REGULAMIN BEZPIECZEŃSTWA FIZYCZNEGO I ŚRODOWISKOWEGO

Spis treści:

§ 1.

Organizacja bezpieczeństwa fizycznego i środowiskowego

1. Działaniami w zakresie zapewniania bezpieczeństwa fizycznego i środowiskowego w Agencji bezpośrednio kierują: Administrator Zabezpieczeń Fizycznych w zakresie ochrony osób i mienia oraz administrator obiektu, w zakresie bezpieczeństwa środowiskowego, a w szczególności prawa budowlanego i ochrony przeciwpożarowej.
2. Administrator Zabezpieczeń Fizycznych sprawuje nadzór funkcjonalny nad działaniami realizowanymi przez agencje ochrony zabezpieczające obiekty Agencji.
3. Dyrektor komórki właściwej ds. bezpieczeństwa informacji w Centrali ARiMR a Inspektor Bezpieczeństwa Informacji w Oddziale Regionalnym lub Administrator Zabezpieczeń Fizycznych przynajmniej raz w roku organizuje szkolenie pracowników w zakresie ochrony osób i mienia Agencji.

§ 2.

Podstawowe zasady bezpieczeństwa fizycznego i środowiskowego

1. Środki bezpieczeństwa fizycznego dotyczą:
   1) rozmieszczenia i granic stref bezpieczeństwa,
   2) konstrukcji budowlanych wyznaczających granice stref bezpieczeństwa,
   3) sposobu zabezpieczenia wejścia do obiektu oraz do stref bezpieczeństwa,
   4) stosowania bezpośredniej ochrony fizycznej,
   5) stosowania systemu sygnalizacji napadu i włamania,
   6) stosowania systemu monitoringu wizyjnego,
   7) stosowania mechanicznych zabezpieczeń technicznych,
   8) dostępu do obszarów bezpiecznych oraz wykonywanie prac w obszarach bezpiecznych.
2. Bezpieczeństwo środowiskowe obejmuje:
   1) stosowanie urządzeń ochrony przeciwpożarowej,
   2) zabezpieczenie przed zalaniem wodą,
   3) zapewnienie właściwych warunków pracy w zakresie temperatury i wilgotności powietrza,
   4) stosowanie środków ochrony odgromowej na liniach telekomunikacyjnych,
   5) stosowanie zabezpieczeń przeciwprzepięciowych.
3. Zakres stosowania środków bezpieczeństwa fizycznego i środowiskowego wynika z przeprowadzonego i udokumentowanego szacowania ryzyka.
4. Szacowanie ryzyka i określanie wymagań bezpieczeństwa przeprowadza się w oparciu o:
   1) charakterystykę obiektu i pełnione przez niego funkcje, w szczególności rodzaj umieszczonych w nim zasobów podlegających ochronie (ludzie, dokumentacja, sprzęt komputerowy, itp.),
   2) określenie kategorii potencjalnych zagrożeń obiektu,
   3) opis topografii, konstrukcji obiektu i architektury, najbliższego otoczenia (zabezpieczenia budowlane i mechaniczne, ogrodzenie, bramy, furty, oświetlenie, miejsca do parkowania, drogi komunikacyjne i ewakuacyjne, inne budowle i elementy towarzyszące),
   4) odnotowane w przeszłości czyny przestępcze (rodzaj i typ czynu przestępczego, działania zewnętrzne, wewnętrzne, data, rozmiary, wartość szkody, wynik śledztwa),

5) aktualny stan bezpieczeństwa obiektu,
6) opis i ocenę funkcjonalności i poprawności zainstalowanych technicznych systemów zabezpieczenia, ich poprawności eksploatacji i aktualny stan techniczny (poziom technologiczny, sprawność, dokumentacja, serwisowanie),
7) aktualny stan ochrony fizycznej obiektu,
8) opis stosowanych procedur i rozwiązań organizacyjnych,
9) wnioski co do odpowiedniości (w stosunku do rodzaju i stopnia zagrożeń) kompletności i poprawności zastosowanych zabezpieczeń (mechanicznych, technicznych i proceduralno – organizacyjnych),
10) propozycje doskonalenia systemów oraz procedur ochrony obiektu.

§ 3.

Zapewnianie bezpieczeństwa fizycznego i środowiskowego

1. Dyrektor komórki właściwej ds. bezpieczeństwa informacji, dyrektorzy oddziałów regionalnych, kierownicy biur powiatowych ustalają podział powierzchni biurowych zajmowanych przez komórki i jednostki organizacyjne Agencji na:
   1) strefy administracyjne, do których dostęp posiadają wszyscy pracownicy Agencji,
   2) strefy bezpieczeństwa, do których dostęp jest ograniczony do osób posiadajacych specjalne prawa dostępu.
   3) strefy obsługi klienta, do której dostęp posiadają beneficjenci ARiMR, goście i inni interesanci.
2. Ochrona stref administracyjnych i stref bezpieczeństwa sprawowana jest na zasadach określonych w:
   1) przepisach o ochronie osób i mienia.
   2) planie ochrony obiektu (jeżeli został opracowany),
   3) niniejszym Regulaminie.
3. Na granicy strefy administracyjnej odbywa się kontrola ruchu osobowego i materiałowego. Wejścia gości do strefy administracyjnej jest rejestrowane. Wzór rejestru wejść stanowi załącznik nr 2 do niniejszego Regulaminu.
4. Strefa bezpieczeństwa powinna być ustalona na obszarze wydzielonym solidnymi konstrukcjami budowlanymi. Za solidne konstrukcje budowlane uznaje się takie, których ściany zewnętrzne i stropy budynków, w których zlokalizowane są strefy bezpieczeństwa, posiadają klasę odporności włamaniowej równoważnej murowi o grubości 25 cm wykonanemu z pełnej cegły. Natomiast pomieszczenia stref bezpieczeństwa powinny mieć ściany o odporności włamaniowej równoważnej murowi o grubości 12,5 cm. Zasady organizacji strefy bezpieczeństwa kancelarii niejawnej w ARiMR określają odrębne regulacje.
5. Wszystkie osoby przebywające w strefie administracyjnej muszą posiadać identyfikatory noszone w widocznym miejscu. Pracownicy Agencji posiadają identyfikatory zawierające: zdjęcie, imię i nazwisko, symbol lub nazwę jednostki organizacyjnej lub komórki organizacyjnej. Goście posiadają identyfikatory z napisem „Gość" i numerem identyfikatora.
6. Goście mogą poruszać się w obrębie strefy administracyjnej wyłącznie w asyście pracownika odpowiedzialnego za ich przyjęcie. Pracownik ten przed wprowadzeniem gości do strefy administracyjnej winien dopilnować pobrania przez nich w strefie obsługi klienta lub na stanowisku recepcyjnym identyfikatorów, o których mowa w ust. 5.

7. W jednostkach organizacyjnych, w których odbywa się masowa obsługa interesantów dopuszcza się wydzielenie z części strefy administracyjnej strefy obsługi klienta, w której goście – interesanci mogą przebywać bez identyfikatorów. Strefa obsługi klienta musi być oddzielona od pozostałych części strefy administracyjnej kontrolowanymi przejściami.
8. W przypadku stosowania systemu kontroli dostępu musi być to system z klasą dostępu B. Dla stref administracyjnych i bezpieczeństwa wymagana jest klasa rozpoznania 2 na wejściu i klasa rozpoznania 0 na wyjściu.
9. Klasa dostępu B oznacza, że w systemie możliwe jest przyznawanie dostępu w określonych godzinach oraz, że transakcje uzyskania dostępu są rejestrowane. Klasa rozpoznania 0 oznacza, że dostęp uzyskiwany jest bez sprawdzania tożsamości (np. wyjście po naciśnięciu przycisku). Klasa rozpoznania 2 oznacza, że dostęp uzyskiwany jest po sprawdzeniu tożsamości na podstawie danych zawartych na identyfikatorze lub na podstawie danych biometrycznych. (Według Polskiej Normy PN-EN 50133-1 - „Systemy alarmowe. Systemy kontroli dostępu. Wymagania systemowe").
10. Wszystkie drzwi z kontrolą dostępu muszą być zaopatrzone w urządzenia samozamykające.
11. Kontrolę ruchu osobowego i materiałowego na granicy strefy administracyjnej może sprawować pracownik ze strefy obsługi klienta lub stanowiska recepcyjnego, który wydaje identyfikatory gościom.
12. Pomieszczenia biurowe w strefie administracyjnej posiadają zamki klasy 0. Pomieszczenia w strefach bezpieczeństwa powinny posiadać zamki klasy C lub klasy 7 zabezpieczenia (wg normy PN-EN 12209:2005) oraz drzwi antywłamaniowe klasy C (wg normy PN-EN 14351-1) lub drzwi o odporności co najmniej klasy 4 (wg normy PN-EN 1627:2011), z odpornością ogniową co najmniej 60 minut.
13. Wejście oraz wyjście ze stref bezpieczeństwa jest rejestrowane. Rejestruje się tożsamość osób, cel pobytu oraz czas ich wejścia i wyjścia. Wzór rejestru stanowi załącznik nr 1 do niniejszego Regulaminu.

§ 4.

Zarządzanie kluczami

1. Klucze od pomieszczeń przechowywane są u ochrony obiektu, z tym, że klucze do pomieszczeń w strefach bezpieczeństwa muszą być zdawane na przechowanie w zaplombowanych pojemnikach.
2. Jeżeli obiekt nie posiada stałej ochrony po godzinach pracy, to klucze od pomieszczeń biurowych muszą być zdawane przez wyznaczonych pracowników Agencji w zaplombowanej kasecie pracownikowi firmy realizującej ochronę obiektu na zasadzie monitoringu, a następnego dnia roboczego pobierane z tej firmy. Przyjęcie kluczy przez pracownika firmy sprawującej monitoring jest równoznaczne z przyjęciem obiektu pod ochronę. Szczegółowe zasady takiej procedury określa umowa pomiędzy Agencją a firmą sprawującą ochronę. W przypadku braku możliwości obecności pracownika firmy monitorującej, klucze muszą być zdawane wyznaczonemu pracownikowi Agencji w celu zabezpieczenia ich w zaplombowanej kasetce, a następnego dnia roboczego pracownik ten zobowiązany jest wydać klucze upoważnionym pracownikom. Dopuszcza się, w biurach powiatowych Agencji, trwałe wydanie kluczy zewnętrznych do obiektu osobom funkcyjnym posiadającym indywidualny kod dostępu do Systemu Sygnalizacji Włamania i Napadu (SSWiN), w takim przypadku jeden z kluczy musi być zdeponowany w jednostce monitorującej obiekt, klucze

wewnętrzne mogą być przechowywane w skrytce wewnątrz obiektu, osoba otwierająca obiekt odpowiedzialna jest za wydanie kluczy, osoba zamykająca obiekt odpowiedzialna jest za przyjęcie do skrytki wszystkich kluczy wewnętrznych.

3. Klucze wydaje się na podstawie rejestru osób upoważnionych do ich pobierania. Fakt wydania kluczy i przyjęcia ich na przechowanie musi być odnotowany. Rejestr wydawania i zdawania kluczy prowadzony jest w formie papierowej w książce wydawania kluczy lub w formie elektronicznej w dedykowanym systemie elektromechanicznego depozytora kluczy. Wzór książki wydawania i zdawania kluczy stosowany w jednostce organizacyjnej określa Administrator Zabezpieczeń Fizycznych danej jednostki w porozumieniu z Inspektorem Bezpieczeństwa Informacji. Prowadzony rejestr musi określać:
   - nr pomieszczenia / nr klucza,
   - dokładną godzinę pobrania / zdania,
   - imię i nazwisko osoby pobierającej / zdającej bądź jej identyfikator (w systemie elektronicznego depozytora),
   - czytelny podpis osoby pobierającej / zdającej oraz przyjmującej klucz na przechowanie (w przypadku rejestru w formie papierowej).
4. Za przyznanie i odebranie prawa do pobierania kluczy do konkretnego pomieszczenia odpowiedzialny jest:
   1) w Centrali – dyrektor komórki organizacyjnej, któremu podlega dane pomieszczenie,
   2) w oddziale regionalnym – kierownicy biur w stosunku do pomieszczeń zajmowanych przez pracowników biura lub kierownik biura oddziału regionalnego w stosunku do pozostałych pomieszczeń oddziału,
   3) w biurze powiatowym – kierownik biura powiatowego.
5. Za organizację wydawania kluczy do pomieszczeń odpowiada administrator obiektu lub Administrator Zabezpieczeń Fizycznych. Organizacja wydawania kluczy musi być uzgodniona z:
   1) w Centrali Agencji - dyrektorem komórki właściwej ds. bezpieczeństwa informacji,
   2) w oddziale regionalnym i biurach powiatowych - Inspektorem Bezpieczeństwa Informacji.
6. Klucze do szaf i mebli biurowych, w których przechowywane są dokumenty zawierające informacje wrażliwe, nie mogą po zakończeniu pracy pozostawać w zamkach. Za organizację przechowywania takich kluczy odpowiada Administrator Zabezpieczeń Fizycznych, w uzgodnieniu z:
   1) w Centrali Agencji – dyrektorem komórki organizacyjnej, któremu podlega pomieszczenie z szafami i meblami biurowymi zawierającymi informacje wrażliwe,
   2) w oddziale regionalnym i biurze powiatowym – kierownikiem komórki organizacyjnej, któremu podlega pomieszczenie z szafami i meblami biurowymi zawierającymi informacje wrażliwe.
7. Zasady organizacji przechowywania kluczy do szaf, sejfów i mebli biurowych, w których przechowuje się informacje niejawne określają odrębne regulacje.

§ 5.

Zarządzanie uprawnieniami w systemie kontroli dostępu

1. W przypadku zastosowania systemu kontroli dostępu uprawnienia są jednoznacznie powiązane z urządzeniami aktywującymi przejście, które pełnią także role identyfikatorów.

2. Wstęp do poszczególnych stref, o których mowa w § 3 ust. 1 jest ograniczony tylko do tych osób, które uzyskały stosowne uprawnienia.
3. Uprawnienia przyznawane są zgodne z profilem dostępu (zakresem odpowiedzialności i uprawnień) na danym stanowisku pracy. Uprawnienia dostępu są nadawane wyłącznie w zakresie wynikającym z zajmowanego stanowiska i potrzebą wykonywania obowiązków służbowych na danym stanowisku pracy. Bezzasadne nadawanie uprawnień do pomieszczeń będzie kwalifikowane jako incydent związany z naruszeniem bezpieczeństwa informacji.
4. Za przyznawanie, zmianę oraz odbieranie uprawnień dostępu do stref bezpieczeństwa odpowiedzialny jest:
   1) w Centrali Agencji - dyrektor komórki organizacyjnej, któremu podlega dane pomieszczenie,
   2) w oddziale regionalnym i biurze powiatowym - kierownik biura oddziału regionalnego w stosunku do pomieszczeń oddziału regionalnego lub kierownik biura powiatowego w stosunku do pomieszczeń tego biura.
5. Przyznawanie, zmiana oraz odbieranie uprawnień jest realizowane w systemie kontroli dostępu przez Administratora Zabezpieczeń Fizycznych.
6. Administrator Zabezpieczeń Fizycznych jest obowiązany bezzwłocznie zablokować uprawnienia dostępu w przypadku:
   1) zgłoszenia przez pracownika Agencji utraty lub podejrzenia utraty urządzenia aktywującego przejście,
   2) zgłoszenia telefonicznego, za pośrednictwem faksu lub poczty elektronicznej, potwierdzonego bezzwłocznie pisemnym wnioskiem bezpośredniego przełożonego pracownika.
7. Ponowne nadanie uprawnień dostępu w przypadku zaistnienia okoliczności opisanych w ust. 6 pkt 1) odbywa się zgodnie z zasadami określonymi w ust. 4 i 5.
8. Uprawnienia dostępu są regularnie przeglądane zgodnie z zasadami opisanymi w Regulaminie nadzoru.

§ 6.

Pomieszczenia i zasoby chronione

1. Wnoszenie i wynoszenie do i ze stref bezpieczeństwa komputerowych nośników danych może mieć miejsce tylko w przypadkach wynikających z procedur eksploatacji zainstalowanego tam sprzętu teleinformatycznego.
2. Strefy bezpieczeństwa powinny być chronione systemem sygnalizacji włamania i napadu.
3. W uzasadnionych przypadkach, zarówno strefy administracyjne jak i strefy bezpieczeństwa, powinny być poddane monitoringowi wizyjnemu.
4. Strefy bezpieczeństwa nie posiadają oznakowania wewnątrz lub na zewnątrz, które wskazywałyby na to, że znajdują się w nich szczególnie chronione zasoby.
5. W strefach bezpieczeństwa dopuszcza się przebywanie osób bez uprawnień dostępu do tych stref tylko w wyjątkowych przypadkach, za zezwoleniem:
   1) dla pomieszczeń BP - kierownika biura powiatowego,
   2) dla pomieszczeń OR - kierownika Biura OR,
   3) dla pomieszczeń Centrali:

a) dyrektora komórki właściwej ds. informatyki dla pomieszczeń serwerowni, węzłów teletechnicznych i biblioteki kodów źródłowych,

b) dyrektora komórki właściwej ds. organizacyjno-gospodarczych dla pomieszczeń archiwum zakładowego,

c) Pełnomocnika ds. Ochrony Informacji Niejawnych w przypadku strefy bezpieczeństwa, w której przetwarzane są informacje niejawne.

6. Pobyt osoby, która nie posiada uprawnień do przebywania w strefie bezpieczeństwa jest rejestrowany. Za prowadzenie rejestru odpowiedzialne są osoby wskazane w ust. 5, a wpisy dokonywane są pod nadzorem osoby uprawnionej do przebywania w danej strefie.
7. Serwery, aktywne i pasywne urządzenia sieci teleinformatycznej, centrale telefoniczne i archiwa muszą być umieszczone w strefach bezpieczeństwa.
8. Zasoby, którym nadano status zasobu kluczowego podlegają szczególnej ochronie i są dodatkowo zabezpieczane przed pożarem i zalaniem.
9. Rozmieszczenie sprzętu służącego do przetwarzania informacji, zarówno w obszarach bezpiecznych, jak i w pozostałych pomieszczeniach, poprzedzone jest udokumentowanym szacowaniem ryzyk związanych z systemami zabezpieczeń technicznych oraz systemami wspomagającymi (wentylacyjno-klimatyzacyjnymi, zasilającymi, wodno-kanalizacyjnymi, grzewczymi).

§ 7.

Bezpieczeństwo środowiskowe

1. Przy planowaniu zabezpieczeń technicznych i organizacyjnych, ich rodzaju i siły, bierze się pod uwagę ryzyka związane z występującymi lokalnie zagrożeniami, takimi jak pożar, zalanie, trzęsienie ziemi, wybuch, wyładowania atmosferyczne, niepokoje społeczne i inne formy naturalnych lub spowodowanych przez działania umyślne bądź błędy człowieka katastrof. Ponadto analizie jest poddawany wpływ sąsiedztwa innych obiektów lub lokalnych instalacji i dróg (np. pożar w sąsiednim budynku, woda przeciekająca przez dach, powódź, bliska katastrofa komunikacyjna, eksplozja, zamieszki uliczne).
2. Pomieszczenia, w których zlokalizowane są zasoby kluczowe, wyposaża się w:
   1) system sygnalizujący wystąpienie pożaru,
   2) system klimatyzacji w serwerowniach.
3. Nie prowadzi się instalacji wodnych przez pomieszczenia, w których zlokalizowane są zasoby kluczowe do przetwarzania informacji (serwery, centra danych).
4. Urządzenia zapewniające bezpieczeństwo środowiskowe poddawane są regularnej kontroli zgodnie z obowiązującymi przepisami prawa, normami oraz zaleceniami producentów.
5. Na wypadek zagrożenia pożarem dla każdej z lokalizacji jednostek organizacyjnych Agencji opracowuje się instrukcje przeciwpożarowe. Ciągi komunikacyjne obiektów muszą być zaopatrzone w tabliczki informujące o kierunku ewakuacji i w miarę potrzeby wyposażone w oświetlenie awaryjne.
6. W przypadku, jeśli któreś z wymagań w zakresie bezpieczeństwa środowiskowego nie może być z przyczyn obiektywnych spełnione, Administrator Zabezpieczeń Fizycznych sporządza protokół opisujący: rodzaj odstępstwa, ryzyko wynikające z odstępstwa, zastosowane środki ochrony doraźnej lub zamiennej, plan dojścia do rozwiązania docelowego.

7. Parametry środowiska, w którym pracuje sprzęt systemu teleinformatycznego zaliczany do zasobów kluczowych, tj. temperatura, jest monitorowana w celu natychmiastowego wykrycia odchyleń, które mogłyby mieć negatywne skutki dla tego sprzętu.
8. Budynek, w którym znajdują się systemy teleinformatyczne wskazane w ust. 7 wyposażony jest, zgodnie z przepisami ppoż., w samoczynnie załączające się oświetlenie awaryjne (bezpieczeństwa i ewakuacyjne).
9. Oświetlenie bezpieczeństwa stosowane jest w pomieszczeniach, w których nawet krótkotrwałe wyłączenie oświetlenia podstawowego może spowodować zagrożenie zdrowia i życia podczas ewakuacji.
10. W przypadku, gdy oświetlenie bezpieczeństwa działa, co najmniej przez 2 godziny, nie ma potrzeby stosowania oświetlenia ewakuacyjnego.

§ 8.

Wymagania dla systemów wspomagających

1. Jeżeli jest to możliwe, należy projektować nadmiarową, modułową klimatyzację tak, aby w przypadku awarii lub przeglądu serwisowego jednego modułu pozostałe były w stanie zapewnić wymagane parametry środowiskowe, w szczególności środowiska eksploatacyjnego w serwerowniach.
2. Rozmieszczenie w obiekcie kanałów oraz czerpni należy zaprojektować uwzględniając ryzyko takich zdarzeń, jak przedostanie się przez nie do pomieszczeń chronionych wody, środków niebezpiecznych czy też zwierząt.
3. W przypadku prowadzenia instalacji wodno-kanalizacyjnych i grzewczych w sąsiedztwie (również nad lub bezpośrednio pod pomieszczeniem) serwerowni i pomieszczeń, w których usytuowano infrastrukturę techniczną służącą do przetwarzania w krytycznych systemach Agencji, należy wdrożyć systemy zapewniające wykrycie i alarmowanie w przypadku zalania pomieszczenia oraz zainstalować środki umożliwiające szybkie usunięcie wody (cieczy).
4. Przy ocenie sprawności instalacji wodno – kanalizacyjnej i grzewczej należy uwzględnić jej współdziałanie z innymi systemami wspomagającymi, takimi jak system klimatyzacyjno - wentylacyjny oraz w szczególności system przeciwpożarowy.

§ 9.

Eksploatacja technicznych systemów zabezpieczeń oraz systemów wspomagających

1. Systemy zabezpieczenia technicznego Agencji muszą spełniać następujące funkcje:
   1) zabezpieczenia budowlane i zabezpieczenia mechaniczne muszą zagwarantować uniemożliwienie dostępu osobom niepowołanym do chronionych pomieszczeń i urządzeń oraz zabezpieczyć osoby i mienie przed potencjalnymi zagrożeniami,
   2) system sygnalizacji napadu i włamania (SSWiN) musi zapewnić skuteczne przekazanie sygnału o realnym zagrożeniu do wskazanych osób, miejsc i urządzeń,
   3) system monitorowania w przypadku wystąpienia alarmu musi zapewnić podjęcie odpowiednich działań stosownych do zaistniałego zdarzenia.

4) system monitoringu (CCTV) musi zapewnić, poprzez rozmieszczone kamery, rozpoznanie rodzaju zagrożenia i śledzenie rozwoju sytuacji, prowadzenie obserwacji obrazu z kilku kamer oraz automatyczną jednoczesną rejestrację tych obrazów,
5) system kontroli dostępu (SKD) musi zabezpieczyć chronione pomieszczenie (grupę pomieszczeń) lub wydzieloną strefę przed dostępem do nich osób nieuprawnionych.

2. Wszystkie systemy zabezpieczeń podlegają regularnym przeglądom dokonywanym przez Administratora Zabezpieczeń Fizycznych lub pod jego nadzorem przez osoby posiadające odpowiednie uprawnienia. Przegląd polega na sprawdzeniu poprawności działania danego systemu zgodnie z dokumentacja techniczno-eksploatacyjną systemu. Przeglądy każdego systemu zabezpieczeń wykonywane są zgodnie z harmonogramem ustalonym przez Administratora Zabezpieczeń Fizycznych w porozumieniu z:
   1) w Centrali Agencji - dyrektorem komórki właściwej ds. bezpieczeństwa,
   2) w oddziale regionalnym i biurach powiatowych - Inspektorem Bezpieczeństwa Informacji.
3. Przeglądy dokonywane przez Administratora Zabezpieczeń Fizycznych co 6 miesięcy obejmują dodatkowo sprawdzenie stanu technicznego nośników elektronicznych SKD (identyfikatorów) przeznaczonych dla gości, jeśli mają zastosowanie w danej jednostce organizacyjnej.
4. Przeglądy systemów zabezpieczeń poza ustalonym harmonogramem przeprowadzane są każdorazowo w przypadku wystąpienia incydentów zagrażających lub mogących powodować zagrożenie dla bezpieczeństwa osób i mienia (np. katastrofa budowlana w sąsiedztwie obiektu, tąpnięcie, kolizja drogowa powodująca szczególne zagrożenie w pobliżu budynku, pożar, roboty budowlane w sąsiednich budynkach, ewakuacja osób i mienia z budynku, interwencja służb ratunkowych mająca wpływ na stan techniczny obiektu, wystąpienie anomalii pogodowych, itp.).
5. Administrator Zabezpieczeń Fizycznych odnotowuje przeprowadzenie przeglądu w dzienniku przeglądów prowadzonym dla każdego z funkcjonujących w Agencji systemów zabezpieczeń. Dziennik przeglądu zawiera następujące informacje:
   1) datę i czas przeglądu,
   2) dane personalne wykonującego przegląd,
   3) wynik przeglądu,
   4) dane personalne osoby nadzorującej/kontrolującej,
   5) uwagi z przeglądu.

   Dopuszcza się prowadzenie dziennika w systemie elektronicznym lub wersji elektronicznej umieszczonej na serwerze plików (fileserver).
6. Administrator Zabezpieczeń Fizycznych nadzoruje i dokumentuje bieżące prace konserwacyjne, w tym wymianę lub prostą naprawę elementów każdego z systemów zabezpieczeń, które nie wymagają posiadania stosownych uprawnień specjalistycznych. Pozostałe prace konserwacyjne wykonują pracownicy podmiotów zewnętrznych posiadający stosowne uprawnienia. Prace konserwacyjne polegają na wykonaniu niezbędnych czynności mających na celu utrzymanie systemu w sprawności techniczno-użytkowej zgodnie z dokumentacją techniczno-eksploatacyjną systemu. Prace konserwacyjne dla wszystkich systemów zabezpieczenia przeprowadzane są nie rzadziej niż raz na 12 miesięcy.
7. Administrator Zabezpieczeń Fizycznych nadzoruje i dokumentuje prace serwisowe przeprowadzane przez uprawnionych pracowników podmiotów zewnętrznych. Prace serwisowe

polegają na wykonaniu niezbędnych czynności mających na celu przywrócenie sprawności techniczno-użytkowej systemu zgodnie z dokumentacją techniczno-eksploatacyjną systemu.

8. Wymiany lub naprawy o wysokim poziomie technologicznym dokonuje podmiot zewnętrzny posiadający stosowne uprawnienia producenta, dystrybutora wyrobu lub specjalistyczne urządzenia do naprawy lub wymiany.
9. Dla każdego systemu alarmowego oraz dla każdego innego systemu technicznego zabezpieczeń funkcjonującego w Agencji jest założony dziennik/system rejestrowania zawierający:
   1) rejestr wyposażenia,
   2) rejestr zdarzeń,
   3) rejestr prac konserwacyjnych,
   4) rejestr prac serwisowych.

§ 10.

Eksploatacja zabezpieczeń mechanicznych

1. Do zabezpieczeń mechanicznych zalicza się: kraty, żaluzje, okiennice, folie antywłamaniowe, zamki w drzwiach (w szczególności te, do których bezpośredni dostęp mają osoby postronne), inne zabezpieczenia otworów okiennych, włazów, kanałów wentylacyjnych, rygle, kłódki, zamki, zasuwy z blokadą mechaniczną.
2. Zabezpieczenia mechaniczne muszą być zamontowane przez uprawniony podmiot zgodnie z warunkami technicznymi wynikającymi z certyfikatu lub aprobaty technicznej.
3. Zabezpieczenia mechaniczne podlegają przeglądom przeprowadzanym przez Administratora Zabezpieczeń Fizycznych, zgodnie z harmonogramem - dotyczy tylko tych zabezpieczeń, które są dostępne dla osób postronnych i nie ma możliwości realizacji nadzoru przez inne systemy zabezpieczeń. Harmonogram przeglądów jest ustalany przez Administratora Zabezpieczeń Fizycznych w porozumieniu z:
   1) w Centrali Agencji - dyrektorem komórki właściwej ds. bezpieczeństwa,
   2) w oddziale regionalnym i biurach powiatowych – osobami pełniącymi funkcję Inspektora Bezpieczeństwa Informacji.
4. Przeglądy polegają na sprawdzeniu stanu technicznego elementów zabezpieczenia mechanicznego, przeprowadzanych w następujący sposób:
   1) w przypadku krat, żaluzji, okiennic i innych zabezpieczeń otworów okiennych, włazów, kanałów wentylacyjnych:
      a) sprawdzenie mocowań do murów (np. poprzez poruszenie elementów zabezpieczenia w pionie i poziomie i obserwacji reakcji elementów mocujących),
      b) sprawdzenie istnienia odkształceń mechanicznych na poszczególnych elementach, przy zastosowaniu metody porównawczej z opisem w dokumentacji technicznej,
      c) sprawdzenie występowania śladów po próbach penetracji lub usunięcia zabezpieczenia np. w postaci opiłków, śladów tynku, rysach na elementach zabezpieczeń, itp.,
      d) sprawdzić stan powłok lakierniczych i zabezpieczeń antykorozyjnych elementów narażonych na bezpośrednie działanie czynników atmosferycznych lub innych szkodliwych czynników dla mechanizmów kłódek, zamków, rygli (szczególnie kurz, pył),

2) w przypadku kłódek i zamków - sprawdzenie działania kluczy zapasowych oraz mechanizmu ryglującego przez otwarcie i zamknięcie kłódek i zamków, przegród mechanicznych i budowlanych,

3) w przypadku rygli i zasuw z blokadą mechaniczną - porównanie położenia elementów ruchomych z opisem w dokumentacji technicznej.

5. Przynajmniej dwa razy do roku Administrator Zabezpieczeń Fizycznych dokonuje oceny stanu powłoki lakierniczej, śladów korozji elementów narażonych na bezpośrednie działanie czynników atmosferycznych lub innych szkodliwych czynników dla mechanizmów.

6. Wycofane z użycia elementy zabezpieczeń mechanicznych zawierające informacje o kodzie zamków (klucze, wkładki, karty elektroniczne) niszczone są mechanicznie.

7. Zakup zamków (mechanizmów zamkowych) i wkładek dokonywany jest w sposób określany jako „zakup z półki".

8. Dla stref bezpieczeństwa każda faza procesu wymiany mechanizmów zamkowych, w tym zakup i transport, montaż zamków (mechanizmów zamkowych) i wkładek wykonywany jest co najmniej przez dwie osoby (w tym przez Administratora Zabezpieczeń Fizycznych sprawującego bezpośredni nadzór).

9. Wycofanie elementu zabezpieczenia mechanicznego przeprowadza się po uzyskaniu informacji od dystrybutora/producenta wyrobu o konieczności jego wymiany lub po uzyskaniu informacji o pojawieniu się metod/narzędzi powodujących przełamanie zabezpieczenia lub obniżenie jego właściwości.

10. Z zastrzeżeniem ust. 8, koniec okresu ważności certyfikatu lub świadectwa kwalifikacyjnego nie stanowi przyczyny demontażu elementu zabezpieczenia.

§ 11.

Eksploatacja zabezpieczeń techniczno-budowlanych

1. Do zabezpieczeń techniczno-budowlanych zalicza się drzwi, śluzy, ściany, stropy, ogrodzenia (wykonane z różnych materiałów), furtki, bramy, zapory, szlabany, kołowroty (w szczególności te, do których bezpośrednio dostęp mają osoby postronne).

2. Zabezpieczenia techniczno-budowlane podlegają przeglądowi przeprowadzanym przez Administratora Zabezpieczeń Fizycznych, zgodnie z harmonogramem - dotyczy tylko tych zabezpieczeń, które są dostępne dla osób postronnych i nie ma możliwości realizacji nadzoru przez inne systemy zabezpieczeń. Harmonogram przeglądów jest ustalany przez Administratora Zabezpieczeń Fizycznych w porozumieniu z:

   1) w Centrali Agencji - dyrektorem komórki właściwej ds. bezpieczeństwa,

   2) w oddziale regionalnym i biurach powiatowych – osobami pełniącymi funkcję Inspektora Bezpieczeństwa Informacji.

3. Przeglądy polegają na sprawdzeniu stanu technicznego elementów zabezpieczeń techniczno-budowlanych, przeprowadzanych w następujący sposób:

   1) sprawdzenie mocowań elementów ruchomych i elementów umocowanych na stałe do podłoża (np. poprzez poruszenie elementów konstrukcji zabezpieczenia i obserwacji reakcji elementów mocujących),

   2) sprawdzenie istnienia odkształceń mechanicznych na poszczególnych elementach, przy zastosowaniu metody porównawczej z opisem w dokumentacji technicznej,

3) sprawdzenie występowania śladów po próbach penetracji lub usunięcia zabezpieczenia np. w postaci opiłków, śladów tynku, rysach na elementach zabezpieczeń, rdzy, itp.,

4) sprawdzenie mechanizmów ryglowych (zamków, rygli, itp.),

5) porównanie położenia elementów ruchomych z opisem w dokumentacji technicznej.

4. Przynajmniej dwa razy do roku Administrator Zabezpieczeń Fizycznych dokonuje oceny stanu powłoki lakierniczej, śladów korozji elementów zabezpieczeń techniczno-budowlanych narażonych na bezpośrednie działanie czynników atmosferycznych lub innych czynników środowiskowych.

5. Wymiana/naprawa zabezpieczeń dokonywana jest pod nadzorem administratora obiektu w porozumieniu z Administratorem Zabezpieczeń Fizycznych.

§ 12.

Eksploatacja systemów okablowania zasilającego i teleinformatycznego w zakresie konstrukcyjno-mechanicznym

1. W skład systemów okablowania w zakresie konstrukcyjno-mechanicznym wchodzą: trakty kablowe (listwy PCV, szyny, rury, przepusty), osłony włazów i studzienek, szafy dystrybucyjne, tablice, krosownice.

2. Systemy okablowania znajdujące się w obszarze dostępnym publicznie podlegają przeglądom przeprowadzanym przez Administratora Zabezpieczeń Fizycznych oraz Administratora Systemu. Harmonogram przeglądów jest ustalany przez Administratora Zabezpieczeń Fizycznych w porozumieniu z:

   1) w Centrali Agencji - dyrektorem komórki właściwej ds. bezpieczeństwa,

   2) w oddziale regionalnym i biurach powiatowych – osobami pełniącymi funkcję Inspektora Bezpieczeństwa Informacji.

3. Przeglądy polegają na sprawdzeniu stanu technicznego (konstrukcyjno-mechanicznego) elementów systemu okablowania z dokumentacją techniczną.

4. Przeglądy zabezpieczeń elektronicznych systemów okablowania polegają na sprawdzeniu poprawności funkcjonowania np. systemów sygnalizacji włamania zastosowanych do zabezpieczenia szaf dystrybucyjnych, krosownic lub innych zabezpieczeń.

5. Przeglądy przeprowadzane lub nadzorowane przez Administratora Zabezpieczeń Fizycznych powinny obejmować sprawdzenie:

   1) ciągłości struktury (mocowanie listew) traktów kablowych w miejscach ogólnie dostępnych – np. narażonych na uszkodzenia mechaniczne spowodowane przez przenoszenie przedmiotów o dużych gabarytach (biurko, szafa), ruch osobowy,

   2) stanu powłoki lakierniczej, śladów korozji elementów narażonych na bezpośrednie działanie czynników atmosferycznych lub innych szkodliwych czynników dla obudów, osłon lub innych zabezpieczeń systemów okablowania,

   3) czy występują ślady po próbach penetracji lub usunięcia zabezpieczenia, np. w postaci opiłków, śladów tynku, rysach na elementach zabezpieczeń, itp.

6. Przeglądy prowadzone lub nadzorowane przez Administratora Systemu powinny obejmować sprawdzenie:

1) przestrzegania zasad ochrony okablowania oraz punktów połączeń okablowania (inspekcja pod kątem podłączonych nieautoryzowanych urządzeń przechwytujących, rejestrujących, transmitujących i zniekształcających sygnał transmisyjny),
2) zamknięcia szaf, tablic, osłon włazów i studzienek należących do Agencji,
3) zgodności stanu faktycznego z dokumentacją techniczną okablowania,
4) stanu technicznego instalacji poprzez wykonanie pomiarów okablowania.

§ 13.

Eksploatacja elektronicznych systemów zabezpieczeń

1. Do elektronicznych systemów zabezpieczeń zalicza się systemy sygnalizacji włamania i napadu (SSWiN), systemy kontroli dostępu (SKD), systemy telewizji dozorowej (CCTV) oraz inne systemy współdziałające z elektronicznymi systemami zabezpieczeniowymi, np. system oświetlenia podczerwienią dla systemu CCTV.
2. Elektroniczne systemy zabezpieczeniowe i systemy współdziałające podlegają przeglądom przeprowadzanym przez Administratora Zabezpieczeń Fizycznych zgodnie z harmonogramem i zakresem konserwacji systemu przeprowadzanej przez pracownika podmiotu zewnętrznego, posiadającego licencję pracownika zabezpieczenia technicznego.
3. Przeglądy SSWiN są przeprowadzane przez Administratora Zabezpieczeń Fizycznych i obejmują, w zależności od zastosowanego rozwiązania technicznego, sprawdzenie:
   1) trybu pracy urządzeń wg wskazań paneli sterujących poprzez porównanie z dokumentacją techniczno-eksploatacyjną systemu,
   2) działania przycisków sygnalizacji napadu/przycisków wezwania pomocy,
   3) działania poszczególnych klawiatur strefowych poprzez załączanie i rozłączanie systemu wprowadzając odpowiedni kod,
   4) ilości i rozmieszczenia klawiatur strefowych zgodnie z danymi w dzienniku systemu.
4. Czynności konserwacyjne dokonywane przez pracownika podmiotu zewnętrznego są przeprowadzane nie rzadziej niż raz na 12 miesięcy i obejmują:
   1) sprawdzenie prawidłowości funkcjonowania systemu SSWiN w zakresie określonym w dokumentacji technicznej,
   2) sprawdzenie ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego; (wymiana akumulatorów zgodnie z harmonogramem załączonym do dokumentacji technicznej systemu),
   3) sprawdzenie poprawności działania akustycznych lub optycznych sygnalizatorów alarmowych,
   4) sprawdzenie czujników systemu,
   5) sprawdzenie mocowania czujek do podłoża (uchwytów, ścian); szczególnie dotyczy to stref ogólnego i ograniczonego dostępu oraz znajdujących się poza pomieszczeniami Agencji (płaszczyzna ścian, ogrodzenia).
5. Przeglądy SKD są przeprowadzane przez Administratora Zabezpieczeń Fizycznych i obejmują, w zależności od zastosowanego rozwiązania technicznego, sprawdzenie:
   1) trybu pracy urządzeń wg wskazań paneli sterujących bądź aplikacji zarządzającej, poprzez porównanie z dokumentacją systemu,
   2) działania przycisków otwierających wyjścia z czytnikami działającymi jednostronnie, w tym działania przycisków ewakuacyjnych w przypadku, gdy SKD nie współpracuje z systemem ppoż.,

   3) działania czytników systemu z odpowiednią kartą dostępu,
   4) mocowania czytników, samozamykaczy, zamków elektromagnetycznych drzwi i przejść, w tym istnienia śladów prób penetracji (rysy, wgniecenia, próby podważania, demontażu),
   5) ilości i rozmieszczenia czytników zgodnie z danymi w dzienniku systemu,
   6) limitu użytkowników systemu.
6. Przeglądy dokonywane przez Administratora Zabezpieczeń Fizycznych co 6 miesięcy obejmują dodatkowo sprawdzenie stanu technicznego nośników elektronicznych SKD (identyfikatorów) przeznaczonych dla gości, jeśli mają zastosowanie w danej jednostce organizacyjnej.
7. Czynności konserwacyjne dokonywane przez pracownika podmiotu zewnętrznego są przeprowadzane nie rzadziej niż raz na 12 miesięcy i obejmują sprawdzenie:
   1) prawidłowości funkcjonowania systemu SKD w zakresie określonym w dokumentacji technicznej,
   2) ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego, w tym wymiana akumulatorów zgodnie z harmonogramem załączonym do dokumentacji technicznej systemu,
   3) działania części elektromechanicznych (elektrozaczepów, trzymaczy elektromagnetycznych, śluz, tripodów itp.).
8. Przeglądy CCTV są przeprowadzane przez Administratora Zabezpieczeń Fizycznych i obejmują sprawdzenie:
   1) trybu pracy urządzeń rejestrujących poprzez porównanie z dokumentacją techniczno-eksploatacyjną na podstawie wskazań paneli sterujących informujących o trybie pracy urządzeń,
   2) jakości obrazu i pola obserwacji na monitorach poprzez porównanie z opisem oraz zdjęciem obrazu wykonanym w trybie dziennym i nocnym,
   3) wymiany nośników w urządzeniu rejestrującym zgodnie z dokumentacją techniczną systemu,
   4) poprawności pracy urządzeń rejestrujących poprzez nagranie i odtworzenie przebiegu zdarzeń w trybie czasu rzeczywistego oraz losowo wybranego zdarzenia w czasie przeszłym.
9. Czynności konserwacyjne dokonywane przez pracownika podmiotu zewnętrznego są przeprowadzane nie rzadziej niż raz na 12 miesięcy i obejmują:
   1) sprawdzenie ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego,
   2) wyłączenie monitora i sprawdzenie „poświaty" (efekt „wypalania się" kineskopu objawiający się „pozostawaniem" obrazu na ekranie po odłączeniu źródła sygnału),
   3) sprawdzenie jakości zarejestrowanego obrazu z kamer rejestrujących punkty newralgiczne (szczególnie z kamer zewnętrznych, rejestracja wykonana w godzinach nocnych),
   4) sprawdzenie zapisu z wewnętrznych pamięci kamer (jeśli kamery posiadają taką pamięć),
   5) sprawdzenie mocowania kamer zewnętrznych, jeśli są narażone na działania czynników atmosferycznych i innych np. konary drzew,
   6) sprawdzenie działania wycieraczek, obwodów, grzałek (elementy przeciwśniezne, jeśli zostały zainstalowane),
   7) sprawdzenie działania głowic obrotowych i funkcji „zoom" (optyczny i elektroniczny),
   8) sprawdzenie mocowania reflektorów podczerwieni i oświetlenia sztucznego związanego z CCTV (np. halogeny włączane automatycznie – z czasowym wyłącznikiem).

§ 14.

Systemy wspomagające oświetlenie

1. Przeglądy systemu są przeprowadzane przez Administratora Zabezpieczeń Fizycznych zgodnie z harmonogramem i obejmują sprawdzenie systemów sterujących (włączających i wyłączających oświetlenie). Harmonogram przeglądów jest ustalany przez Administratora Zabezpieczeń Fizycznych w porozumieniu z:
   1) w Centrali Agencji - dyrektorem komórki właściwej ds. bezpieczeństwa,
   2) w oddziale regionalnym i biurach powiatowych – osobami pełniącymi funkcję Inspektora Bezpieczeństwa Informacji.
2. Czynności konserwacyjne dokonywane przez pracownika podmiotu zewnętrznego są przeprowadzane nie rzadziej niż raz na 12 miesięcy i obejmują:
   1) sprawdzenie zasilania podstawowego i awaryjnego,
   2) sprawdzenie innych elementów, zgodnie z dokumentacją systemu.

§ 15.

Systemy transmisji sygnałów alarmowych do centrów monitoringu

1. Przeglądy systemu transmisji sygnałów alarmowych do centrów monitoringu są przeprowadzane przez podmiot zewnętrzny zgodnie z harmonogramem i obejmują sprawdzenie trybu pracy urządzenia wg wskazań paneli sterujących poprzez porównanie z dokumentacją systemu.
2. Czynności konserwacyjne dokonywane przez pracownika podmiotu zewnętrznego są przeprowadzane nie rzadziej niż raz na 12 miesięcy i obejmują:
   1) sprawdzenie ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego (wymiana akumulatorów zgodnie z harmonogramem załączonym do dokumentacji technicznej systemu),
   2) sprawdzenie systemu anten, masztów, stanu uziemienia,
   3) sprawdzenie/potwierdzenie prawidłowego działania systemu/systemów w centrum monitoringu.

§ 16.

Rejestrowanie i przechowywanie informacji w elektronicznych systemach zabezpieczeń

1. Zdarzenia rejestrowane w elektronicznych systemach zabezpieczeniowych podlegają regularnym przeglądom przeprowadzanym przez Administratora Zabezpieczeń Fizycznych.
2. Częstość przeglądu zapisów wyznacza się na podstawie pojemności pamięci zdarzeń danego systemu:
   1) przed czynnością włączenia/wyłączenia dla systemów, których pamięć zdarzeń jest kasowana podczas włączania/wyłączania, lub
   2) przed zapełnieniem pamięci systemu powodującej nadpisywanie danych (wg danych w dokumentacji techniczno-eksploatacyjnej systemu),

   nie rzadziej jednak niż raz 6 miesięcy.

3. Zapisy w systemach telewizji dozorowej (CCTV), kontroli dostępu (SKD) sygnalizacji włamania i napadu (SSWiN) oraz w dziennikach/rejestrach wejścia/wyjścia podlegają wyrywkowej kontroli korelacji rejestrowanych zdarzeń dokonywanej przez Administratora Zabezpieczeń Fizycznych.
4. W przypadku wystąpienia incydentu naruszenia bezpieczeństwa lub podejrzenia wystąpienia, którego okoliczności mogą być wyjaśnione dzięki zapisom z rejestrów elektronicznych systemów zabezpieczeń, Administrator Zabezpieczeń Fizycznych zapewnia utrwalenie zapisów z tych rejestrów elektronicznych systemów zabezpieczeń zgodnie z Regulaminem zarządzania incydentami.

§ 17.

Prowadzenie dokumentacji związanej z technicznymi systemami zabezpieczeń

1. Administrator Zabezpieczeń Fizycznych jest odpowiedzialny za prowadzenie wszelkich ewidencji, wykazów uprawnień, rejestrów, w tym rejestrów elektronicznych systemów zabezpieczeń.
2. Wszelka dokumentacja wskazana w ust. 1 jest klasyfikowana jako informacja wrażliwa.
3. Administrator Zabezpieczeń Fizycznych jest odpowiedzialny za aktualność i kompletność dokumentacji technicznych własnych systemów zabezpieczeń (tzn. dokumentacji powykonawczej, zmian w tej dokumentacji, aktualnych plików konfiguracyjnych systemów i urządzeń).

§ 18.

Zarządzanie zapisami pochodzącymi z elektronicznych systemów zabezpieczeń

1. Administrator Zabezpieczeń Fizycznych jest odpowiedzialny za utrzymanie rejestrów elektronicznych własnych systemów zabezpieczeń (SKD, SSWiN, CCTV). Okres przechowywania zapisów pochodzących z elektronicznych systemów zabezpieczeń powinien wynosić co najmniej 14 dni.
2. W przypadku powierzenia utrzymania rejestrów systemów kontroli dostępu, sygnalizacji napadu i włamania lub telewizji dozorowej podmiotowi zewnętrznemu, umowa z usługodawcą musi zapewniać Agencji skuteczną kontrolę nad zapisami przez umieszczenie w niej:
   1) warunków i czasu przechowywania rejestrów (min. 14 dni),
   2) wymagań bezpieczeństwa w odniesieniu do rejestrów,
   3) zasad dostępu Agencji do przechowywanych zapisów, w tym uzyskania kopii stanowiących materiał dowodowy, jeśli zachodzi taka potrzeba,
   4) sposobów komunikowania się Agencji z usługodawcą, w tym potwierdzania dostarczenia kopii rejestrów w trybie awaryjnym,
   5) zakres odpowiedzialności usługodawcy za utratę lub uszkodzenie rejestrów.
3. W przypadku stwierdzenia incydentu naruszenia bezpieczeństwa informacji Administrator Zabezpieczeń Fizycznych wykonuje kopie rejestrów elektronicznych systemów zabezpieczeń dla celów dowodowych.

Załącznik nr 1 do Regulaminu bezpieczeństwa fizycznego i środowiskowego – Wzór rejestru wejścia/wyjścia do strefy bezpieczeństwa

Rejestr osób przebywających w strefie bezpieczeństwa BP..../OR....

Lp.	Imię i nazwisko osoby otwierającej	Imię i nazwisko osoby wchodzącej	Data i godzina wejścia	Data i godzina wyjścia	Cel wejścia

Załącznik nr 2 do Regulaminu bezpieczeństwa fizycznego i środowiskowego – Wzór rejestru wejścia/wyjścia gości do strefy administracyjnej

Rejestr gości przebywających w strefie Administracyjnej Centrali/BP..../OR....

Lp.	Czas wejścia	Imię i nazwisko gościa	Rodzaj dokumentu tożsamości	Nr dokumentu tożsamości	Imię i nazwisko osoby wizytowanej	Nr identyfikatora	Czas wyjścia