpieczeństwa fizycznego dokonuje się z zachowaniem spójności z przedsięwzięciami właściwymi dla stopni alarmowych oraz stopni alarmowych CRP, o których mowa w art. 15 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2025 r. poz. 194).
3. Założenia systemu bezpieczeństwa fizycznego obejmują:
   1) identyfikację i ustalenie chronionych zasobów przez które rozumie się aktywa, w tym ludzi, informacje, technologie, obiekty i zapasy, które operator musi mieć

dostępne do wykorzystania w osiągnięciu swego celu, a których fizyczna utrata, jak również czasowa niedostępność, niesprawność lub niedyspozycyjność, będą miały niekorzystny wpływ na krytyczne procesy realizowane w organizacji;

2) przyjęcie podstawowych założeń projektowych dla systemu bezpieczeństwa fizycznego, w tym określenie potencjalnych oraz charakterystyki ich działania, z uwzględnieniem przewidywanych scenariuszy ataków, przy czym przez intruza rozumie się osobę, zwierzę, pojazd, statek wodny albo statek powietrzny, w tym załogowy albo bezzałogowy, a także inne urządzenie, obiekt lub maszyna, które w sposób nieuprawniony naruszyły granicę strefy ochrony albo znajdują się w tej strefie;
3) ocenę możliwości wyeliminowania przewidywanych scenariuszy ataków, a w przypadkach, gdy nie jest to możliwe – określenie niezbędnych czasów spowolnienia działania potencjalnych intruzów, powiązanych z rzeczywistym czasem interwencji sił bezpośredniej ochrony fizycznej;
4) ustalenie stref ochrony oraz zasad dostępu do nich;
5) przeprowadzenie szacowania ryzyka, rozumianego jako całościowy proces identyfikacji, analizy i oceny ryzyka, w celu doboru adekwatnych systemów zabezpieczeń technicznych, z uwzględnieniem zabezpieczeń mechanicznych i budowlanych;
6) dobór systemów zabezpieczeń technicznych, z uwzględnieniem zabezpieczeń mechanicznych i budowlanych;
7) opracowanie procedur reagowania uwzględniających specyfikę chronionych obiektów oraz rodzaj identyfikowanych zagrożeń;
8) zapewnienie przeszkolenia personelu ds. ochrony infrastruktury krytycznej w zakresie podejmowania właściwych działań dla identyfikowanych zagrożeń, przy czym przez personel ds. ochrony infrastruktury krytycznej rozumie się osoby wykonujące czynności związane z zapewnieniem bezpieczeństwa infrastruktury krytycznej, posiadające odpowiednie do zakresu zadań kwalifikacje, kompetencje i uprawnienia zarówno będących pracownikami jak i współpracownikami operatora, łącznie z pracownikami wewnętrznej służby ochrony, jeżeli operator utworzył taką służbę zgodnie zprzepisami ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia;
9) instalację i konfigurację systemów zabezpieczeń technicznych;

10) testowanie systemów zabezpieczeń technicznych oraz całego systemu bezpieczeństwa fizycznego infrastruktury krytycznej;
11) przegląd i korektę procedur;
12) systematyczne przeglądy systemu bezpieczeństwa fizycznego, obejmujące w szczególności kontrole działania, konserwacje oraz usuwanie zdiagnozowanych niesprawności, a w przypadkach, gdy nie jest to możliwe stosowanie środków zastępczych o parametrach umożliwiających utrzymanie funkcjonowania systemu zgodnie z dokumentacją powykonawczą;
13) systematyczny audyt lub certyfikację zainstalowanych systemów zabezpieczeń technicznych na zgodność z odpowiadającymi im Polskimi Normami.

4. Rozwiązania proceduralne bezpieczeństwa fizycznego polegają na:
1) stosowaniu działań prewencyjnych;
2) zapewnieniu możliwie najwcześniejszego wykrycia intruza;
3) przekazywaniu informacji o wykryciu intruza, w tym alarmowaniu;
4) stosowaniu środków spowalniających dotarcie intruza do stref ochrony;
5) podejmowaniu interwencji przez personel ds. ochrony infrastruktury krytycznej w celu zapewnienia bezpieczeństwa obiektu oraz rejestracji zdarzeń.

5. W celu zapobiegania zagrożeniom, w zależności od wyników analizy zagrożeń, przy uwzględnieniu przepisów ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, przeprowadza się w sposób stały lub doraźny kontrolę ruchu w strefie ochrony, przez którą rozumie się wyodrębniony obszar, dla którego określono wymagania w zakresie bezpieczeństwa oraz zasady dostępu i przebywania. W zależności od potrzeb w ramach strefy ochrony wyznacza się w szczególności:

1. strefę ochrony wewnętrznej, przez którą rozumie się przestrzeń wokół zasobu chronionego, ograniczona barierą fizyczną, zwaną obrysem, wewnątrz której intruz, po pokonaniu obrysu, może osiągnąć cel ataku bez istotnego opóźnienia;
2. strefę ochrony peryferyjnej, przez którą rozumie się przestrzeń na zewnątrz obrysu ograniczoną obwodem, w której personel ds. ochrony infrastruktury krytycznej może prowadzić działania opóźniające i izolacyjne wobec intruza;
3. strefę ochrony zewnętrznej, przez którą rozumie się przestrzeń na zewnątrz obwodu, pozostająca poza obszarem bezpośredniej ochrony fizycznej.

W strefie ochrony w sposób pełny lub wyrywkowy przeprowadza się kontrolę ładunków wprowadzanych do strefy i wyprowadzanych z tej strefy oraz kontrolę zasobów

i pracowników operatora, kontrahentów, dostawców, wykonawców, podwykonawców i gości, przy czym:

1) określa się procedury kontroli osób i ładunków w procedurach wewnętrznych, obejmujących w szczególności zasady wejścia, wjazdu, wyjścia i wyjazdu do i z obiektu oraz stref ochrony, a także zasady poruszania się w strefie ochrony z uwzględnieniem odrębnych zasad wobec określonych osób lub grup osób, jeżeli operator dopuszcza takie rozwiązania;
2) poruszanie się gości w strefie ochrony odbywa się pod nadzorem osoby upoważnionej przez operatora, od momentu wejścia do chwili opuszczenia obiektu, jeżeli operator nie określi inaczej w procedurach;
3) zapewnia się zarządzanie dostępem do stref ochrony poprzez nadawanie, zmianę oraz cofanie uprawnień dostępu z wykorzystaniem:
   a) przepustek (identyfikatorów lub kart dostępu),
   b) kodów dostępu, w tym kodów pierwszego logowania,
   c) kluczy do pomieszczeń lub stref ochrony;
4) określa się zasady:
   a) wydawania, ewidencjonowania i odbierania przepustek, identyfikatorów, kart i kluczy,
   b) przechowywania kluczy oraz zarządzania kodami dostępu,
   c) okresowej weryfikacji oraz aktualizacji uprawnień dostępu;
5) przepustki, identyfikatory lub karty dostępu podlegają indywidualizacji oraz ewidencjonowaniu w sposób umożliwiający identyfikację osoby uprawnionej;
6) przepustki, identyfikatory lub karty dostępu powinny posiadać zabezpieczenia utrudniające ich przerabianie lub nieuprawnione wykorzystanie;
7) przepustki stałe oraz okresowe umożliwiające samodzielne poruszanie się w strefie ochrony umożliwiają jednoznaczną identyfikację ich posiadacza;
8) przepustki jednorazowe mogą być wydawane na czas określony i podlegają zwrotowi po opuszczeniu strefy ochrony. Należy zastosować rozwiązania uniemożliwiające ich wykorzystanie po upływie okresu ważności;
9) przepustki nie zawierają informacji, których ujawnienie mogłoby ułatwić ich nieuprawnione wykorzystanie w przypadku utraty;

10) stosuje się środki techniczne służące identyfikacji i weryfikacji osób wchodzących do obiektów infrastruktury krytycznej, w tym rozwiązania biometryczne, jeżeli jest to uzasadnione oceną ryzyka.

6. Zapewnia się rejestrowanie wejścia osób i wjazdu pojazdów do stref ochrony oraz wyjścia i wyjazdu z tych stref, a także przechowywanie zarejestrowanych danych nie krócej niż 90 dni. W przypadku wykrycia albo uzasadnionego podejrzenia popełnienia czynu zabronionego w rozumieniu Kodeksu karnego, dane mogące mieć związek z tym czynem podlegają zabezpieczeniu i archiwizowaniu w sposób niezmieniający ich treści, do czasu zakończenia czynności wyjaśniających albo postępowania prowadzonego w sprawie.

7. Zapewnia się doraźną lub stałą bezpośrednią ochronę fizyczną infrastruktury krytycznej w zależności od wyników analizy zagrożeń oraz charakterystyki chronionej infrastruktury krytycznej, a w przypadku infrastruktury krytycznej ujętej w ewidencji, o której mowa w art. 5 ust. 5 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2025 r. poz. 532) zapewnia się ochronę wynikającą z planu ochrony, o którym mowa w art. 7 ust. 1 tej ustawy, przy czym:

1) bezpośrednia ochrona fizyczna może być realizowana przez operatora w formie Wewnętrznej Służby Ochrony albo zapewniana przez podmiot zewnętrzny posiadający koncesję na prowadzenie działalności gospodarczej w zakresie usług ochrony osób i mienia, o której mowa w art. 17 ust. 1 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. 2025 poz. 532);

2) zapewnia się, aby pracownicy ochrony fizycznej posiadali broń na podstawie świadectwa broni, o którym mowa w art. 29 ust. 1 pkt 1 i 2 ustawy z dnia 21 maja 1999 r. o broni i amunicji (Dz. U. z 2024 r. poz. 485), jeżeli wynika to z analizy zagrożeń lub planu ochrony, o którym mowa w art. 7 ust. 1 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia;

3) wymogu stałej bezpośredniej ochrony fizycznej nie stosuje się dla obiektów liniowych (rurociągi, linie energetyczne, drogi i linie kolejowe) oraz obiektów bez stałej obsługi, chyba że przeprowadzona analiza zagrożeń wykaże taką potrzebę.

8. Wyznacza się fizyczną barierę oddzielającą strefę zewnętrzną od pozostałych stref ochrony infrastruktury krytycznej, przy czym:

1) fizyczna bariera jest realizowana w szczególności jako jeden element lub kombinacja kilku elementów, którymi mogą być:
   a) ogrodzenie, bramy, furtki,
   b) ściana budynku,
   c) naturalna, ukształtowana przeszkoda terenowa lub obszar wodny,
   d) zabezpieczenie drogowe antyterrorystyczne,
3) inny element konstrukcyjny, architektoniczny lub krajobrazowy spełniający funkcję ochronną;
2) fizyczna bariera jest projektowana i utrzymywana w sposób umożliwiający skuteczną integrację z systemami zabezpieczeń technicznych;
3) zapewnia się całodobową obserwację fizycznej bariery oraz punktów wejścia i wjazdu do stref ochrony;
4) w zakresie ogrodzeń, bram i furtek stosuje się przepisy rozporządzenia ministra infrastruktury z 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (tj. Dz. U. z 2022 r. poz. 1225);
5) zapewnia się, aby bramy i furtki stanowiące element fizycznej bariery:
   a) odpowiadały wysokości oraz charakterystyce bariery fizycznej,
   b) uwzględniały odporność na nieuprawnione sforsowanie lub staranowanie, stosownie do wyników analizy zagrożeń,
   c) były wyposażone w środki umożliwiające kontrolę ruchu osobowego i pojazdów;
6) bramy i urządzenia zamykane automatycznie wyposaża się w rozwiązania uniemożliwiające ich zamknięcie w czasie trwania ruchu osobowego lub pojazdów oraz w środki ostrzegawcze;
7) stosuje się dodatkowe zabezpieczenia wjazdów, w szczególności urządzenia zaporowe lub kontrolne, jeżeli wynika to z analizy zagrożeń;
8) w przypadku przewidywania zagrożeń polegających na celowym wykorzystaniu pojazdów jako środka ataku (vehicle-borne attack) zapewnia się zastosowanie zabezpieczeń drogowych antyterrorystycznych z uwzględnieniem:
   a) przewidywanego typu pojazdu stanowiącego zagrożenie, w tym z jego masy i prędkości,
   b) dopuszczalnej odległości penetracji pojazdu w głąb strefy ochrony, wymaganych czasów reakcji i interwencji;

9) zabezpieczenia drogowe antyterrorystyczne realizuje się w szczególności jako:
   a) zapory drogowe stałe lub wysuwane,
   b) słupki antyterrorystyczne, w tym stałe, wysuwane lub mobilne,
   c) bariery liniowe lub segmentowe, w tym rozwiązania powierzchniowe,
   d) bramy i zapory drogowe o podwyższonej odporności na uderzenie pojazdu,
   e) elementy krajobrazowe lub architektoniczne zaprojektowane i wykonane w sposób zapewniający funkcję ochrony antyterrorystycznej;
10) jeżeli fizyczna bariera nie spełnia wymagań wynikających z charakterystyki i lokalizacji infrastruktury krytycznej, zapewnia się zastosowanie rozwiązań kompensacyjnych zapewniających równoważny poziom bezpieczeństwa;
11) rozwiązania kompensacyjne mogą obejmować w szczególności:
   a) systemy ochrony obwodowej,
   b) systemy dozoru wizyjnego (VSS),
   c) zwiększenie liczby posterunków ochrony, patroli lub innych środków organizacyjnych;
12) jeżeli fizyczną barierę stanowi ściana budynku, zapewnia się, aby jej konstrukcja oraz stan techniczny zapewniały poziom ochrony nie niższy niż w przypadku ogrodzenia;
13) w przypadku drzwi lub okien stanowiących element bariery fizycznej zapewnia się zastosowanie rozwiązań proceduralnych, technicznych lub organizacyjnych zapobiegających ich pozostawieniu w stanie otwartym, odblokowanym lub innym stanie, który umożliwia ominięcie albo osłabienie bariery fizycznej;
14) drzwi i okna, których dostępność może powodować nieakceptowalne ryzyko nieuprawnionego wejścia, zapewniają odporność adekwatną do wymaganego czasu spowolnienia potencjalnego intruza albo są zabezpieczone innymi równoważnymi rozwiązaniami;
15) fizyczną barierę oznacza się informacją o zakazie nieuprawnionego wstępu do strefy ochrony;
16) zapewnia się warunki do skutecznej obserwacji strefy zewnętrznej oraz patrolowania strefy peryferyjnej, jeżeli wynika to z charakterystyki i lokalizacji infrastruktury krytycznej;

17) jeżeli jest to uzasadnione analizą zagrożeń, stosuje się rozwiązania umożliwiające wczesne wykrycie naruszenia bariery fizycznej, w szczególności systemy zabezpieczeń technicznych.

9. Zapewnia się, by systemy zabezpieczeń technicznych były zaprojektowane, zainstalowane i skonfigurowane w taki sposób, aby czas pomiędzy wykryciem intruza a reakcją personelu ds. ochrony infrastruktury krytycznej był krótszy niż czas potrzebny do uszkodzenia lub narażenia bezpieczeństwa zasobów infrastruktury krytycznej, przy czym:
   1) systemy zabezpieczeń technicznych są objęte wsparciem w zakresie aktualizacji bezpieczeństwa, zapewnionym przez operatora w umowie z producentem albo dostawcą przez okres nie krótszy niż 5 lat od dnia zakończenia produkcji urządzenia lub rozwiązania, obejmującym udostępnianie poprawek usuwających podatności, informowanie o wykrytych podatnościach i zalecanych działaniach naprawczych oraz techniczną możliwość bezpiecznej instalacji aktualizacji;
   2) każdy z systemów, po zainstalowaniu i skonfigurowaniu, powinien spełniać co najmniej wymagania stopnia 3 określone w:
      a) PN-EN 50131-1 – dla systemów sygnalizacji włamania i napadu,
      b) PN-EN 60839-11-1 – dla systemów kontroli dostępu,
      c) PN-EN 62676-1-1 – dla systemów dozoru wizyjnego
      - wykorzystując optymalne parametry techniczne urządzeń, funkcjonując poprawnie w przewidzianych dla nich warunkach środowiska pracy i nie utrudniając codziennej pracy personelu;
   3) dopuszcza się stosowanie kamer, których ustawienia fabryczne można przywrócić programowo (zdalnie) bez konieczności ingerencji fizycznej pod warunkiem, że kamery pracują w systemie zamkniętym, izolowanym od sieci Internet;
   4) czynności obejmujące projektowanie, instalowanie, konserwację i naprawy systemów zabezpieczeń technicznych są wykonywane przez:
      a) personel ds. ochrony infrastruktury krytycznej operatora lub
      b) usługodawców zewnętrznych;
   5) osoby wykonujące projektowanie, instalowanie, konserwację i naprawy systemów zabezpieczeń technicznych muszą posiadać kwalifikacje,

kompetencje oraz uprawnienia odpowiednie do zakresu realizowanych czynności, potwierdzone w szczególności przez:

a) zaświadczenie o wpisie na listę kwalifikowanych pracowników zabezpieczenia technicznego,
b) zaświadczenie o ukończeniu kursu pracownika zabezpieczenia technicznego wydane przez wyspecjalizowaną w tym zakresie placówkę kształcenia ustawicznego działającą w systemie oświaty,
c) dokument potwierdzający odbycie szkolenia aktualizującego, jeśli od wydania zaświadczenia o ukończeniu kursu pracownika zabezpieczenia technicznego upłynęło 3 lata lub więcej, przy czym przez dokument należy rozumieć każdy przedmiot lub inny zapisany nośnik informacji;
d) dokumenty potwierdzające ukończenie szkoleń produktowych właściwych dla zastosowanych systemów SZT,
e) dokumenty potwierdzające posiadanie innych uprawnień niezbędnych do realizacji powierzonych czynności, jeżeli wynika to z ich charakteru.

10. Dokonuje się weryfikacji spełnienia wymagań w zakresie kwalifikacji, kompetencji oraz uprawnień pracowników oraz usługodawców zewnętrznych przed rozpoczęciem realizacji czynności związanych z SZT oraz w trakcie ich trwania, poprzez przedłożenie do wglądu oryginałów:
    a) zaświadczeń i innych dokumentów potwierdzających spełnienie wymagań, o których mowa w ust. 9 pkt. 5,
    b) certyfikatów lub innych dokumentów potwierdzających posiadanie odpowiednich kompetencji i uprawnień przez usługodawców zewnętrznych, zgodnie z art. 6ze ust. 5 pkt. 1 oraz art. 6ze ust. 6 ustawy o zarządzaniu kryzysowym,
    c) koncesji, o której mowa w art. 15 ust. 1 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia.
11. Zapewnia się przeprowadzenie szkolenia personelu ds. ochrony infrastruktury krytycznej w zakresie obsługi i eksploatacji zainstalowanych systemów zabezpieczeń technicznych.
12. Przed odbiorem końcowym systemu zabezpieczeń technicznych, przeprowadza się okres próbny działania tego systemu w czasie określonym w dokumentacji technicznej wykonawczej.

13. Zapewnia się monitorowanie działania systemu w okresie próbnym przez personel ds. ochrony infrastruktury krytycznej, w szczególności w zakresie identyfikacji nieprawidłowości w jego działaniu oraz okoliczności ich występowania.
14. Zidentyfikowane w okresie próbnym nieprawidłowości podlegają rejestracji. Rejestr nieprawidłowości jest przekazywany w sposób udokumentowany pomiotowi, który zainstalował system, w celu usunięcia usterek.
15. Po zakończeniu okresu próbnego, jeżeli nie stwierdzono nieprawidłowości w działaniu systemu zabezpieczeń technicznych lub jeżeli zostały one skutecznie usunięte, dokonuje się udokumentowanego odbioru końcowego systemu.
16. Odbiór końcowy systemu zabezpieczeń technicznych obejmuje minimum weryfikację:
    1) dokumentacji technicznej powykonawczej,
    2) zgodności zainstalowanych urządzeń i elementów z dokumentacją techniczną powykonawczą,
    3) oprogramowania systemu,
    4) posiadania ważnych licencji uprawniających do korzystania z oprogramowania,
    5) parametrów technicznych systemu zabezpieczeń technicznych oraz urządzeń wchodzących w jego skład,
    6) poprawności działania systemu oraz wszystkich jego elementów we wszystkich konfiguracjach przewidzianych w dokumentacji technicznej i instrukcji użytkowania,
    7) zdolności do pracy ze źródła zasilania podstawowego i rezerwowego zgodnie z wymaganiami właściwymi dla stopnia zabezpieczenia określonego w dokumentacji technicznej,
    8) sposobu konfiguracji mechanizmów zdalnego dostępu do systemu zabezpieczeń technicznych z uwzględnieniem zapewnienia dostępu wyłącznie podmiotom uprawnionym i po odpowiednim uwierzytelnieniu się,
    10) poprawności wydzielenia logicznego lub fizycznego systemu zabezpieczeń technicznych od innych sieci teleinformatycznych operatora,
    11) jakości wykonanych prac, w tym sposobu wykonania połączeń wewnętrznych oraz oznakowania elementów systemu, kabli i przewodów,

12) sposobu zabezpieczenia przed nieautoryzowanym zastąpieniem urządzenia w systemie zabezpieczeń technicznych urządzeniem identycznym lub symulowanym,
13) dokumentacji z przeprowadzonego szkolenia w zakresie obsługi zainstalowanego systemu zabezpieczeń technicznych.

17. Czynności, o których mowa w ust. 18 nie przeprowadza się, jeżeli właściwa w zakresie systemów zabezpieczeń technicznych jednostka certyfikująca dokonała oceny zgodności dokumentacji wykonawczej systemu zabezpieczeń technicznych z odpowiednią dla danego systemu Polską Normą, a zainstalowany system zabezpieczeń uzyskał certyfikat zgodności z tą samą Polską Normą.
18. Ocena zgodności dokumentacji wykonawczej obejmuje w szczególności weryfikację:
    1) zgodności przyjętych rozwiązań projektowych z odpowiednimi Polskimi Normami,
    2) spójności dokumentacji wykonawczej z wynikami analizy zagrożeń przeprowadzonej dla infrastruktury krytycznej,
    3) kompletności i jednoznaczności dokumentacji wykonawczej w zakresie niezbędnym do certyfikacji systemu.
19. Zapewnia się rozpoczęcie czynności utrzymaniowych niezwłocznie po odbiorze końcowym.
20. Zapewnia się utrzymanie uzyskanego stopnia zabezpieczenia systemów zabezpieczeń technicznych przez wykonywanie systematycznych przeglądów technicznych, konserwacji oraz napraw, w okresach określonych w dokumentacji technicznej, z uwzględnieniem wymagań określonych w Polskich Normach i wytycznych do ich stosowania właściwych dla danego systemu.
21. Prowadzi się rejestr przeglądów technicznych, konserwacji i napraw systemów zabezpieczeń technicznych obejmujący w szczególności:
    1) oznaczenie systemu zabezpieczeń technicznych, urządzenia albo elementu systemu, a także oznaczenie lub lokalizację obiektu, w którym są zainstalowane;
    2) datę i godzinę rozpoczęcia oraz zakończenia prac;
    3) rodzaj i zakres wykonanych prac, w tym numer protokołu odbioru, jeżeli został sporządzony;
    4) nazwę wykonawcy oraz imię i nazwisko osoby wykonującej pracę;

5) numery albo inne oznaczenia dokumentów potwierdzających kwalifikacje, kompetencje lub uprawnienia osoby wykonującej pracę lub usługodawcy zewnętrznego;
6) podpis osoby wykonującej pracę;
7) stanowisko, imię i nazwisko użytkownika systemu oraz jego podpis;
8) stan systemu po wykonaniu przeglądu technicznego, konserwacji albo naprawy;
9) inne uwagi.

22. Zapewnia się przechowywanie zapisu zdarzeń z systemu sygnalizacji włamania i napadu oraz zapisu obrazu z systemu dozoru wizyjnego, przez okres co najmniej 90 dni. W przypadku wykrycia albo uzasadnionego podejrzenia popełnienia czynu zabronionego w rozumieniu Kodeksu karnego zapis mogący mieć związek z tym czynem podlega zabezpieczeniu i archiwizowaniu w sposób niezmieniający jego treści, do czasu zakończenia czynności wyjaśniających albo postępowania prowadzonego w sprawie.
23. Zapewnia się funkcjonowanie systemu transmisji alarmów generowanych przez SZT oraz centrum monitorowania alarmów w ramach wewnętrznej służby ochrony, albo poprzez powierzenie ich wykonywania koncesjonowanemu podmiotowi wykonującemu działalność gospodarczą w zakresie usług ochrony osób i mienia; przy czym przez centrum monitorowania alarmów rozumie się wyodrębnioną organizacyjnie jednostkę przeznaczoną do całodobowego przyjmowania, przetwarzania i obsługi sygnałów alarmowych oraz innych informacji o zdarzeniach związanych z bezpieczeństwem infrastruktury krytycznej, a także do dysponowania grupami interwencyjnymi i koordynacji ich działań.
24. System transmisji alarmów zapewnia przekazywanie informacji o stanie systemów alarmowych z obiektów infrastruktury krytycznej do centrum monitorowania alarmów; przy czym przez system transmisji alarmów (STA) rozumie się zespół urządzeń wraz z łączącymi je torami komunikacji służący do przesyłania informacji ze strefy ochrony do centrum monitorowania alarmów, dotyczących stanu systemu sygnalizacji włamania i napadu.
25. Transmisja informacji alarmowych jest realizowana w sposób nieprzerwany, niezawodny i bezpieczny, adekwatnie do poziomu ryzyka, charakterystyki oraz lokalizacji chronionej infrastruktury krytycznej.

26. Parametry systemu transmisji alarmu powinny odpowiadać stopniowi zabezpieczenia systemu sygnalizacji włamania i napadu.
27. System transmisji alarmów powinien zapewniać redundancję transmisji, w szczególności poprzez zastosowanie co najmniej dwóch niezależnych torów komunikacyjnych.
28. System transmisji alarmów powinien monitorować dostępność i sprawność każdego z wykorzystywanych torów transmisji. W przypadku stwierdzenia błędów lub utraty komunikacji system powinien wygenerować alarm techniczny.
29. Przekaz sygnałów alarmowych z monitorowanych systemów alarmowych powinien odbywać się ze zwrotnym potwierdzeniem odbioru. Brak sygnału potwierdzenia odebrania alarmu powinien skutkować wygenerowaniem komunikatu alarmowego w obiekcie chronionym.
30. Funkcjonowanie systemu transmisji alarmów podlega bieżącemu nadzorowi, analizie dostępności oraz dokumentowaniu parametrów jego pracy, a zapisy dotyczące jego działania są przechowywane przez okres co najmniej jednego roku.
31. Centrum monitorowania alarmów może być zlokalizowane w obiekcie operatora albo funkcjonować jako wyodrębniona jednostka organizacyjna podmiotu zewnętrznego realizującego zadania ochrony fizycznej.
32. Zapewnia się, aby centrum monitorowania alarmów realizowało całodobowe przyjmowanie, przetwarzanie i obsługę sygnałów alarmowych.
33. Zapewnia się ciągłość funkcjonowania centrum monitorowania alarmów przez zastosowanie rozwiązań organizacyjnych i technicznych umożliwiających przejęcie jego funkcji przez zapasowe centrum monitorowania alarmów, zlokalizowane w innym miejscu niż centrum podstawowe.
34. Centrum monitorowania alarmów funkcjonuje w pomieszczeniach zabezpieczonych przed nieuprawnionym dostępem oraz zdarzeniami mogącymi zakłócić jego pracę, chronionych systemami zabezpieczeń technicznych.
35. Informacje o stanie bezpieczeństwa centrum monitorowania alarmów są przekazywane do innego, niezależnego centrum monitorowania alarmów.
36. Centrum monitorowania alarmów posiada zasilanie rezerwowe umożliwiające jego nieprzerwaną pracę przez okres odpowiadający wymaganiom ciągłości działania infrastruktury krytycznej.

37. Personel centrum monitorowania alarmów posiada kwalifikacje, kompetencje i uprawnienia adekwatne do realizowanych zadań.
38. Zapewnia się odbywanie przez personel centrum monitorowania alarmów okresowych szkoleń co najmniej w zakresie obsługi sygnałów alarmowych, dysponowania grupami interwencyjnymi i procedur reagowania. Jeżeli centrum jest prowadzone przez podmiot zewnętrzny, obowiązek ten operator zapewnia w umowie z tym podmiotem.
39. Obsługa centrum monitorowania alarmów odbywa się z zachowaniem zasad rozliczalności obejmujących jednoznaczną identyfikację, autoryzację i rolę osób obsługujących centrum oraz rejestrację podejmowanych przez nie działań.
40. Obsługa zdarzeń alarmowych obejmuje ciągłe monitorowanie sygnałów z chronionych obiektów oraz podejmowanie działań adekwatnych do rodzaju zdarzenia.
41. Zapewnia się priorytetyzację obsługi zdarzeń alarmowych, w szczególności w odniesieniu do zdarzeń o charakterze napadu, włamania, sabotażu lub awarii technicznej.
42. Zapewnia się możliwość niezwłocznego dysponowania grupami interwencyjnymi w ramach wewnętrznej służby ochrony lub poprzez zawarcie umowy z przedsiębiorcą, który uzyskał koncesję na wykonywanie działalności gospodarczej w zakresie usług ochrony osób i mienia, a także skuteczną koordynację działań interwencyjnych z wykorzystaniem odpowiednich środków łączności.
43. Gotowość operacyjna grup interwencyjnych podlega bieżącemu nadzorowi, w tym monitorowaniu ich stanu i dostępności.
44. Komunikacja związana z obsługą zdarzeń alarmowych podlega rejestracji i archiwizacji przez okres umożliwiający analizę zdarzeń oraz prowadzenie postępowań wyjaśniających nie krótszy niż 6 miesięcy.
45. Zapewnia się w czasie rzeczywistym wymianę danych oraz informacji o potencjalnym zagrożeniu z właściwymi służbami odpowiedzialnymi za zapewnienie bezpieczeństwa publicznego.

II. Bezpieczeństwo fizyczne infrastruktury krytycznej zlokalizowanej na polskich obszarach morskich

1. W ramach bezpieczeństwa fizycznego obiektów zlokalizowanych na polskich obszarach morskich w rozumieniu ustawy z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej:
   1) chroni się:
      a) stacje elektroenergetyczne zlokalizowane na morzu, w rozumieniu art. 3 ustawy z dnia 17 grudnia 2020 r. o promowaniu wytwarzania energii elektrycznej w morskich farmach wiatrowych,
      b) kablowe linie eksportowe na odcinku morskim,
      c) inne istotne elementy lub urządzenia związane z wyprowadzeniem mocy z morskiej farmy wiatrowej, zlokalizowane na morzu, których potrzeba szczególnej ochrony wynika z przeprowadzonej analizy zagrożeń.
   2) zapewnia się:
      a) zautomatyzowany system umożliwiający wykrywanie i rejestrację działań realizowanych przez statki, okręty, bezzałogowe obiekty pływające oraz bezzałogowe statki powietrzne, obejmujący obszar strefy bezpieczeństwa ustanowionej dla stacji elektroenergetycznej zlokalizowanej na morzu, umożliwiający ich obserwację, śledzenie, rozpoznanie i identyfikację wraz z analizą sposobu ich manewrowania, w celu określenia potencjalnego zagrożenia dla infrastruktury krytycznej,
      b) system detekcji umożliwiający wykrycie próby ingerencji w kabel eksportowy,
      c) system teleinformatyczny umożliwiający monitorowanie ruchu statków pływających co najmniej w obszarze strefy bezpieczeństwa ustanowionej dla infrastruktury, o której mowa w pkt 1,
      d) okresowe przeglądy techniczne infrastruktury podwodnej, w celu wykrycia zagrożeń,
      e) system przekazywania informacji o incydentach do centrum monitorowania alarmów, w którym na podstawie obowiązujących procedur operatora podejmowana będzie decyzja o ewentualnym powiadomieniu odpowiednich służb państwowych,

f) stosowanie systemów zabezpieczeń technicznych posiadających klasę szczelności dostosowaną do warunków środowiskowych panujących w miejscu instalacji urządzenia (m.in. strefy rozbryzgu, zanurzenia lub narażenia na mgłę solną), określoną w dokumentacji wykonawczej,

g) wymianę danych oraz informacji o potencjalnym zagrożeniu w czasie rzeczywistym z właściwymi służbami odpowiedzialnymi za zapewnienie bezpieczeństwa na morzu.

2. W przypadku braku redundancji kabla eksportowego opracowuje się i wdraża plan postępowania na wypadek jego awarii, obejmujący w szczególności zautomatyzowane przełączenie obciążenia lub plan przełączenia ręcznego z poziomu stacji elektroenergetycznej zlokalizowanej na morzu.

III. Bezpieczeństwo techniczne

1. W ramach bezpieczeństwa technicznego:
   1) prowadzi się analizę ryzyka operacyjnego związanego z zawodnością urządzeń, instalacji technologicznych oraz systemów organizacyjnych, rozumianego jako ryzyko strat materialnych i reputacyjnych oraz odpowiedzialności prawnej, wynikających z niedostosowania lub zawodności procesów i niezbędnych dla nich zasobów (osobowych, materialnych, informacyjnych i finansowych), a powstających w wyniku zakłóceń będących następstwem oddziaływania zagrożeń wewnętrznych i zewnętrznych,
   2) wdraża się zintegrowane zarządzanie bezpieczeństwem technicznym obiektu infrastruktury krytycznej obejmujące:
      a) nośność i stateczność konstrukcji,
      b) bezpieczeństwo pożarowe,
      c) higienę, zdrowie i środowisko,
      d) bezpieczeństwo użytkowania i dostępność,
      e) ochronę przed hałasem,
      f) oszczędność energii i izolacyjność cieplną,
      g) zrównoważone wykorzystania zasobów naturalnych;
   3) analizuje się potencjalne zakłócenia dla niezawodności technicznej poszczególnych instalacji i wdraża środki zapewniające niezawodność poprzez:
      a) redundancję urządzeń,
      b) skracanie czasu naprawy,
      c) stały nadzór lub monitoring stanu technicznego,
      d) dobór elementów składowych o podwyższonej jakości;
   4) zapewnia się zdolność serwisową poprzez:
      a) remonty zapobiegawcze planowane,
      b) remonty wyznaczone na podstawie analizy stanu technicznego;
   5) ogranicza się możliwość powstania uszkodzeń infrastruktury krytycznej na skutek zaniku zaopatrzenia w wodę i czynniki chłodzące, przerwanie transmisji danych albo braku energii elektrycznej;
   6) zapewnia się podtrzymanie zasilania w energię elektryczną przez okres co najmniej 4 godzin przedłużony o czas niezbędny na bezpieczne zakończenie lub planowe ograniczenie procesów technologicznych;

7) wyznacza się podstawowe i zapasowe miejsce funkcjonowania zespołu zarządzania bezpieczeństwem technicznym.

2. Wymóg zapewnienia awaryjnego zasilania w energię elektryczną nie dotyczy jednostek wytwórczych w rozumieniu prawa energetycznego dla których 8-godzinna przerwa w dostawach energii elektrycznej nie wpływa na ciągłość działania.

IV. Bezpieczeństwo osobowe

1. W ramach bezpieczeństwa osobowego:
   1) opracowuje się, wdraża i poddaje okresowym przeglądom politykę bezpieczeństwa osobowego;
   2) definiuje się role i odpowiedzialności oraz przydziela uprawnienia w obszarze bezpieczeństwa osobowego;
   3) prowadzi się analizę zagrożeń związaną z możliwym negatywnym oddziaływaniem na bezpieczeństwo infrastruktury krytycznej własnego personelu i usługodawców;
   4) opracowuje się i wdraża procedurę ustalania tożsamości osób przed dopuszczeniem do pracy;
   5) dokonuje się weryfikacji kwalifikacji i kompetencji personelu związanego z funkcjonowaniem infrastruktury krytycznej;
   6) opracowuje i stosuje się procedurę sprawdzania przeszłości kryminalnej kandydatów i pracowników związanych z funkcjonowaniem infrastruktury krytycznej zgodnie z przepisami ustawy o zarządzaniu kryzysowym i innych ustaw;
   7) zapewnia się personelowi dostęp do stref ochrony, systemów i informacji wyłącznie w zakresie niezbędnym do wykonywania obowiązków;
   8) opracowuje się i wdraża procedury udzielania czasowego dostępu do stref ochrony, systemów i informacji dla usługobiorców realizujących czynności serwisowe i naprawcze;
   9) zapewnia się jednoznaczną identyfikację wizualną personelu związanego z infrastrukturą krytyczną z podziałem na pracowników, gości i podwykonawców;
   10) okresowo organizuje się udokumentowane szkolenia dla personelu w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, prawnego i ciągłości działania adekwatnie do ról realizowanych w organizacji obejmujące w szczególności:
      a) znajomość obowiązujących przepisów prawa i wymagań normatywnych w zakresie ochrony infrastruktury krytycznej,
      b) umiejętność identyfikacji zagrożeń oraz rozpoznawania sytuacji kryzysowych,

c) znajomość zasad bezpieczeństwa obowiązujących, w tym procedur reagowania na zdarzenia i incydenty,

d) świadomość ról, uprawnień oraz odpowiedzialności w systemie ochrony infrastruktury krytycznej,

e) podstawowe zasady postępowania w przypadku zagrożeń o charakterze antagonistycznym,

f) znaczenie infrastruktury krytycznej, którą zarządza operator, przy czym dla personelu ds. ochrony infrastruktury krytycznej szkolenia obejmują dodatkowo zagadnienia odpowiadające zakresowi realizowanych zadań oraz podtrzymują posiadane kwalifikacje, kompetencje i uprawnienia.

2. W przypadku powierzania podwykonawcom części procesów związanych z funkcjonowaniem infrastruktury krytycznej w umowach z usługodawcami zewnętrznymi określa się wymagania w zakresie bezpieczeństwa osobowego, w szczególności dotyczące weryfikacji personelu, szkoleń, zasad dostępu, odpowiedzialności oraz szczegółowych wymagań co do kompetencji pracowników usługodawcy, a także zasady dostępu do stref ochrony, systemów teleinformatycznych, systemów sterowania przemysłowego, danych, urządzeń i innych zasobów infrastruktury krytycznej, w tym zasady dostępu zdalnego, jeżeli ma on zastosowanie.

3. Opracowuje się i wdraża procedury reagowania w zakresie:

1) niezwłocznego zwrotu wszystkich aktywów przekazanych pracownikowi, podwykonawcy lub usługodawcy, w szczególności sprzętu, identyfikatorów, kart dostępu, dokumentów, nośników danych, kluczy oraz urządzeń służących uwierzytelnianiu;

2) niezwłocznego odebrania, zablokowania albo zmiany uprawnień i dostępów fizycznych lub teleinformatycznych, w tym zmiany haseł lub kodów współdzielonych oraz aktualizacji rejestrów dostępu, w przypadku rozwiązania stosunku pracy, zakończenia współpracy albo zaistnienia zagrożenia lub incydentu związanego z działalnością pracownika, podwykonawcy lub usługodawcy.

4. Raz do roku i po każdej zmianie stanowiska przeprowadza się weryfikację, czy uprawnienia i dostępy przyznane pracownikowi pozostają adekwatne do aktualnie realizowanych obowiązków.

V. Cyberbezpieczeństwo w zakresie przetwarzania i przechowywania informacji

1. W ramach cyberbezpieczenstwa w zakresie przetwarzania i przechowywania informacji:
   1) przydziela się uprawnienia i okresowo weryfikuje poprawność przydzielonych uprawnień do zasobów i usług teleinformatycznych w zakresie wykonywanych obowiązków służbowych;
   2) chroni się tożsamość osób posiadających uprawnienia do zasobów i usług teleinformatycznych poprzez dwuetapową identyfikację, a w przypadku dostępu zdalnego i dostępu do kluczowych zasobów stosuje się rozwiązania oparte o kryptografię lub klucze sprzętowe;
   3) chroni się dostęp do zasobów poprzez logiczny lub fizyczny podział sieci na segmenty i stosuje kontrolę przepływu danych pomiędzy poszczególnymi segmentami;
   4) stosuje się szyfrowanie danych, zgodnie z ich klasyfikacją przyjętą przez operatora, przesyłanych wewnątrz sieci oraz wszystkich danych przesyłanych poza sieć wewnętrzną.
2. Zapewnia się możliwość odzyskania danych poprzez proces tworzenia kopii zapasowych przy założeniu, że wykonywane są minimum 3 kopie, które są przechowywane w minimum 2 różnych lokalizacjach z czego jedna jest przechowywana poza siedzibą podmiotu lub w chmurze obliczeniowej.

3. Dokonuje się weryfikacji, czy rozwiązania określone w ust. 1 i 2 zostały ustanowione i obejmują wszystkie wymagane tymi przepisami elementy. Weryfikacji nie przeprowadza się, w przypadku posiadania ważnego certyfikatu potwierdzającego zgodność systemu zarządzania bezpieczeństwem informacji z PN-EN ISO/IEC 27001, którego zakres obejmuje zasoby teleinformatyczne związane z funkcjonowaniem infrastruktury krytycznej.

VI. Cyberbezpieczeństwo systemów sterowania przemysłowego

1. W ramach cyberbezpieczeństwa systemów sterowania przemysłowego (OT):
   1) ogranicza się dostęp do kodów, aplikacji i sieci zarządzających urządzeniami i systemami sterowania przemysłowego wyłącznie do osób, dla których dostęp jest niezbędny ze względu na realizowane obowiązki służbowe;
   2) w przypadku podwykonawców i serwisantów udziela się wyłącznie czasowego dostępu do systemów sterowania przemysłowego, po uprzedniej weryfikacji danych osoby ubiegającej się o taki dostęp, przy czym uprawnienia są nadawane na pisemny wniosek przełożonego albo innej osoby wskazanej w umowie zawartej z operatorem;
   3) zapewnia się stały nadzór nad osobami, o których mowa w pkt 2;
   4) prowadzi się ewidencję obejmującą dane osoby, której udzielono dostępu, dane osoby nadzorującej, okres udzielenia dostępu oraz czynności wykonane w tym okresie;
   5) stosuje się rozwiązania techniczne lub organizacyjne eliminujące możliwość przełamania ochrony sieci OT przez nośniki i urządzenia wykorzystywane przez podwykonawców i serwisantów;
   6) zapewnia się fizyczną separację systemów IT i OT z wykorzystaniem bram jednokierunkowych lub logiczną separację systemów IT i OT za pomocą strefy zdemilitaryzowanej (DMZ) z mechanizmami segregacji komunikacji między sieciami OT i IT na potrzeby badania stanu sieci OT i zbierania danych generowanych w ramach tej sieci;
   7) przechowuje się kody źródłowe lub oprogramowanie służące do sterowania systemami OT oraz kolejne wersje tych kodów lub oprogramowania z możliwością przywrócenia ostatniej poprawnie działającej wersji;
   8) przechowuje się we własnych zasobach dane generowane przez systemy OT, które zostały zakwalifikowane jako istotne dla celów operacyjnych lub diagnostycznych, przez okres wynikający z analizy ryzyka;
   9) prowadzi się analizę danych generowanych przez systemy OT, w szczególności w celu wykrywania anomalii w pracy systemów sterowania przemysłowego oraz rekonstrukcji zdarzeń;
2. W przypadku powierzenia obsługi urządzeń i systemów sterowania przemysłowego (OT) podmiotowi zewnętrznemu:

1) żąda się od usługodawcy wszelkich danych generowanych przez urządzenia i systemy OT i przechowuje te dane we własnych zasobach operatora (jeżeli umowa z usługodawcą nie przewiduje udostępniania tych danych, stosuje się postanowienia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828).
2) prowadzi się analizę danych generowanych przez systemy OT, w szczególności w celu wykrywania anomalii w pracy systemów sterowania przemysłowego oraz rekonstrukcji zdarzeń, w oparciu o zasoby własne albo zasoby innego podmiotu niż podmiot, któremu powierzono obsługę urządzeń i systemów OT;
3) zapewnia się w umowie z podmiotem, któremu powierzono obsługę urządzeń i systemów sterowania przemysłowego, że podmiot ten, w czasie obowiązywania umowy oraz po jej zakończeniu, niezależnie od przyczyny zakończenia, jest obowiązany do zachowania poufności, integralności i dostępności danych generowanych przez urządzenia i systemy OT oraz do zachowania poufności informacji związanych z realizacją umowy;
4) wdraża się mechanizmy czasowego dostępu do systemów sterowania przemysłowego po wcześniejszej weryfikacji danych osoby ubiegającej się o taki dostęp i po wcześniejszym zarchiwizowaniu danych, które mogą być zmieniane w wyniku udzielonego dostępu.

3. W przypadku stosowania lokalnych pulpitów operatorskich (Human Machine Interface HMI) zapewnia się ich ochronę przed nieupoważnionym dostępem fizycznym, ogranicza ich funkcjonalność wyłącznie do interfejsów użytkownika i blokuje możliwość dostępu do portów fizycznych urządzenia.
4. Jeżeli do sterowania wykorzystywana jest sieć bezprzewodowa dokonuje się separacji tej sieci od pozostałych sieci wewnętrznych, szyfruje transmisję danych, wyłącza rozgłaszanie SSID (service set identifier), blokuje dostęp do sieci poprzez mechanizm dozwolonych adresów MAC oraz ogranicza zasięg sieci wyłącznie do stref, gdzie dostęp do sieci jest wymagany.
5. Dokonuje się weryfikacji, czy rozwiązania, o których mowa w ust. 1–4, zostały ustanowione i obejmują wszystkie wymagane tymi przepisami elementy.

Weryfikacji nie przeprowadza się, w przypadku posiadania ważnego certyfikatu potwierdzającego zgodność systemu zarządzania bezpieczeństwem systemów sterowania przemysłowego z:

1) PN-EN IEC 62443-2-1, lub
2) PN-ISO/IEC 27019 - w przypadku operatorów w sektorze energetycznym, lub
3) PN-EN ISO/IEC 27001, którego zakres obejmuje systemy sterowania przemysłowego związane z funkcjonowaniem infrastruktury krytycznej.

VI. Cyberbezpieczeństwo przetwarzania danych w chmurze obliczeniowej

1. W ramach cyberbezpieczeństwa przetwarzania danych w chmurze obliczeniowej w zawieranej umowie z dostawcą usługi przestrzega się następujących zasad:
   1) dostawca usługi posiada siedzibę albo oddział na terytorium państwa członkowskiego Unii Europejskiej i występuje wobec operatora w charakterze strony umowy;
   2) prawo właściwe dla umowy z dostawcą jest prawem polskim albo prawem innego państwa członkowskiego Unii Europejskiej;
   3) dane pozostają wyłączną własnością i pod kontrolą operatora;
   4) dane są szyfrowane zarówno w spoczynku, jak i podczas transmisji;
   5) dostawca zapewnia wybór lokalizacji centrum lub centrów przetwarzania danych, w tym w postaci regionu, dokonywany z uwzględnieniem kategorii przetwarzanych danych;
   6) dostawca, dla świadczonej usługi, posiada wdrożony system zarządzania bezpieczeństwem informacji wraz z ważnym certyfikatem zgodności z PN-EN ISO/IEC 27001, wydanym przez właściwą w tym zakresie jednostkę certyfikującą;
   7) dostawca, dla świadczonej usługi posiada wdrożony system zarządzania ciągłością działania, wraz z ważnym certyfikatem zgodności z PN-EN ISO 22301, wydanym przez właściwą w tym zakresie jednostkę certyfikującą; przy czym przez system zarządzania ciągłością działania rozumie się część systemu zarządzania operatora obejmującą politykę, role i odpowiedzialności, procesy planowania, wdrażania, realizacji, monitorowania, przeglądu i doskonalenia, a także dokumentację, służącą zapewnieniu ciągłości działania;
   8) dostawca zapewnia kontraktowo standard dostępności rozwiązania chmurowego na poziomie nie niższym niż 99%;
   9) dostawca zapewnia kontraktowo odpowiedzialność za swoich poddostawców, których lista jest dostępna dla operatora;
   10) dostawca zapewnia kontraktowo proces zgłaszania incydentów bezpieczeństwa;
   11) dostawca zapewnia bezpośrednie wsparcie techniczne na terytorium Rzeczypospolitej Polskiej;
   12) dostawca przeprowadza okresowe audyty bezpieczeństwa, których zakres obejmuje świadczoną usługę, oraz udostępnia operatorowi ich wyniki.

2. Na wypadek zagrożenia utraty własnych obiektów w których przetwarzane są dane opracowuje się i okresowo aktualizuje Plan Ewakuacji Danych do Chmury Obliczeniowej.
3. Na wypadek konieczności odbudowy zasobów po incydencie cyberbezpieczeństwa zawiera się umowy z podmiotem lub ekspertami zewnętrznymi, w których określa się:
   1) wymóg posiadania przez personel realizujący czynności na rzecz operatora poświadczeń bezpieczeństwa albo upoważnień do dostępu do informacji niejawnych, o których mowa w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych na poziomie odpowiadającym klauzuli tajności informacji, do których dostęp może być niezbędny w toku odbudowy zasobów;
   2) wymóg posiadania przez podmiot, z którym zawarto umowę, zdolności do ochrony informacji niejawnych o klauzuli „zastrzeżone” lub wyższej, potwierdzonej zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;
   3) zasady udzielania personelowi, o którym mowa w pkt 1, czasowego dostępu niezbędnego do usunięcia następstw incydentu, w tym zakres tego dostępu oraz tryb jego ewidencjonowania.
4. Opracowuje się i stale aktualizuje plan lub plany postępowania z incydentami cyberbezpieczeństwa. Plany uwzględniają komunikację z podmiotami zewnętrznymi, w tym z Policją i innymi służbami, dostawcami usług sieciowych, właściwym Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) oraz mediami.

VII. Bezpieczeństwo prawne

1. W ramach bezpieczeństwa prawnego zapewnia się:
   1) zgodność procesów ochrony infrastruktury krytycznej z przepisami prawa;
   2) ochronę kluczowych zasobów infrastruktury krytycznej przed działaniami prawnymi innych podmiotów.
2. W zakresie zgodności z przepisami:
   1) opracowuje się i stosuje mechanizm systematycznej identyfikacji nowych zmieniających się przepisów, norm, wytycznych, standardów, regulacji oraz wymagań dotyczących infrastruktury krytycznej;
   2) komunikuje się zmiany właściwym pracownikom i komórkom organizacyjnym;
   3) implementuje się obowiązki wynikające ze zmian otoczenia prawnego i monitoruje ich wdrażanie,
   4) każdorazowo przy zawieraniu umów z dostawcami i podwykonawcami dokonuje się analizy ryzyka wynikającego z tych umów pod kątem wpływu na ciągłość i bezpieczeństwo infrastruktury krytycznej.
3. Ochrona kluczowych zasobów obejmuje:
   1) tytuł prawny (w szczególności: własność, użytkowanie, licencje) do kluczowych zasobów niezbędnych do funkcjonowania infrastruktury krytycznej;
   2) tytuły prawne do kluczowych zasobów (umowy, decyzje administracyjne, licencje, zgody regulacyjne), które są udokumentowane i aktualizowane;
   3) wymagania dla zawieranych umów z dostawcami lub usługodawcami, które uwzgledniają:
      a) zakres odpowiedzialności, w tym odpowiedzialność za szkody,
      b) zasady weryfikacji kompetencji pracowników dostawcy lub usługodawcy,
      c) zasady usuwania wykrytych podatności, których wykorzystanie może powodować ryzyko zakłócenia funkcjonowania infrastruktury krytycznej, a w przypadku oprogramowania uwzględnia zasady dostępu do kodu źródłowego zarówno w trakcie obowiązywania umowy jak i po jej zakończeniu,
      d) mechanizmy unikania uzależnienia od jednego dostawcy (vendor lock - VL),
      e) maksymalny dopuszczalny czas reakcji serwisu (umowy SLA).
4. Opracowuje się procedury wymiany informacji z właściwym wojewodą, ministrem i Dyrektorem Rządowego Centrum Bezpieczeństwa o zagrożeniach

i incydentach mogących spowodować zakłócenia w funkcjonowaniu infrastruktury krytycznej, w tym o zagrożeniach związanych z działalnością prawną innych podmiotów, obejmujących w szczególności:

1) możliwość przejęcia udziałów;
2) zmianę struktury właścicielskiej mogącą naruszać zasady kontroli inwestycji bezpośrednich;
3) zmianę struktury właścicielskiej stwarzającą ryzyko naruszenia obowiązujących sankcji.

VIII. Ciągłość działania

1. W zakresie ciągłości działania:
   1) opracowuje się, stosuje i aktualizuje dokumentację w zakresie systemu zarządzania ciągłością działania obejmującą:
      a) role poszczególnych osób w systemie,
      b) analizę wpływu biznesowego, rozumianą jako proces identyfikacji procesów krytycznych dla ciągłości działania infrastruktury krytycznej, oceny skutków ich zakłócenia w czasie oraz ustalenia wymagań dotyczących zasobów niezbędnych do ich odtworzenia,
      c) analizę zagrożeń dla procesów krytycznych, przez które rozumie się procesy, których zakłócenie, wstrzymanie lub nieplanowana przerwa w realizacji mogłyby spowodować niedopuszczalne zakłócenie funkcjonowania infrastruktury krytycznej,
      d) strategię ciągłości działania,
      e) plan ciągłości działania, przez który rozumie się udokumentowany zbiór procedur określających sposób postępowania w przypadku zakłócenia, służących utrzymaniu lub przywróceniu realizacji procesów krytycznych w określonym czasie i na określonym poziomie,
      f) scenariusze testów i raportów z przeprowadzonych testów i przeglądów;
   2) minimum raz na dwa lata dokonuje się analizy poprawności działania systemu ciągłości działania bazując na wynikach audytów, wynikach testów i przeglądów oraz wnioskach z zaistniałych incydentów;
   3) prowadzi się doskonalenie systemu ciągłości działania.
2. Na wypadek wystąpienia incydentu lub sytuacji kryzysowej:
   1) sporządza się plan zarządzania kryzysowego opisujący zasady organizacji postępowania jednostki kierującej i koordynującej działaniami podejmowanymi w ramach reakcji na zdarzenie kryzysowe;
   2) sporządza się plany/procedury awaryjne koncentrujące się na przywróceniu/wznowieniu działania procesów i zasobów po wystąpieniu awarii, incydentu lub sytuacji kryzysowej;
   3) sporządza się plany/procedury odtworzenia utraconych zasobów;

4) ustala się docelowy czas przywrócenia przez który rozumie się maksymalny czas od wystąpienia zakłócenia, do momentu w którym następuje wznowienie realizacji procesu krytycznego;

5) ustala się docelowy moment przywrócenia kluczowych procesów, przez który rozumie się maksymalny dopuszczalny zakres utraty danych, wyrażony jako odstęp czasu poprzedzający wystąpienie zakłócenia, do którego dane muszą zostać odtworzone w celu wznowienia realizacji procesu krytycznego;

3. Dokonuje się weryfikacji, czy rozwiązania określone w ust. 1–2 zostały ustanowione i obejmują wszystkie wymagane elementy. Weryfikacji nie przeprowadza się w przypadku posiadania ważnego certyfikatu potwierdzającego zgodność systemu zarządzania ciągłością działania z PN-EN ISO 22301.