Załącznik nr 11
do Zasad Zarządzania
Bezpieczeństwa Informacji

Załącznik nr 3

do Umowy nr .....

z dnia .....

WYTYCZNE BEZPIECZEŃSTWA INFORMACJI DLA KONTRAHENTÓW I JEDNOSTEK ZEWNĘTRZNYCH

(zbiór zasad regulujących działania kontrahentów/jednostek zewnętrznych, realizujących dostawy lub świadczących usługi na rzecz Agencji Rezerw Materiałowych)

Dział I
Zasady wynikające z Polityki Bezpieczeństwa Informacji

§ 1

1. Polityka Bezpieczeństwa Informacji obejmuje wszystkich kontrahentów, jednostki zewnętrzne i ich pracowników, jeśli w trakcie realizacji umowy posiadają dostęp do zasobów informacyjnych oraz zasobów do przetwarzania informacji Agencji Rezerw Materiałowych.
2. Ochronie podlegają niżej wymienione zasoby:
   1) dane i informacje przetwarzane w Agencji Rezerw Materiałowych, niezależnie od ich formy i nośnika;
   2) oprogramowanie i sprzęt wykorzystywany do przetwarzania, przesyłania i przechowywania danych i informacji w Agencji Rezerw Materiałowych;
   3) pomieszczenia zawierające kluczowy sprzęt teleinformatyczny, jak również te, w których przechowuje się dokumenty zawierające informacje niejawne oraz inne informacje prawnie chronione;
   4) pozostałe mienie wykorzystywane przez Agencję Rezerw Materiałowych lub będące jej własnością;
   5) relacje z podmiotami zewnętrznymi współpracującymi z Agencją Rezerw Materiałowych;
   6) wizerunek Agencji Rezerw Materiałowych.
3. Ustanowienie Polityki Bezpieczeństwa Informacji ma na celu zapewnienie ochrony informacji rozumiane jako zachowanie poufności, dostępności i integralności informacji przetwarzanych w Agencji Rezerw Materiałowych.
4. Naruszenie postanowień Polityki Bezpieczeństwa Informacji przez kontrahenta może spowodować natychmiastowe rozwiązanie umowy oraz stanowi podstawę do żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeśli taki obowiązek wynika z zawartej umowy.
5. Jednostki zewnętrzne mają dostęp do zasobów informacyjnych Agencji Rezerw Materiałowych na podstawie odrębnych przepisów lub upoważnień.
6. Odpowiedzialność za bezpieczeństwo informacji obejmuje wszystkie jednostki Agencji Rezerw Materiałowych oraz wszystkie sytuacje, w których informacje związane z działalnością Agencji Rezerw Materiałowych są przetwarzane poza jej siedzibą.
7. Postanowień Polityki Bezpieczeństwa Informacji, o których mowa w tym zbiorze nie stosuje się do przedsiębiorców zawierających umowy z Agencją Rezerw Materiałowych w zakresie gospodarowania rezerwami strategicznymi i gospodarowania zapasami ropy naftowej i paliw. W tym przypadku zobowiązuje się dyrektorów jednostek/komórek organizacyjnych do stosowania przepisów gwarantujących właściwe zabezpieczenie informacji zawartych w umowie.

Dział II
Bezpieczeństwo fizyczne

Rozdział 1
Obszary bezpieczne

§ 2

1. Powierzchnia biurowa zajmowana przez Centralę Agencji Rezerw Materiałowych jest dzielona na:
   1) strefę administracyjną;
   2) strefę dedykowaną.
2. Powierzchnia biurowa zajmowana przez Oddziały Terenowe i Składnice Agencji Rezerw Materiałowych jest dzielona na:
   1) strefę administracyjną;
   2) strefę ochronną.
3. Powierzchnia biurowa zajmowana przez Dział Obsługi Szkoleniowo-Konferencyjnej Agencji Rezerw Materiałowych jest dzielona na:
   1) strefę administracyjną;
   2) strefę ochronną;
   3) strefę dedykowaną.
4. Strefa administracyjna to powierzchnia będąca w użytkowaniu Agencji Rezerw Materiałowych.
5. Strefa dedykowana to wydzielona część strefy administracyjnej lub ochronnej wyposażona w dodatkowe, niezależne systemy zabezpieczeń.

6. Strefa ochronna to specjalnie wydzielona część obiektu, poddana szczególnej kontroli wejść, wyjść i przebywania, wyposażona w dodatkowe, niezależne systemy zabezpieczeń.
7. Kontrola dostępu w Składnicach Agencji Rezerw Materiałowych odbywa się przez Wewnętrzną Służbę Ochrony, która rejestruje osobę w książce ewidencji ruchu osobowego i wydaje mu przepustkę.
8. W siedzibie Centrali Agencji Rezerw Materiałowych, Oddziałach Terenowych oraz Centrum Zapasowym samodzielne wejście do stref dostępu objętych elektronicznym systemem kontroli dostępu odbywa się wyłącznie na podstawie karty magnetycznej.
9. Wszystkie drzwi z kontrolą dostępu powinny być zaopatrzone w urządzenie samozamykające.
10. Wstęp do strefy dedykowanej ograniczony jest tylko do osób, które uzyskały stosowne uprawnienia z zastrzeżeniem ust. 11–13.
11. Dopuszcza się przebywanie osób bez uprawnień dostępu do stref dedykowanych w tych strefach w określonym celu w:
    1) Centrali za wiedzą i zgodą właściwego Dyrektora Biura lub osoby go zastępującej;
    2) Centrum Zapasowym za zezwoleniem (jednorazowym lub czasowym) osób odpowiedzialnych za nadzór nad poszczególnymi strefami (odpowiednio: Dyrektora BT, Dyrektora BIL, POIN);
    3) w OT Agencji Rezerw Materiałowych za zezwoleniem Dyrektora OT Agencji Rezerw Materiałowych;
    4) w Składnicach za zezwoleniem Kierownika Składnicy ARM.
12. Przebywanie osób bez uprawnień dostępu do stref dedykowanych w tych strefach możliwe jest wyłącznie pod nadzorem osoby posiadającej uprawnienia dostępu do danej strefy.
13. Pobyt osoby, która nie posiada uprawnień do przebywania w serwerowni, musi zostać odnotowany. W książce ewidencji osób wchodzących do serwerowni należy zarejestrować jej dane, a także datę i godzinę jej wejścia i wyjścia.
14. Wnoszenie i wynoszenie do i ze stref dedykowanej i stref ochronnych elektronicznych nośników informacji może mieć miejsce tylko i wyłącznie w przypadkach wynikających z procedur eksploatacji zainstalowanego tam sprzętu teleinformatycznego.
15. Ciągi komunikacyjne obiektów Agencji Rezerw Materiałowych są zaopatrzone w tabliczki informujące o kierunku ewakuacji i w miarę potrzeby wyposażone w oświetlenie awaryjne. Zgodnie z przepisami prawa opracowane są instrukcje przeciwpożarowe.
16. Drogi ewakuacyjne są oznaczone.

Rozdział 2
Wejścia i wyjścia do Agencji Rezerw Materiałowych osób nie będących pracownikami Agencji oraz pracowników OT i Składnic Agencji Rezerw Materiałowych

§ 3

1. Wejścia i wyjścia do strefy administracyjnej danej komórki/jednostki organizacyjnej osób nie będących pracownikami Agencji Rezerw Materiałowych wymagają potwierdzenia możliwości przyjęcia Gościa i zaewidencjonowania przez:
    1) Recepcję w Centrali Agencji Rezerw Materiałowych;
    2) Stanowisko do spraw Kancelaryjno-Biurowych w Oddziałach Terenowych Agencji Rezerw Materiałowych;
    3) Wewnętrzną Służbę Ochrony w Składnicach Agencji Rezerw Materiałowych;
    4) Recepcję Działu Obsługi Szkoleniowo-Konferencyjnej (w przypadku Centrum Zapasowego).
2. Rejestrację Gościa pracownik w Centrali odnotowuje w aplikacji „EWIDENCJA GOŚCI".
3. W Centrum Zapasowym rejestracji Gościa dokonuje pracownik Recepcji Działu Obsługi Szkoleniowo-Konferencyjnej w „Książce ewidencji gości Centrum Zapasowego". W Oddziałach Terenowych/Składnicach rejestracja Gościa odbywa się w sposób określony przez Dyrektora OT/Kierownika Składnicy.
4. Pracownik Recepcji w Centrali/Dziale Obsługi Szkoleniowo-Konferencyjnej, Stanowisko do spraw Kancelaryjno-Biurowych w Oddziałach Terenowych, pracownik Wewnętrznej Służby Ochrony w Składnicy spisuje zgodnie z istniejącą procedurą z dokumentu tożsamości lub legitymacji służbowej imię i nazwisko Gościa, rodzaj i nr dokumentu tożsamości, cel wizyty, godzinę wejścia, imię i nazwisko pracownika Agencji Rezerw Materiałowych przyjmującego Gościa.
5. Gość w Centrali, Centrum Zapasowym oraz w Oddziale Terenowym ARM otrzymuje identyfikator „Gość" a w Składnicy przepustkę jednorazową.

6. Nr identyfikatora odnotowuje: pracownik Recepcji w Centrali ARM w aplikacji „EWIDENCJA GOŚCI", pracownik Recepcji w Dziale Obsługi Szkoleniowo-Konferencyjnej w „Książce ewidencji gości Centrum Zapasowego", pracownik Oddziału Terenowego ARM w rejestrze „Ewidencji gości".
7. Pracownik Recepcji w Centrali odprowadza Gościa do właściwej komórki organizacyjnej, natomiast w Centrum Zapasowym, Oddziałach Terenowych i Składnicach właściwy pracownik odbiera Gościa odpowiednio od pracownika Recepcji, osoby zajmującej Stanowisko do spraw Kancelaryjno-Biurowych albo od Wewnętrznej Służby Ochrony i towarzyszy mu przez cały czas pobytu na terenie Agencji Rezerw Materiałowych lub do momentu przejęcia Gościa przez innego pracownika.
8. Gość ma obowiązek noszenia identyfikatora albo przepustki w miejscu widocznym, o czym powinien go poinformować pracownik wydający identyfikator lub przepustkę.
9. Odprowadzenie Gościa następuje poprzez:
   1) Recepcję w Centrali Agencji Rezerw Materiałowych;
   2) pracownika ARM towarzyszącego Gościowi w Centrum Zapasowym;
   3) Stanowisko do spraw Kancelaryjno-Biurowych w Oddziałach Terenowych Agencji Rezerw Materiałowych;
   4) Wewnętrzną Służbę Ochrony w Składnicach Agencji Rezerw Materiałowych.
10. Pracownik recepcji/Wewnętrznej Służby Ochrony odbiera identyfikator/ przepustkę i odnotowuje godzinę wyjścia.

Rozdział 3
Zasady dostępu do sieci ARM dla pracowników firm zewnętrznych wykonujących zadania na rzecz Agencji

§ 4

1. Pracownicy firm zewnętrznych wykonujący pracę na rzecz Agencji posiadają dostęp tylko do zasobów, które są im potrzebne do realizacji prac na rzecz ARM – dostęp do innych zasobów jest zabroniony.
2. Dostęp do sieci ARM dla pracowników firm zewnętrznych wykonujących prace na rzecz Agencji odbywa się poprzez przygotowane i skonfigurowane stanowisko SFZ (stanowisko dla firmy zewnętrznej).
3. Podłączenie i korzystanie z jakiegokolwiek własnego (nie będącego własnością ARM) sprzętu IT możliwe jest wyłącznie po uzyskaniu zgody Dyrektora Biura Teleinformatyki. Zgoda udzielana jest na formularzu stanowiącym załącznik nr 10 do Zasad Zarządzania Bezpieczeństwem Informacji.
4. Uprawnienia do zasobów ARM pracownikom firm zewnętrznych nadaje upoważniony pracownik BT na wniosek pracownika ARM, który nadzoruje wykonywane prace na podstawie wniosku zaakceptowanego przez Dyrektora Biura Teleinformatyki oraz w przypadku dostępu do zasobów poufnych (ZSI-P) przez Inspektora Bezpieczeństwa Teleinformatycznego oraz Pełnomocnika Prezesa ds. Ochrony Informacji Niejawnych, a w przypadku dostępu do danych osobowych przez Administratora Bezpieczeństwa Informacji. Wzór wniosku zawiera załącznik do ZZBI "Wniosek z dnia ..... o nadanie/odebranie uprawnień do pracy w systemie teleinformatycznym ARM" oraz „Wniosek z dnia ..... o przyznanie/odebranie uprawnień do systemu „ZSI-P ARM" stanowiący załącznik do Procedur Bezpiecznej Eksploatacji systemów niejawnych.
5. Pracownik ARM odpowiedzialny za realizację konkretnej umowy/zamówienia występuje z wnioskiem o nadanie uprawnień do pracy w systemie IT ARM:
   1) we wniosku muszą być określone zasoby;
   2) wniosek nie może dotyczyć nadania uprawnień na czas nieokreślony.
6. Konto blokowane jest każdego dnia na koniec pracy.
7. Wykonawcy dokonujący, w ramach realizacji zadań umowy zmiany w systemach Agencji podlegają nadzorowi ze strony Biura Teleinformatyki. Pracownicy firm zewnętrznych wykonujący pracę na rzecz ARM korzystający z własnego sprzętu wyrażają zgodę na każdorazowy wgląd do logów systemu operacyjnego, procesów oraz usług przez pracowników Agencji, w okresie trwania prac.
8. Dostęp do zasobów sieci ARM dla pracowników firm zewnętrznych wykonujących prace na rzecz Agencji może się odbywać wyłącznie poprzez wydzieloną podsieć (wydzielony vlan).
9. Wykorzystywanie przez pracowników Wykonawcy uprawnień (loginów i haseł) pracowników Agencji do uzyskania dostępu do zasobów Agencji jest stanowczo zabronione.

10. Pracownicy firm zewnętrznych wykonujący pracę na rzecz ARM zobowiązani są do przestrzegania zasad wynikających z „Wytycznych bezpieczeństwa informacji dla kontrahentów i jednostek zewnętrznych".
11. W przypadku zlecenia firmie zewnętrznej prac wymagających dostępu do informacji niejawnych o klauzuli „poufne", oprócz obowiązku zastosowania się do zasad wymienionych w ust. 1-10, wymagane jest posiadanie przez tę firmę dokumentu potwierdzającego zdolność do ochrony informacji niejawnych w postaci „świadectwa bezpieczeństwa przemysłowego" wydanego przez Agencję Bezpieczeństwa Wewnętrznego (ABW) lub Służbę Kontrwywiadu Wojskowego (SKW). Pracownicy wykonujący zadania objęte umową winni posiadać Poświadczenie bezpieczeństwa uprawniające do dostępu co najmniej do klauzuli „poufne".
12. Pracownicy firmy zewnętrznej zobowiązani są do zachowania w tajemnicy wszelkich informacji dotyczących Agencji Rezerw Materiałowych uzyskanych w związku z realizacją zadań na jej rzecz – zarówno w czasie ich realizacji, jak też w terminie późniejszym, wyjąwszy przypadki przewidziane prawem. W przypadku, gdy pracownikowi firmy zewnętrznej przyznany zostanie dostęp do zasobów sieciowych Agencji Rezerw Materiałowych, jest on zobowiązany do podpisania oświadczenia o zachowaniu w tajemnicy wszelkich informacji dotyczących Agencji Rezerw Materiałowych, stanowiącego załącznik nr 1 do niniejszych „Wytycznych Bezpieczeństwa Informacji dla kontrahentów i jednostek zewnętrznych".
13. W przypadku, gdy do wykonania zadań niezbędna jest instalacja oprogramowania na komputerach lub serwerach Agencji Rezerw Materiałowych przez firmę zewnętrzną, firma ta instaluje oprogramowanie, które użytkuje zgodnie z postanowieniami licencyjnymi. Za nieprawidłowości dotyczące wykorzystania oprogramowania zainstalowanego przez firmę zewnętrzną i wykorzystywanego przez nią przy realizacji zadań odpowiedzialność ponosi ta firma.
14. Jeżeli postanowienia regulujące wykonanie zadań nie stanowią inaczej, po ich zakończeniu firma zewnętrzna ma obowiązek usunięcia wszelkich dokonanych przez nią instalacji oprogramowania użytkowanego przy realizacji zadań z komputerów oraz serwerów Agencji Rezerw Materiałowych.

Dział III
Postępowanie w przypadku uzasadnionego podejrzenia naruszenia bezpieczeństwa informacji.

§ 5

1. Incydentem w zakresie bezpieczeństwa jest sytuacja powodująca naruszenie zasad bezpieczeństwa a w szczególności utratę poufności, integralności lub dostępności przetwarzanych informacji. Wdrożenie zasad reagowania na incydenty w zakresie ochrony danych jest istotnym elementem utrzymania odpowiedniego poziomu ich bezpieczeństwa.
2. Do przypadków mogących świadczyć lub świadczących o naruszeniu Zasad Zarządzania Bezpieczeństwem Informacji zalicza się:
   1) nie zabezpieczenie informacji nadzorowanych przed dostępem osób niepowołanych;
   2) odtajnienie kodu dostępu do stref chronionych;
   3) przetwarzanie niezgodnie z instrukcją ochrony informacji niejawnych dokumentów zakwalifikowanych jako „Poufne" lub „Zastrzeżone";
   4) brak właściwego nadzoru nad osobami trzecimi mającymi dostęp do informacji niejawnych;
   5) ujawnienie informacji niejawnych;
   6) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w szczególności wyłamane lub zacinające się zamki, naruszone plomby, nie domykające się bądź wybite okna;
   7) udostępnienie informacji wrażliwych osobom nieupoważnionym;
   8) pozyskiwanie oprogramowania z nielegalnych źródeł;
   9) wprowadzenie do systemu teleinformatycznego treści prawnie zakazanych i chronionych;
   10) instalację oprogramowania niepochodzącego i nieautoryzowanego przez Agencję Rezerw Materiałowych;
   11) naruszenie ochrony informacji w systemie, w szczególności nieautoryzowane logowanie lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu z zewnątrz;
   12) nieautoryzowaną modyfikację to jest dodanie, zmiana, usunięcie lub zniszczenie danych przez osoby nieuprawnione lub uprawnione działające w złej wierze lub jako błąd osoby uprawnionej, w szczególności zmiana zawartych danych, utrata całości lub części danych;

13) nieuprawniony dostęp lub próba dostępu do danych znajdujących się w systemie, w szczególności nieuprawniona praca na koncie użytkownika, istnienie nieautoryzowanych kont dostępu do informacji, pojawienie się nowych lub nie zablokowanie czy nie usunięcie aktualnych kont dostępu;
14) ujawnienie indywidualnych haseł dostępu użytkowników do systemu przetwarzającego informacje;
15) zanotowanie w krótkim czasie dużej liczby nieudanych prób logowania;
16) utratę usługi, urządzenia lub funkcjonalności;
17) pojawianie się nietypowych komunikatów na ekranie;
18) spowolnienie pracy oprogramowania;
19) nieuprawniony dostęp lub próba dostępu do pomieszczeń, gdzie są przetwarzane informacje;
20) wykonywanie nieuprawnionych kopii informacji, w szczególności wydruki, kopie na pendrive lub innym nośniku przenośnym;
21) nieuprawnioną zmianę lub usunięcie informacji zapisanych na kopiach bezpieczeństwa i archiwalnych;
22) utratę nośnika zwierającego informację, w szczególności kradzież lub zaginięcie kopii bezpieczeństwa, wydruku, pendrive czy dysku;
23) niszczenie nośników informacji w niewłaściwy sposób pozwalający na ich odczyt, w szczególności wydruk, pendrive;
24) niewłaściwe nadawanie uprawnień do przetwarzania informacji, a także nadawanie uprawnień osobie nieupoważnionej;
25) brak dostępu do informacji dla podmiotów uprawnionych;
26) inne sytuacje powodujące lub wskazujące na naruszenie bezpieczeństwa informacji w Agencji Rezerw Materiałowych.

3. Kontrahent/jednostka zewnętrzna ma obowiązek zgłaszania wszelkich zdarzeń mogących mieć wpływ na bezpieczeństwo informacji do osoby realizującej daną umowę z ramienia Agencji Rezerw Materiałowych.
4. Naruszenie Zasad Zarządzania Bezpieczeństwem Informacji funkcjonujących w ARM przez kontrahenta może spowodować natychmiastowe rozwiązanie umowy oraz stanowi podstawę do żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeśli taki obowiązek wynika z zawartej umowy.