UMOWA nr 2401-ILZ.023.1……2026
(PROJEKT)

zawarta w Katowicach w dniu / zdalnie w postaci elektronicznej z chwilą złożenia ostatniego z kwalifikowanych podpisów elektronicznych stosownie do wskazania znacznika czasu ujawnionego w szczegółach dokumentu zawartego w postaci elektronicznej *, pomiędzy

** Zamawiający odpowiednio dostosuje zapisy umowy po wyborze najkorzystniejszej oferty dla danej części (w zależności czy wybrany Wykonawca może podpisać Umowę kwalifikowanym podpisem elektronicznym)*

Skarbem Państwa - Izbą Administracji Skarbowej w Katowicach,
ul. Damrota 25, 40-022 Katowice,
NIP: 954-13-02-993, REGON 001021234,
zwaną dalej **Zamawiającym**
reprezentowaną przez:

a

……. z siedzibą w ……., wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS ……., o numerze NIP: …….. i numerze REGON: ……,

/Panią/Panem …….. przedsiębiorcą prowadzącym działalność gospodarczą na podstawie wpisu do Centralnej Ewidencji i Informacji o Działalności Gospodarczej pod nazwą ……. z siedzibą w ……, ul. ……., o numerze NIP: …….. i numerze REGON: ……../*

reprezentowaną /-nym przez: ……*

zwaną /-nym dalej **Wykonawcą**,

a wspólnie **Stronami**

** Zamawiający odpowiednio dostosuje zapisy umowy po wyborze najkorzystniejszej oferty.*

(W przypadku osób prowadzących działalność gospodarczą w formie spółki cywilnej Wykonawca zobowiązany jest do udostępnienia Zamawiającemu umowy spółki wraz ze wszystkimi aneksami).

PREAMBUŁA

Umowa została zawarta w wyniku przeprowadzonego rozpoznania rynku nr 2401-ILZ.261.55.2026 na dostawę kalendarzy ściennych, trójdzielnych oraz książkowych w formacje B5 na rok 2027.

§ 1
PRZEDMIOT UMOWY

Przedmiotem zamówienia jest dostawa 3814 sztuk kalendarzy ściennych trójdzielnych oraz 160 sztuk kalendarzy książkowych w formacie B5 na rok 2027 w cenach zgodnych z Formularzem oferty stanowiącym załącznik nr 1 do Umowy.

§ 2
WARUNKI DOSTAWY

1 Poprzez dostawę Zamawiający rozumie także wyładunek dostarczonego towaru oraz wniesienie go do miejsca wskazanego przez Zamawiającego.

2 Strony ustalają, że koszty i ryzyko dostawy ponosi Wykonawca. Wykonawca ponosi również odpowiedzialność za szkody powstałe w czasie transportu.
3 Wykonawca zobowiązany jest zrealizować dostawę jednorazowo.
4 Przedmiot Umowy powinien być wolny od wad, wykonany starannie i zgodnie z wymogami technicznymi.

§ 3
TERMIN I WARUNKI REALIZACJI UMOWY

1. Wykonawca zobowiązuje się do zrealizowania przedmiotu zamówienia w terminie do **30 listopada 2026 r.**
2. Wykonawca zobowiązuje się dostarczyć przedmiot Umowy do magazynu Izby Administracji Skarbowej w Katowicach, ul. Damrota 25, 40-022 Katowice, zabezpieczony przed zniszczeniem i uszkodzeniem.
3. Za szkody powstałe z powodu nienależytego zabezpieczenia towaru winę ponosi Wykonawca.
4. Dostawa zostanie zrealizowana w dni robocze (od poniedziałku do piątku) w godzinach od 7:00 – 14:00, z wyjątkiem dni ustawowo wolnych od pracy. Wykonawca zobowiązany jest poinformować osobę wyszczególnioną w ust. 6 o terminie dostawy z minimum jednodniowym wyprzedzeniem.
5. Szczegółowy termin dostawy zostanie ustalony przez Wykonawcę z osobą wyznaczoną przez Zamawiającego do kontaktów z Wykonawcą.
6. Osoby wyznaczone do kontaktu w przedmiocie realizacji Umowy.
   - **ze strony Wykonawcy:**

     imię i nazwisko ……
     nr telefonu ……
     e- mail ……
   - **ze strony Zamawiającego**

     imię i nazwisko ……
     nr telefonu …….
     e- mail ……
7. Zrealizowanie przedmiotu zamówienia zostanie potwierdzone protokołem odbioru podpisanym przez obie Strony (Załącznik nr 2 do Umowy).

§ 4
ODPOWIEDZIALNOŚĆ WYKONAWCY

1. W przypadku stwierdzenia przez Zamawiającego niezgodności dostarczonego asortymentu z zamówieniem co do ilości Wykonawca zobowiązany jest do dostarczenia brakującego towaru do siedziby Zamawiającego w terminie do 1 dnia roboczego od dnia zgłoszenia informacji przez Zamawiającego.
2. W przypadku stwierdzenia przez Zamawiającego niezgodności dostarczonego asortymentu z zamówieniem co do jakości lub treści, Wykonawca zobowiązany jest do wymiany asortymentu na produkt nowy wolny od wad, spełniający wymagania Zamawiającego i dostarczenia go do siedziby Zamawiającego w terminie do 2 dni roboczych od dnia zgłoszenia informacji przez Zamawiającego. Koszt wymiany towaru ponosi Wykonawca.

§ 5

CENY I WARUNKI PŁATNOŚCI

1. Całkowite wynagrodzenie brutto Umowy za wykonanie przedmiotu zamówienia wynosi: brutto …….. (słownie: ……), netto …… (słownie: ……), zgodnie z Formularzem oferty, stanowiącym Załącznik nr 1 do Umowy, w tym:
    a) wartość wynagrodzenia za dostawę 3 814 kalendarzy ściennych trójdzielnych wynosi: brutto …….. zł (słownie: ……), netto (słownie: ……), …… (słownie: ……..)
    b) wartość wynagrodzenia za dostawę 160 kalendarzy książkowych w formacie B5 wynosi: brutto …….. zł (słownie: ……), netto …… (słownie: ……..)
2. Wynagrodzenie wskazane w ust. 1 Umowy obejmuje wszelkie koszty związane z realizacją zamówienia, w szczególności koszty dostawy (transportu) oraz należny podatek VAT.
3. Zapłata należności nastąpi po dostarczeniu zamówienia, przelewem na podany na fakturze numer rachunku bankowego Wykonawcy, w ciągu 21 dni od dnia otrzymania przez Zamawiającego prawidłowo wystawionej faktury.
4. Faktura powinna zostać wystawiona na: Izba Administracji Skarbowej w Katowicach, ul. Damrota 25, 40-022 Katowice, NIP 954 13 02 993.
5. Za dzień zapłaty uważa się dzień obciążenia rachunku Zamawiającego.
6. Strony uzgadniają, że w przypadkach dopuszczonych przez ustawę o podatku od towarów i usług (w szczególności w przypadku awarii systemu KSeF lub braku obowiązku wystawiania i odbierania faktur w KSeF):
    a) faktury i faktury korygujące oraz
    b) wymagane umową dokumenty świadczące o jej wykonaniu (protokoły, raporty, rozliczenia itp.) przesyłane będą na kancelaria.ias.katowice@mf.gov.pl. adres poczty elektronicznej Zamawiającego:
7. Wykonawca, działając zgodnie z przepisami prawa, zapewnia autentyczność pochodzenia, integralność treści i czytelność dokumentów, które przesyła w sposób wskazany w ust. 6.
8. W sytuacji opisanej w ust. 6, w przypadku zaistnienia przeszkód technicznych, które uniemożliwią przesłanie dokumentów we wskazany sposób, Zamawiający zobowiązuje się przyjmować dokumenty w formie papierowej.
9. W czasie trwania umowy wynagrodzenie Wykonawcy z tytułu wykonania umowy nie podlega zmianie i waloryzacji.
10. Wykonawca bez pisemnej zgody Zamawiającego nie może przenieść na osobę trzecią, praw i obowiązków wynikających z Umowy, w całości lub części, a w razie uzyskania zgody, o której mowa powyżej, ponosi odpowiedzialność za prawidłowe wykonanie usługi przez osobę trzecią.

§ 6

KARY UMOWNE

1. Strony zastrzegają sobie prawo naliczania kar umownych za niewykonanie lub nienależyte wykonanie przedmiotu Umowy.
2. W razie nienależytego wykonania Umowy, Zamawiający nałoży na Wykonawcę następujące kary

umowne:

1) w przypadku nieprzystąpienia do realizacji przedmiotowego zamówienia lub zaprzestania jego wykonywania z przyczyn zależnych od Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10% całkowitego wynagrodzenia brutto, o którym mowa w § 5 ust. 1;
2) w przypadku przekroczenia terminu dostawy, określonego w § 3 ust. 1 i 2, Wykonawca zapłaci Zamawiającemu karę umowną za każdy rozpoczęty dzień zwłoki w wysokości 0,5% całkowitego wynagrodzenia brutto, o którym mowa w § 5 ust. 1.

3. Każdej ze Stron wypowiadającej Umowę w przypadkach opisanych w §7 ust. 4 przysługuje prawo obciążenia drugiej Strony karą umowną w wysokości 10% całkowitego wynagrodzenia brutto, o którym mowa w § 5 ust. 1
4. Zapłata przez Wykonawcę kary umownej nie zwalnia Wykonawcy z realizowania obowiązków określonych Umową, z wyłączeniem ust. 2 pkt 1.
5. Kary umowne zastrzeżone na rzecz Zamawiającego mogą być dochodzone z każdego tytułu odrębnie i podlegają łączeniu, z wyłączeniem ust. 2 pkt 1.
6. Termin zapłaty kary umownej wynosi 7 dni od daty doręczenia zawiadomienia o obciążeniu karą umowną.
7. W przypadku opóźnienia w zapłacie kary umownej, Zamawiającemu przysługuje prawo naliczenia odsetek ustawowych za opóźnienie, zgodnie z art. 481 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2026 r., poz. 795).
8. Jeżeli Wykonawca nie zapłaci kary w terminie 7 dni od dnia otrzymania zawiadomienia o obciążeniu karą umowną, kara może zostać potrącona z należnego wynagrodzenia wykonawcy.
9. Wykonawca wyraża zgodę na potrącanie przez zamawiającego kar umownych z należnego Wykonawcy wynagrodzenia.
10. Zamawiający zastrzega sobie prawo dochodzenia odszkodowania uzupełniającego na zasadach określonych w Kodeksie cywilnym do wysokości poniesionej szkody na zasadach ogólnych, w przypadku, gdy szkoda wyrządzona Zamawiającemu w związku z niewykonaniem lub nienależytym wykonaniem Umowy przez Wykonawcę przewyższy wysokość kar umownych określonych w ust. 2 i ust. 3

§ 7

ROZWIĄZANIE, ODSTĄPIENIE ORAZ WYPOWIEDZENIE OD UMOWY

1. Umowa wygasa na skutek czynności podejmowanych przez Strony na podstawie i w sposób wskazany w Umowie oraz w przepisach Kodeksu cywilnego.
2. W uzasadnionych przypadkach Umowa może być rozwiązana na mocy zgodnego porozumienia Stron, określającego tryb oraz konsekwencje rozwiązania Umowy.
3. W przypadku wcześniejszego rozwiązania Umowy, Wykonawcy przysługuje jedynie wynagrodzenie za faktycznie zrealizowaną część Umowy.
4. Każda ze Stron może wypowiedzieć Umowę ze skutkiem natychmiastowym z powodu niewykonania przez drugą Stronę istotnych warunków Umowy lub w przypadku zwłoki drugiej Strony w wykonaniu zobowiązania. Wypowiedzenie Umowy może nastąpić w terminie 7 dni po bezskutecznym upływie wyznaczonego drugiej Stronie dodatkowego terminu do wykonania zobowiązania.
5. Odstąpienie od Umowy i jej wypowiedzenie wymaga formy pisemnej pod rygorem nieważności.

§ 8

ZACHOWANIA POUFNOŚCI

1. Wykonawca zobowiązuje się do zachowania w poufności wszelkich informacji technicznych, technologicznych, prawnych i organizacyjnych, oraz innych informacji Zamawiającego uzyskanych w trakcie wykonywania Umowy niezależnie od formy pozyskania tych informacji i ich źródła.
2. Wykonawca zobowiązuje się do wykorzystania informacji jedynie w celach określonych ustaleniami Umowy oraz wynikającymi z obowiązujących uregulowań prawnych.
3. Wykonawca zobowiązuje się do ujawnienia informacji dotyczących przedmiotu Umowy, w tym informacji technicznych, technologicznych i organizacyjnych jedynie tym osobom, którym będą one niezbędne do wykonywania powierzonych im czynności i tylko w zakresie, w jakim odbiorca informacji musi mieć do nich dostęp dla celów realizacji zadania wynikającego z tytułu realizacji Umowy.
4. Wykonawcę zobowiązuje się do niekopiowania, niepowielania, a także do nierozpowszechniania jakiejkolwiek części informacji związanych z realizacją Umowy z wyjątkiem uzasadnionej potrzeby do celów związanych z realizacją Umowy po uprzednim uzyskaniu pisemnej zgody od Zamawiającego, którego informacja lub źródło informacji dotyczy.
5. Strony zobowiązują się do przestrzegania przy wykonywaniu Umowy wszystkich postanowień zawartych w obowiązujących przepisach prawnych związanych z ochroną tajemnic prawnie chronionych.
6. Obowiązek określony w ust. 1 nie dotyczy informacji powszechnie znanych oraz udostępniania informacji na podstawie bezwzględnie obowiązujących przepisów prawa, a szczególności na żądanie sądów, prokuratury, organów podatkowych lub organów kontrolnych, a także informacji dostępnych publicznie, o których mowa w ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej.
7. Nie będą uważane za chronione informacje, które:
8. wcześniej stały się informacją publiczną w okolicznościach niebędących wynikiem czynu bezprawnego lub naruszającego Umowę przez którąkolwiek ze Stron;
9. zostały przekazane Stronie otrzymującej przez osobę trzecią niebędącą Stroną Umowy zgodnie z prawem i bez ograniczeń;
10. były zatwierdzone do rozpowszechniania na podstawie uprzedniej pisemnej zgody Strony, której dotyczą.
11. Wykonawca ponosi odpowiedzialność za zachowanie w poufności informacji przez swoich pracowników, podwykonawców i wszelkich innych osób, którymi będzie się posługiwać przy wykonywaniu Umowy.
12. Wykonawca podejmie wszelkie niezbędne kroki dla zapewnienia, że żaden pracownik Wykonawcy lub inna osoba, o której mowa w ust. 8, otrzymujący powyższe informacje, nie ujawni tych informacji, ani ich źródła, zarówno w całości, jak i w części podmiotom trzecim bez uzyskania uprzednio wyraźnej pisemnej zgody Zamawiającego, którego informacja lub źródło informacji dotyczy.
13. Obowiązek zachowania w poufności informacji przez Wykonawcę i osoby, o których mowa w ust. 8, obowiązuje także po ustaniu Umowy.
14. Wykonawca odpowiada za szkodę wyrządzoną Zamawiającemu przez ujawnienie, przekazanie, wykorzystanie, zbycie lub oferowanie do zbycia informacji otrzymanych od Zamawiającego,

wbrew postanowieniom Umowy. Zobowiązanie to wiąże Wykonawcę również po wykonaniu przedmiotu Umowy, jej rozwiązaniu, wygaśnięciu lub odstąpieniu, bez względu na przyczynę.

15. Wykonawca oświadcza, że:
16. znana jest mu treść przepisów w zakresie ochrony informacji i tajemnic prawnie chronionych tj.
17. ustawa z dnia 6 czerwca 1997 r. Kodeks Karny,
18. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE („RODO"),
19. ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych,
20. a także, że będzie ich przestrzegał zarówno w czasie realizacji Umowy jak i po jej zakończeniu;
21. każda z osób uczestniczących w realizacji przedmiotu Umowy zobowiązała się wobec niego jako Wykonawcy, nie ujawniać żadnych informacji, z którymi zapozna się podczas wykonywania czynności zleconych do realizacji oraz zapoznała się z treścią ww. przepisów i zobowiązała się do ich przestrzegania, zarówno w czasie realizacji Umowy, jak i po jej zakończeniu.
22. Wykonawca i osoby, o których mowa w ust. 8, zobowiązani są do zapoznania się z treścią Polityki Bezpieczeństwa Informacji Resortu Finansów stosowanej przez Zamawiającego i przestrzegania jej postanowień. Zamawiający udostępnia Wykonawcy Politykę Bezpieczeństwa Informacji Resortu Finansów i inne dokumenty z nią powiązane niezbędne do realizacji Przedmiotu Umowy.
23. Wykonawca i osoby, o których mowa w ust. 8, są obowiązani do złożenia podpisanego oświadczenia o zapoznaniu się z treścią Polityki, o której mowa w ust. 13, przed rozpoczęciem świadczenia Usługi. Oświadczenie może być złożone w formie elektronicznej.
24. Wzór OŚWIADCZENIA o zapoznaniu się z Polityką Bezpieczeństwa Informacji Resortu Finansów określa Załącznik nr 4 do Umowy. Dodatkowo Zamawiający informuje, że treść Polityki Bezpieczeństwa Informacji jest opublikowana w Dz. Urz. Min. Fin. I Gosp. z 2026 r. poz. 69 /adres internetowy do publikacji: https://www.gov.pl/web/finanse/du-mffipr/.

§ 9

USTALENIA KOŃCOWE

1. W kwestiach nieuregulowanych Umową obowiązują przepisy ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny.
2. Każda zmiana warunków, w trakcie obowiązywania Umowy, wymaga zachowania formy tożsamej z formą niniejszej Umowy pod rygorem nieważności, z wyłączeniem: nazw/określeń Stron, siedziby Stron ani osób wyznaczonych do kontaktu z Wykonawcą/Zamawiającym.
3. Jeżeli którekolwiek z postanowień Umowy jest lub stanie się nieważne, nie narusza to ważności pozostałych postanowień Umowy. W miejsce postanowień nieważnych Strony niezwłocznie uzgodnią takie postanowienia, które będą odpowiadać znaczeniu i celowi postanowień nieważnych.
4. Strony Umowy będą dążyć do rozstrzygnięcia ewentualnych sporów w sposób polubowny w drodze negocjacji. W przypadku braku polubownego załatwienia, spory wynikające z Umowy będą rozstrzygane przez Sąd właściwy dla siedziby Zamawiającego.
5. Umowa zawarta w postaci elektronicznej. [Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron].*

.....	.....
Zamawiający	Wykonawca

Załączniki do umowy:

Załącznik nr 1 – Formularz ofertowy
Załącznik nr 2 – Protokół odbioru
Załącznik nr 3 – Wzór Oświadczenia o zapoznaniu się z Polityką Bezpieczeństwa Informacji Resortu Finansów

*) Zamawiający odpowiednio dostosuje zapisy Umowy po wyborze najkorzystniejszej oferty

Załącznik nr 2 do Umowy

PROTOKÓŁ ODBIORU PRZEDMIOTU ZAMÓWIENIA

sporządzony w dniu ……. 2026 roku

Zamawiający

Skarb Państwa – Izba Administracji Skarbowej w Katowicach

40-022 Katowice, Damrota 25

Nip: 954-130-29-93

Wykonawca

……

……..

NIP: ……

Dotyczy: „Dostawy kalendarzy ściennych, trójdzielnych oraz książkowych w formacje B5 na rok 2027”

Po stronie Zamawiającego:

1. ……..

Po stronie Wykonawcy:

1. ……

Zgodnie zawartą umową Nr …… dokonano odbioru depozytorów:

L.p.	Rodzaj kalendarza	Liczba kalendarzy
1	**Kalendarz trójdzielny**	3814
2	**Kalendarz książkowy format B5**	160

Uwagi:

……

……

Na tym protokół zakończono i podpisano:

……. ……..

Zamawiający Wykonawca

Załącznik nr 3 do Umowy

.....

(miejscowość i data)

.....

(Nazwisko i Imię)

.....

(Nazwa podmiotu zewnętrznego realizującego

usługi na rzecz Resortu Finansów)

.....

(Stanowisko/funkcja)

OŚWIADCZENIE

o zapoznaniu się z zasadami bezpieczeństwa informacji w Resorcie Finansów

we współpracy z podmiotami zewnętrznymi

W związku z realizacją zobowiązań z tytułu Umowy Nr **2401-ILZ.023.1……2026** oświadczam, że zapoznałam/em się z *Zasadami bezpieczeństwa informacji w Resorcie Finansów we współpracy z podmiotami zewnętrznymi,* stanowiącymi załącznik do niniejszego oświadczenia.

.....

(czytelny podpis)[1]

[1] wypełnić tylko w wersji papierowej

Załącznik do oświadczenia

Zasady bezpieczeństwa informacji w Resorcie Finansów
we współpracy z podmiotami zewnętrznymi

1. W Resorcie Finansów w ramach współpracy z podmiotami zewnętrznymi stosuje się następujące zasady dotyczące bezpieczeństwa informacji:
   1) zasada wiedzy koniecznej (ograniczonego dostępu do informacji) – pracownicy posiadają dostęp tylko do tych informacji, które są konieczne do realizacji powierzonych im zadań (różne zadania oznaczają różną wiedzę konieczną do ich wykonania, a tym samym inny profil dostępu);
   2) zasada potrzeby koniecznej - pracownicy mają zapewniony dostęp tylko do środków przetwarzania informacji (urządzeń teleinformatycznych, systemów, aplikacji, pomieszczeń), które są im konieczne do wykonania powierzonych im zadań;
   3) zasada uprawnionego dostępu – pracownicy są dopuszczeni do przetwarzania informacji prawnie chronionych i przeznaczonych wyłącznie do użytku wewnętrznego po uzyskaniu wiedzy z zasad postępowania, w tym ochrony, określonych grup informacji~~,~~ oraz do odbycia szkolenia z zasad ochrony informacji (w celu spełnienia kryteria dopuszczenia do przetwarzania określonych informacji i danych);
   4) zasada obecności koniecznej – prawo przebywania w obszarze przetwarzania, w tym przechowywania informacji i danych prawnie chronionych i wrażliwych, mogą mieć tylko osoby upoważnione. Przebywanie osób nieupoważnionych w tym obszarze jest możliwe wyłącznie w obecności upoważnionych pracowników;
   5) zasada świadomości zbiorowej - wszyscy pracownicy mają świadomość konieczności ochrony aktywów informacyjnych i aktywnie uczestniczą w tym procesie; świadomość pracowników w zakresie istniejących zagrożeń i zasad ochrony informacji jest podnoszona, w szczególności przez szkolenia i działania informacyjne;
   6) indywidualnej odpowiedzialności – za utrzymanie odpowiedniego poziomu bezpieczeństwa poszczególnych aktywów lub ich elementów odpowiadają konkretne osoby, w zakresie nałożonych na nich obowiązków i nadanych im uprawnień. Zasada ta dotyczy np. powierzonego sprzętu:

      - każdy pracownik odpowiada za powierzony mu do użytkowania sprzęt komputerowy, wydruków z systemu centralnego wydruku,

      - każdy pracownik odpowiada za sporządzony przez siebie wydruk;

   7) rozdzielenia obowiązków - zadania krytyczne z punktu widzenia bezpieczeństwa systemu nie mogą być realizowane przez jedną osobę. Obowiązki i odpowiedzialności pozostające w konflikcie ze sobą należy rozdzielić w celu ograniczenia okazji do nieuprawnionej lub nieumyślnej modyfikacji lub nadużycia aktywów organizacji, w szczególności należy rozdzielić realizację funkcji operacyjnych od nadzorczych i kontrolnych;
   8) czystego biurka - podczas nieobecności pracownika na stanowisku pracy, także w przypadku krótkotrwałego opuszczenia pomieszczenia, dokumenty i informatyczne nośniki danych zawierające informacje prawnie chronione lub przeznaczone wyłącznie do użytku wewnętrznego należy zabezpieczyć przed dostępem osób postronnych i nieupoważnionych. Środki organizacyjno-techniczne dot. przechowywania dokumentów i informatycznych nośników danych dostosowywane są zidentyfikowanego ryzyka, z wykorzystaniem m.in. nieprzeszklonych, zamykanych na klucz mebli biurowych, szaf metalowych zamykanych na klucz lub kod, przeznaczonych do tego pomieszczeń zamykanych na klucz lub wyposażonych w system kontroli dostępu;

9) czystego ekranu - na czas nieobecności pracownika dostęp do komputera jest blokowany, a po zakończeniu pracy komputer jest wyłączany, chyba że dany komputer musi pracować w trybie ciągłym – w szczególności dotyczy to serwera obsługującego systemy alarmowe, komputerów administratorów, serwerów do monitoringu. W czasie obecności pracownika monitor jest ustawiony tak, aby nie pozwalał na zapoznawanie się z wyświetlanymi treściami przez osoby postronne, nieupoważnione;
10) czystego kosza – dokumenty papierowe, z wyjątkiem materiałów zawierających informacje publicznie dostępne, w tym promocyjno-informacyjne, muszą być niszczone w sposób uniemożliwiający ich odczytanie lub odtworzenie. W celu zniszczenia dokumentów papierowych zawierających informacje prawnie chronione i przeznaczone wyłącznie do użytku wewnętrznego należy korzystać z udostępnionych niszczarek o odpowiedniej klasie niszczenia, adekwatnej do informacji oraz danych utrwalonych na niszczonych dokumentach. Niszczenie informatycznych nośników danych należy przeprowadzić zgodnie z zasadami określonymi w umowie/porozumieniu;
11) czystej tablicy - po zakończonym spotkaniu należy uprzątnąć wszystkie materiały oraz wyczyścić tablice oraz flipchart (tablice do szkoleń);
12) czystych drukarek – w przypadku drukowania dokumentów z użyciem ogólnodostępnej drukarki drukowane informacje są zabierane z drukarek niezwłocznie po wydrukowaniu. W przypadku nieudanej próby wydrukowania użytkownik ma obowiązek skontaktować się z osobą odpowiedzialną za eksploatację urządzenia, jeżeli zachodzi podejrzenie, iż wydruk zostanie wydrukowany bez nadzoru;
13) poufności informacji uwierzytelniających – każdy pracownik jest obowiązany do zachowania poufności udostępnionych mu haseł, kodów dostępu, kodów PIN, w szczególności do systemów informacyjnych;
14) prywatności kont w systemach – każdy użytkownik jest obowiązany do pracy w systemach informacyjnych wyłącznie na przypisanych lub udostępnionych mu kontach, które jednoznacznie go identyfikują. Zabronione jest udostępnianie własnych kont osobom trzecim. Zasada ta ma również zastosowanie do kart wykorzystywanych w systemach kontroli dostępu funkcjonujących w Resorcie Finansów. Stosowanie się do tej reguły pozwala zachować rozliczalność działań użytkowników;
15) dyskrecji – wszelkie informacje służbowe mogą być przekazywane innym osobom uprawnionym do pozyskania tych informacji zgodnie z obowiązującymi przepisami prawa i przyjętymi w Resorcie Finansów zasadami;
16) zamkniętego pomieszczenia – niedopuszczalne jest pozostawienie pod nieobecność pracownika niezabezpieczonego pomieszczenia służbowego, zarówno w godzinach pracy, jak i po jej zakończeniu. Na zakończenie dnia pracy ostatnia wychodząca z pomieszczenia osoba jest obowiązana zamknąć wszystkie okna i drzwi oraz zabezpieczyć klucze do pomieszczenia;
17) zgłaszania incydentów bezpieczeństwa informacji i naruszeń ochrony danych osobowych – każdy użytkownik ma obowiązek niezwłocznie zgłosić wystąpienie lub podejrzenie wystąpienia incydentu lub naruszenia mającego lub mogącego mieć wpływ na bezpieczeństwo informacji, w tym danych osobowych w Resorcie Finansów;
18) bezpiecznej współpracy z podmiotami zewnętrznymi – dokumenty regulujące współpracę, w tym umowy, porozumienia, zawierają stosowne klauzule bezpieczeństwa, w tym o zachowaniu poufności, zasadach postępowania z pozyskaną informacją, niszczenia lub zwrotu aktywów informacyjnych po zakończeniu współpracy;

19) automatyzacji backupu - procesy tworzenia kopii zapasowych są odpowiednio zaplanowane z uwzględnieniem wymogów prawnych i potrzeb Resortu Finansów, jak również są zautomatyzowane oraz niemożliwe do przerwania przez pracownika;
20) legalnego oprogramowania – na serwerach i stacjach roboczych jest zainstalowane wyłącznie legalne oprogramowanie;
21) ochrony zewnętrznych (wymiennych) nośników danych – dane i informacje utrwalone na zewnętrznych nośnikach danych i wynoszone poza pomieszczenia użytkowane przez Resort Finansów są odpowiednio zabezpieczone przed nieuprawnionym dostępem, zniszczeniem oraz utratą integralności w czasie transportu i przechowywania. W szczególności dotyczy to informacji prawnie chronionych np. tajemnicy skarbowej, tajemnicy celnej, danych osobowych.
22) zasada bezpieczeństwa informacji w usługach chmurowych - wszystkie dane przetwarzane w usługach chmurowych muszą być lokalizowane w regionach Europejskiego Obszaru Gospodarczego (EOG), z preferencją regionów zlokalizowanych w Polsce. Odstępstwa od tej zasady wymagają uprzedniej zgody DBE MF, opartej na analizie ryzyka wraz z zastosowaniem mechanizmów transferowych i technicznych środków ochrony (np. szyfrowanie, kontrola kluczy). W przypadku, gdy przetwarzanie obejmuje dane osobowe, odstępstwa od lokalizacji EOG wymagają również oceny zgodności transferu danych zgodnie z RODO oraz zastosowania adekwatnych mechanizmów transferowych i środków technicznych.

2. Stosowanie zabezpieczeń lub ich grup uwzględnia następujące zasady:
   1) minimalny stosowany poziom zabezpieczeń odpowiada wymogom obowiązujących przepisów prawa;
   2) zabezpieczenia są wdrażane we wszystkich obszarach określonych w deklaracji stosowania zabezpieczeń, zgodnie z wymogami normy ISO/IEC 27001 i zasadami określonymi w normie ISO/IEC 27002;
   3) używane mechanizmy zabezpieczeń są adekwatne (odpowiednie) do zagrożeń, podatności, wartości aktywów oraz wyników szacowania ryzyka w bezpieczeństwie informacji;
   4) w doborze zabezpieczeń należy uwzględnić zalecenia i rekomendacje sformułowane w wyniku przeprowadzonych audytów bezpieczeństwa i kontroli;
   5) zabezpieczenia fizyczne, techniczne, prawne i organizacyjne uzupełniają się wzajemnie (grupy zabezpieczeń), zapewniając wymagany poziom bezpieczeństwa informacji;
   6) należy unikać niepotrzebnego dublowania zabezpieczeń, przy uwzględnieniu racjonalnego gospodarowania środkami publicznymi, optymalizacji potrzeb oraz ograniczeń i uwarunkowań prawno-organizacyjnych Resortu Finansów;
   7) niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających systemy informacyjne funkcjonujące w Resorcie Finansów bez zastosowania alternatywnych mechanizmów; systemy są sprawne i przygotowane na wystąpienie zidentyfikowanych zagrożeń;
   8) domniemanej odmowy - przyjęcia jako standardowych najbardziej restrykcyjnych ustawień, które można zwolnić jedynie w określonych sytuacjach („to, co nie jest dozwolone, jest zabronione”);
   9) ciągłego doskonalenia – SZBI jest stale monitorowany, stosowane zabezpieczenia są dostosowywane do zmieniających się warunków wewnętrznych i zewnętrznych, w celu zapewnienia ich przydatności, adekwatności i skuteczności.