

Rozwiązania informatyczne

Dokument opisuje przyjęte u ADO rozwiązanie, mające na celu zapewnienie bezpieczeństwa danych osobowych, przetwarzanych w aplikacjach, programach lub systemach informatycznych.

Spis treści

1. Zasady zarządzania bezpieczeństwem w systemach informatycznych.....	2
2. Zasady uwierzytelniania w systemach informatycznych.....	2
2.1 Stosowanie identyfikatorów i haseł	2
2.2 Blokada i usuwanie kont użytkowników	4
2.3 Konta specjalne (nieprzypisane, grupowe, dla osób z zewnątrz).....	4
3. Zasady nadawania uprawnień w systemach informatycznych	4
4. Zasady dotyczące zabezpieczeń infrastruktury informatycznej	5
5. Zasady dotyczące monitorowania infrastruktury informatycznej.....	6
6. Zasady postępowania w przypadku wystąpienia zdarzenia krytycznego dla procesu przetwarzania danych osobowych	7
7. Zasady wykonywania kopii zapasowych.....	8
8. Zasady zarządzania stacjami końcowymi	9
9. Zasady zarządzania zewnętrznymi stacjami końcowymi.....	10
10. Zasady dostępu zdalnego do infrastruktury ADO.....	10
11. Zasady zarządzania infrastrukturą sieciową	11
12. Zasady aktualizacji elementów środowiska informatycznego	12
13. Zasady postępowania z nośnikami danych	12
13. Zasady dotyczące przeglądów, konserwacji, modernizacji lub naprawy elementów środowiska informatycznego.....	14
14. Zasady zabezpieczenia infrastruktury przed skutkami utraty zasilania	14
15. Zasady współpracy z podmiotami zewnętrznymi, świadczącymi usługi informatyczne	14
16. Postanowienia końcowe.....	15

1. Zasady zarządzania bezpieczeństwem w systemach informatycznych

1. ADO powinien, adekwatnie do skali i profilu prowadzonej działalności:
 - 1) określić sposób zarządzania bezpieczeństwem danych osobowych przetwarzanych w systemach informatycznych.
 - 2) zapewnić strukturę organizacyjną umożliwiającą bezpieczne funkcjonowanie infrastruktury informatycznej wykorzystywanej do przetwarzania danych osobowych.
2. Sposób zarządzania bezpieczeństwem powinien określać wszystkie aspekty organizacji pracy ADO, zmierzające do zabezpieczenia systemów IT. W szczególności powinien zawierać:
 - 1) sposób podejmowania decyzji i zakres obowiązków oraz uprawnienia osób odpowiedzialnych za bezpieczeństwo systemów;
 - 2) zakresy uprawnień i obowiązków poszczególnych użytkowników.
3. Określenie zasad powinno mieć formę utrwaloną na piśmie lub elektroniczną.
4. Podział obowiązków powinien minimalizować ryzyko nadużyć i błędów oraz umożliwić skuteczny nadzór oraz kontrolę nad procesem zarządzania bezpieczeństwem danych osobowych przetwarzanych w systemach informatycznych.
5. Określając obowiązki, ADO powinien uwzględnić rozdzielenie ról związanych z realizacją procesów organizacyjnych w obszarze bezpieczeństwa, zarządzaniem infrastrukturą informatyczną oraz obowiązków związanych z kontrolą obszaru bezpieczeństwa. W szczególności dotyczy to takich ról jak:
 - 1) nadawanie rzeczywistych uprawnień działom/użytkownikom (realizacja procesów organizacyjnych wynikająca z nadawania upoważnień do przetwarzania danych osobowych);
 - 2) realizowanie czynności technicznych w tym również administrowania systemami (w szczególności stosownie do rzeczywistych uprawnień zakładanie kont użytkowników, ich modyfikacja, wykonywanie kopii zapasowych);
 - 3) weryfikacja poprawności działania systemów bezpieczeństwa (kontrole, audyty).

2. Zasady uwierzytelniania w systemach informatycznych

1. Dostęp do danych przetwarzanych w systemach informatycznych:
 - 1) powinny posiadać tylko osoby upoważnione do ich przetwarzania.
 - 2) powinien być możliwy wyłącznie po pozytywnie zakończonym procesie uwierzytelniania – w szczególności opartym na podaniu identyfikatora i hasła.
2. ADO może stosować inne metody uwierzytelniania (np. karty magnetyczne, karty zbliżeniowe, dane biometryczne).
3. Implementacja w systemach IT danych biometrycznych, genetycznych lub innych szczególnych kategorii danych w rozumieniu art. 9 RODO w celu uwierzytelniania dostępu powinna zostać uprzednio przeanalizowana pod kątem zgodności z wymaganiami wynikającymi w szczególności z obowiązujących przepisów prawa.
4. Jeśli możliwości techniczne systemów informatycznych na to pozwalają, powinny zostać uruchomione mechanizmy udostępniające uwierzytelnianie wieloskładnikowe.

2.1 Stosowanie identyfikatorów i haseł

5. Podczas logowania do systemów informatycznych wpisywane hasło nie powinno być wyświetlane jawnym tekstem.
6. Systemy informatyczne powinny posiadać funkcję blokującą konto użytkownika po przekroczeniu ustalonej liczby błędnych prób logowań.
7. Systemy informatyczne powinny wymuszać zmianę hasła w regularnych odstępach czasu.

8. Czas zmiany hasła powinien zostać uzależniony od kategorii przetwarzanych danych.
9. ADO może wyrazić zgodę na użycie kont, które nie podlegają wymogom czasowej zmiany hasła.
10. Systemy informatyczne powinny posiadać możliwość zdefiniowania warunków jakie powinny spełniać hasła, tj. ich minimalnej długości i stopnia skomplikowania.
11. Systemy informatyczne powinny zapobiegać stosowaniu haseł, które zostały wcześniej wykorzystane.
12. Podczas tworzenia nowego konta użytkownika lub resetowania hasła istniejącego konta, należy nadać hasło tymczasowe.
13. Podczas pierwszego logowania hasłem tymczasowym system informatyczny powinien wymusić zmianę hasła tymczasowego i umożliwić użytkownikowi zdefiniowanie własnego hasła.
14. Dane umożliwiające dostęp do systemów informatycznych, w tym również hasła tymczasowe, powinny być przekazywane:
 - 1) po pozytywnej identyfikacji tożsamości użytkownika;
 - 2) w sposób gwarantujący ich poufność.
15. Należy sporządzić instrukcje określające zasady pracy w wykorzystywanych systemach informatycznych, w przypadku, gdy nie realizują one następujących zasad:
 - 1) wymuszenia zmiany hasła w regularnych odstępach czasu;
 - 2) określenia warunków jakie powinny spełniać hasła;
 - 3) wymuszenia zmiany hasła tymczasowego;
 - 4) ograniczenia w wykorzystywaniu haseł historycznych.
16. Należy zobowiązać osoby pracujące w systemach do przestrzegania instrukcji, o których mowa w ust. 17 powyżej – fakt otrzymania instrukcji i zapoznani się z nią każdy z użytkowników powinien potwierdzić na piśmie lub w inny ustalony u ADO sposób.
17. Systemy informatyczne powinny zapewniać bezpieczeństwo przechowywanych haseł, w szczególności hasła nie mogą być przechowywane w postaci jawnego tekstu.
18. Systemy informatyczne nie powinny stosować mechanizmów zapamiętywania haseł oraz mechanizmów automatycznego logowania do systemu.
19. Systemy informatyczne powinny posiadać mechanizm automatycznego wylogowania lub blokowania dostępu, w przypadku braku aktywności użytkownika przez określony czas.
20. Przed przekazaniem systemu do użytkowania, powinny zostać zmienione wszelkie domyślne hasła ustawione przez dostawców systemów informatycznych.
21. W przypadku naruszenia bezpieczeństwa systemu informatycznego związanego z ujawnieniem haseł użytkowników, należy niezwłocznie zmienić hasła wszystkim użytkownikom.
22. Szczególną ochroną powinny zostać objęte dane umożliwiające wykorzystywanie kont z uprawnieniami administratora systemu informatycznego.
23. ADO powinien zapewnić sobie awaryjne dostępy z uprawnieniami administratora systemu informatycznego do systemów informatycznych.
24. Identyfikator każdego użytkownika musi być unikalny.
25. Identyfikatory powinny być nadawane zgodnie z określoną konwencją nazewnictwa, która umożliwi jednoznaczną identyfikację użytkownika.
26. Identyfikator użytkownika nie powinien być zmieniany. W uzasadnionych przypadkach ADO może wyrazić zgodę na zmianę identyfikatora użytkownika.
27. Zmiana identyfikatora użytkownika może nastąpić tylko w przypadku, gdy wszystkie dotychczasowe zapisy, dotyczące zarówno aktywności użytkownika w systemie informatycznym jak i czynności związanych z modyfikacją uprawnień na koncie użytkownika, zostaną przypisane do nowego identyfikatora.

28. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, nie może być ponownie nadany innemu użytkownikowi.

2.2 Blokada i usuwanie kont użytkowników

29. Konta użytkowników, z którymi ADO zakończył współpracę, powinny zostać niezwłocznie zablokowane.
30. ADO może podjąć decyzję dotyczącą blokady konta użytkownika, w przypadku którego wszczęto postępowanie dyscyplinarne.
31. Czynności związane z blokowaniem lub odblokowaniem konta, powinny zostać zatwierdzone przez ADO i udokumentowane.
32. Konta użytkowników oraz przypisane do nich uprawnienia powinny podlegać okresowemu przeglądowi i weryfikacji.

2.3 Konta specjalne (nieprzypisane, grupowe, dla osób z zewnątrz)

33. Konta powinny być przypisywane indywidualnie do każdego użytkownika.
34. Niedozwolone jest zakładanie kont, które nie zostały przypisane do określonej osoby. Wyjątkiem od tej zasady są konta wymagane do prawidłowego działania systemu informatycznego służącego do przetwarzania danych osobowych. ADO powinien dysponować listą kont nieprzypisanych do konkretnych osób.
35. Tworzenie kont grupowych jest możliwe wyłącznie po uzyskaniu uprzedniej zgody ADO.
36. Zgoda na udostępnienie użytkownikom kont grupowych powinna dotyczyć tylko systemów operacyjnych zainstalowanych na stacjach roboczych, w których bezpośrednio dochodzi do przetwarzania tylko pojedynczych danych osobowych.
37. Z kont grupowych mogą korzystać tylko osoby, które posiadają identyczny zakres uprawnień określony w upoważnieniu do przetwarzania danych osobowych.
38. W przypadku zgody na użytkowanie kont grupowych należy ściśle zdefiniować grupę użytkowników korzystających z takich kont.
39. W przypadku zgody na użytkowanie kont grupowych, ADO powinien posiadać listę osób korzystających z takich kont.
40. ADO może wyrazić zgodę na utworzenie konta osobie nieposiadającej statusu osoby zatrudnionej.
41. Zakładanie konta osobie nieposiadającej statusu osoby zatrudnionej, w szczególności wykonującej czynności na podstawie umowy łączącej ADO z tą osobą lub podmiotem zewnętrznym, powinno być możliwe jedynie po uregulowaniu zasad współpracy z ADO.
42. Konta pracowników podmiotów zewnętrznych powinny być specjalnie oznaczone oraz powinny jednoznacznie identyfikować osobę korzystającą z takiego konta.
43. Zabronione jest tworzenie lub udostępnienie kont grupowych użytkownikom nieposiadającym statusu osoby współpracującej z ADO.
44. Konta osób reprezentujących podmioty zewnętrzne powinny być aktywne tylko na czas realizacji ich zadań w okresie obowiązywania stosunku prawnego, łączącego je z ADO.

3. Zasady nadawania uprawnień w systemach informatycznych

1. Osoby zatrudnione muszą posiadać uprawnienia niezbędne do wykonania obowiązków służbowych, zgodne z upoważnieniem do przetwarzania danych osobowych.
2. Użytkownikom należy przyznawać tylko minimum uprawnień, zgodnie z zakresem nadanego upoważnienia do przetwarzania danych osobowych.

3. Użytkownicy po zalogowaniu do systemu informatycznego, powinni mieć dostęp tylko do tych funkcji, które wynikają z przyznanych im uprawnień.
4. Wszelkie zmiany uprawnień wynikające z ich nadania, modyfikacji oraz odebrania, powinny następować wyłącznie na podstawie wniosków zatwierdzonych przez ADO.
5. Zatwierdzone i zrealizowane wnioski związane z nadaniem uprawnień lub ich zmianą powinny być archiwizowane.
6. Systemy informatyczne powinny zapisywać zdarzenia dotyczące tego kto, w jakim czasie i w jakim zakresie wykonał zmiany nadania, modyfikacji i odebrania uprawnień.
7. Zmiany w uprawnieniach nie powinny wiązać się z usunięciem historii czynności wykonanych przez użytkowników w systemach informatycznych.
8. Wszelkie uprawnienia użytkowników, z którymi umowa ulegnie rozwiązaniu, powinny być unieważnione niezwłocznie po zakończeniu współpracy.
9. Uprawnienia przyznane osobom nieposiadającym statusu osoby zatrudnionej u ADO powinny być adekwatne do wykonania czynności wynikających ze stosunku łączącego ADO z tą osobą i powinny być nadawane jedynie na czas realizacji prac zleconych przez ADO.
10. Za nadawanie uprawnień w systemach informatycznych jest odpowiedzialne IT.
11. ADO może zlecić podmiotom zewnętrznym wykonywania czynności związanych z nadawaniem uprawnień w systemach informatycznych.
12. ADO powinien zorganizować proces zarządzania uprawnieniami w sposób zapewniający rozdzielenie czynności związanych z określeniem zakresu uprawnień (uprawnienia rzeczywiste: bezpośredni przełożony w porozumieniu z osobą lub działem odpowiedzialnym z za sprawy kadrowe) od czynności związanych z bezpośrednim nadawaniem uprawnień w systemach informatycznych (uprawnienia w systemach IT: informatyk).
13. Okresowej weryfikacji ze stanem faktycznym należy poddawać:
 - 1) uprawnienia użytkowników w systemach informatycznych,
 - 2) listę osób zatrudnionych u ADO z listą osób posiadających konta w systemach informatycznych.
14. Weryfikacja procesu nadawania uprawnień użytkowników nie powinna być wykonywana przez osoby odpowiedzialne za bezpośrednie nadawanie uprawnień w systemach informatycznych.
15. ADO powinien posiadać dokumentację zawierającą opis ról, profili lub uprawnień jakie może nadać użytkownikom.

4. Zasady dotyczące zabezpieczeń infrastruktury informatycznej

1. Systemy zabezpieczające infrastrukturę informatyczną powinny zapewniać ochronę przed próbami uzyskania nieautoryzowanego dostępu do danych osobowych zarówno od wewnątrz (z sieci lokalnej), jak i z zewnątrz (z sieci publicznej).
2. ADO powinien zapewnić przynajmniej dwie strefy ochrony przed próbami uzyskania nieautoryzowanego dostępu danych osobowych:
 - 1) globalną, nadzorującą cały ruch przychodzący z sieci publicznej do sieci lokalnej;
 - 2) lokalną, zapewnioną przez oprogramowanie chroniące, umieszczone bezpośrednio na stacjach roboczych oraz serwerach.
3. Dostęp do systemów zapewniających ochronę przed próbami uzyskania nieautoryzowanego dostępu danych osobowych powinien być ograniczony, a ich zarządzaniem powinien zajmować się tylko wykwalifikowany personel IT.
4. Systemy zapewniające ochronę danych osobowych powinny pochodzić od różnych producentów.
5. Systemy zapewniające ochronę danych osobowych powinny funkcjonować w trybie ochrony w czasie rzeczywistym.

6. Systemy zapewniające ochronę danych osobowych powinny być regularnie aktualizowane.
7. Aktualizacja powinna obejmować zarówno silniki systemów, jak i wszelkie sygnatury, reguły odpowiadające za wykrywanie i blokowanie złośliwego oprogramowania oraz blokowanie nieautoryzowanego ruchu sieciowego.
8. Systematyczność aktualizacji powinna zostać określona w oparciu o częstotliwość aktualizacji udostępnianych przez producenta.
9. W przypadku konieczności wykonania aktualizacji w sposób manualny, termin jej wykonania powinien zależeć od poziomu jej krytyczności dla bezpieczeństwa danych osobowych.
10. Przed przystąpieniem do wykonania aktualizacji, a w szczególności aktualizacji krytycznej systemu przetwarzającego dane osobowe, powinny zostać zapewnione kopie zapasowe umożliwiające, w razie awarii lub błędnego działania systemu, powrót do stanu sprzed aktualizacji.
11. Podczas wykonywania aktualizacji należy zachować szczególną ostrożność oraz zweryfikować czy po zakończeniu aktualizacji, systemy zapewniające ochronę danych osobowych funkcjonują właściwie.
12. W zależności od liczby stacji końcowych, ADO powinien wprowadzić scentralizowany system zarządzający ochroną stacji roboczych.
13. Aplikacja zapobiegająca działaniu szkodliwego oprogramowania powinna automatycznie i regularnie skanować wszystkie zasoby stacji roboczych.
14. W przypadku podłączenia do stacji roboczej przenośnego nośnika danych, aplikacja chroniąca przed szkodliwym oprogramowaniem powinna automatycznie przeskanować urządzenie lub poinformować użytkownika o możliwości wykonania takiego skanowania.
15. Aplikacje chroniące przed szkodliwym oprogramowaniem powinny automatycznie naprawiać zainfekowane pliki. W przypadku braku możliwości naprawy, plik powinien zostać poddany kwarantannie, a użytkownik poinformowany o takim zdarzeniu.
16. W miarę możliwości, w celu monitorowania zagrożeń, o zdarzeniach związanych z funkcjonowaniem aplikacji zapobiegającej działaniu szkodliwego oprogramowania powinien zostać automatycznie poinformowany ADO.

5. Zasady dotyczące monitorowania infrastruktury informatycznej

1. Monitoring infrastruktury informatycznej nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika.
2. ADO może monitorować służbowe skrzynki pocztowe lub inne narzędzia komunikacyjne (komunikatory, platformy peer-to-peer itp.) w celu zabezpieczenia bezpieczeństwa danych lub infrastruktury informatycznej, z zastrzeżeniem, że w momencie podjęcia wiedzy, że dany komunikat zawiera dane prywatne użytkownika – monitoring danej wiadomości / komunikatu musi być przerwany.
3. ADO powinien zapewnić warunki umożliwiające monitorowanie infrastruktury informatycznej w celu zapewnienia bezpieczeństwa infrastruktury przetwarzającej dane osobowe i wykrycia zdarzeń mogących wskazywać na naruszeniu zasad bezpieczeństwa danych osobowych.
4. ADO powinien dążyć do tego, aby proces monitorowania był w jak największym stopniu scentralizowany.
5. W szczególności zakres monitorowania powinien dotyczyć wykrywania zdarzeń świadczących o:
 - 1) niezgodnej z zasadami bezpieczeństwa aktywności użytkowników;
 - 2) działaniach mających na celu przełamanie zabezpieczeń sieciowych;
 - 3) działaniach mających na celu dystrybucję złośliwego oprogramowania;

- 4) powstaniu błędu mającego wpływ na bezpieczeństwo systemu informatycznego (podatności).
6. Systemy informatyczne biorące bezpośredni udział w przetwarzaniu danych osobowych, powinny umożliwiać zapisywanie w dziennikach uporządkowanych informacji o zdarzeniach.
7. W dziennikach systemów informatycznych powinny zostać zarejestrowane zdarzenia dotyczące w szczególności aktywności użytkowników na danych osobowych oraz błędów systemowych.
8. W dziennikach systemów informatycznych powinny zostać odnotowane również zdarzenia wynikające operacji na danych osobowych przeprowadzonych przez użytkowników:
 - 1) z uprawnieniami administratora systemu informatycznego;
 - 2) z uprawnieniami wykraczającymi poza użytkową obsługę systemów.
9. W dziennikach powinny być dokumentowane zdarzeń zapewniające możliwość określenia działań wykonanych przez użytkowników, a także określenie czasu ich realizacji.
10. Informacje opisujące poszczególne zdarzenie powinny zapewnić w szczególności dostateczną identyfikację zdarzenia oraz być podstawą rozliczalności.
11. ADO powinien posiadać możliwość szczegółowej analizy zdarzeń generowanych przez systemy informatyczne, w tym systemy zabezpieczające infrastrukturę informatyczną.
12. Monitorowanie powinno uwzględniać pozyskiwanie informacji na temat podatności w zarządzanych przez ADO systemach informatycznych.
13. W miarę możliwości proces monitorowania powinien zostać rozszerzony o informacje dotyczące zmian konfiguracji elementów infrastruktury informatycznej biorących udział w przetwarzaniu danych osobowych.
14. Systemy informatyczne powinny posiadać mechanizmy umożliwiające ustawienie automatycznych powiadomień w przypadku wykrycia zdefiniowanych zdarzeń mogących świadczyć o naruszeniu zasad przetwarzania danych osobowych.
15. Dzienniki zdarzeń powinny być zabezpieczone przed modyfikacją oraz powinny być dostępne tylko dla upoważnionych osób.
16. ADO powinien wdrożyć rozwiązania odpowiedzialne za synchronizację i poprawność czasu zdarzeń rejestrowanych w dziennikach zdarzeń.
17. ADO powinien ustalić okres przechowywania w systemie informatycznym rejestru czynności wykonywanych przez wszystkich użytkowników, uwzględniając wymogi wynikające z przepisów prawa.
18. ADO powinni regularnie monitorować czynności wykonywane przez wszystkich użytkowników w celu zlokalizowania działań niezgodnych z przyjętymi zasadami bezpieczeństwa.

6. Zasady postępowania w przypadku wystąpienia zdarzenia krytycznego dla procesu przetwarzania danych osobowych

1. Monitoring infrastruktury informatycznej nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika.
2. ADO powinien dysponować planem reakcji w momencie wystąpienia zdarzenia krytycznego, którego skutkiem będzie konieczność odzyskania dostępu do przetwarzanych danych osobowych.
3. Plan powinien określać działania jakie należy podjąć w celu przywrócenia czynności przetwarzania do stanu przed wystąpieniem krytycznego zdarzenia.
4. W planie należy uwzględnić:
 - 1) zasoby oraz procedury, które w początkowej fazie umożliwią w minimalnym stopniu zachowanie czynności przetwarzania danych;

- 2) zasoby oraz procedury niezbędne do przeprowadzenia procesu odtworzenia;
 - 3) wskazanie funkcji lub osób biorących udział w procesie odtworzenia oraz zakres ich odpowiedzialności;
 - 4) sposób komunikacji dotyczący przebiegu planu odtwarzania oraz spis kontaktów do osób biorących udział w procesie odtworzenia; spis kontaktów powinien zawierać wyłącznie numer telefonu, adres e-mail oraz stanowisko osoby odpowiedzialnej (podawanie imienia i nazwiska nie jest konieczne, wskazane jest używanie zamiast imienia i nazwiska stanowiska lub pełnionej funkcji osoby odpowiedzialnej;
 - 5) dostęp do dokumentacji umożliwiającej odtwarzanie systemów informatycznych.
5. Plan odtwarzania powinien zakładać w pierwszej kolejności przywrócenie w jak najkrótszym czasie kluczowych funkcji odpowiadających za przetwarzanie danych osobowych.
 6. Dla każdego systemu informatycznego przetwarzającego dane osobowe powinna powstać instrukcja określająca szczegółowy opis czynności, jakie należy wykonać, aby doprowadzić do odtworzenia systemu informatycznego.
 7. W działaniach, zmierzających do odtworzenia przetwarzania danych osobowych, mogą brać udział podmioty zewnętrzne.

7. Zasady wykonywania kopii zapasowych

1. Podstawą procesu odtworzenia powinny być regularnie wykonywane kopie zapasowe baz danych, w których gromadzone są dane osobowe.
2. Proces tworzenie kopii zapasowych powinien zostać zaplanowany w sposób umożliwiający zapewnienie:
 - 1) dostępności danych osobowych z uwzględnieniem jak najmniejszej ich utraty;
 - 2) integralności danych osobowych;
 - 3) poufności danych osobowych.
3. ADO powinien dążyć do posiadania przynajmniej trzech równorzędnych kopii baz danych.
4. Przynajmniej dwie kopie zapasowe baz danych powinny być przechowywane na różnych nośnikach danych (urządzeniach).
5. W miarę możliwości ADO powinien przechowywać jedną kopię zapasową baz danych poza obszarem przetwarzania (w lokalizacji oddalonej od miejsca, w którym przechowywane są pozostałe kopie zapasowe).
6. W przypadku transferowania kopii zapasowej baz danych poza obszar przetwarzania, należy zabezpieczyć ją przy wykorzystaniu środków kryptograficznych (szyfrowania).
7. Szyfrowanie powinno nastąpić przed przesłaniem kopii zapasowych baz danych poza obszar przetwarzania.
8. W przypadku transferowania kopii zapasowej baz danych poza obszar przetwarzania, przy wykorzystaniu zasobów podmiotu zewnętrznego należy podpisać stosowną umowę z takim podmiotem.
9. W miarę możliwości ADO powinien posiadać dostęp również do kilku historycznych kopii zapasowych.
10. Obok kopii danych osobowych powinno tworzyć się kopie konfiguracji elementów krytycznych dla przetwarzania danych osobowych.
11. W miarę możliwości ADO powinien zapewnić sobie dostęp do kopii zapasowych aplikacji krytycznych dla przetwarzania danych osobowych.
12. Kopie baz danych powinny być przechowywane w bezpiecznym miejscu, do którego nie mają dostępu osoby postronne.
13. Bez względu na to powinno się przestrzegać ustalonych terminów sporządzania kopii zapasowych oraz dokonywać okresowych kontroli odczytu tych danych.

14. Bezwzględnie należy wykonywać regularną weryfikację kopii zapasowych.
15. Weryfikacja powinna polegać na próbie pełnego przywrócenia danych z kopii i kontroli ich kompletność, aktualność, poprawności i spójności.
16. Uprawnienie umożliwiające wykonywanie kopii danych z systemów informatycznych powinny zostać ograniczone do minimum i przyznane jedynie upoważniony pracownikom lub podmiotom zewnętrznym, współpracującym z ADO w tym zakresie.

8. Zasady zarządzania stacjami końcowymi

1. Wszelkie czynności związane z konfiguracją stacji roboczych, a w szczególności oprogramowanie chroniące przed zagrożeniami, powinny zostać wykonywane tylko i wyłącznie przez wykwalifikowany personel IT. Podejmowanie takich czynności przez użytkowników końcowych powinno być zabronione.
2. Na stacjach roboczych podłączonych do sieci ADO, powinna zostać uruchomiona aplikacja chroniąca je przed szkodliwym oprogramowaniem.
3. Na stacjach roboczych podłączonych do sieci ADO, powinny zostać uruchomione wszystkie możliwe mechanizmy udostępnione w ramach oprogramowania sprzętowego, systemu operacyjnego i aplikacji przetwarzającej dane osobowe, zapewniające bezpieczeństwo danych osobowych.
4. Wygaszacz ekranu komputera powinien być skonfigurowany w taki sposób, by uruchamiał się automatycznie w przypadku braku aktywności ze strony użytkownika przez określony czas.
5. Czas, po jakim uruchomiony zostanie automatycznie wygaszacz ekranu, powinien być uwarunkowany od tego czy do pomieszczenia, w którym znajduje się stacja robocza, mają dostęp osoby nie posiadające upoważnienia do przetwarzania danych osobowych lub posiadające upoważnienie nadane w innym zakresie.
6. Odblokowanie wygaszacza ekranu powinno wiązać się z podaniem hasła do systemu operacyjnego.
7. Na stacjach roboczych powinno zostać zainstalowane oprogramowanie niezbędne do wykonania czynności służbowych.
8. Nieużywane oprogramowanie oraz zbędne elementy systemu powinny zostać odinstalowane.
9. ADO powinien zaplanować proces okresowej weryfikacji stacji końcowych, w szczególności pod kątem obecności nieautoryzowanego oprogramowania.
10. Stacje robocze powinny zostać skonfigurowane w taki sposób, by funkcjonowały na nich tylko niezbędne usługi systemowe, konta systemowe itp.
11. Na stacjach roboczych powinny funkcjonować dwa profile kont dla użytkowników:
 - 1) konto standardowe z uprawnieniami ograniczającymi do minimum możliwość administracji stacją roboczą;
 - 2) konto administratora, posiadające pełne uprawnienia do zarządzania stacją roboczą.
12. Stacje robocze powinny zostać skonfigurowane w taki sposób, aby standardowy użytkownik nie miał możliwości:
 - 1) samodzielnego modyfikowania ustawień w systemie operacyjnym;
 - 2) zmiany ustawień uruchomionych mechanizmów zabezpieczających.
13. Oprogramowanie zainstalowane na stacjach końcowych użytkowników powinno zostać skonfigurowane tak, aby nie dawało możliwości zapamiętania identyfikatora i hasła użytkownika.
14. ADO powinien podjąć działania mające na celu zmniejszenia do minimum możliwości przechowywania danych osobowych na stacjach roboczych.

15. W celu zmniejszenia do minimum możliwości przechowywania danych osobowych na stacjach roboczych ADO powinien udostępnić użytkownikom zasoby sieciowe, które będą wykorzystywane zarówno do przekazywania jak i magazynowania danych osobowych.
16. W przypadku udostępnienia użytkownikom przenośnych stacji roboczych ADO powinien zapewnić użytkownikom:
 - 1) środki zapewniające fizyczne bezpieczeństwo;
 - 2) bezpieczne miejsce, w którym pracownik może zostawić przenośną stację końcową po zakończeniu pracy.
17. ADO powinien prowadzić działania mające na celu inwentaryzację zarówno stacji końcowych, jak i użytkowanego oprogramowania.
18. Inwentaryzacja stacji końcowych może polegać na prowadzeniu spisu sprzętu lub uruchomieniu narzędzia, które umożliwiają inwentaryzację.
19. Dostęp do informacji dotyczących konfiguracji stacji końcowych powinien zostać udostępniony wyłącznie upoważnionym osobom.

9. Zasady zarządzania zewnętrznymi stacjami końcowymi

1. O ile ADO nie wyrazi zgody, żadna zewnętrzna stacja robocza nie może być podłączona do jego infrastruktury informatycznej.
2. W przypadku wyrażenia zgody na podłączenie stacji zewnętrznej, czyli prywatnej stacji osoby zatrudnionej u ADO lub stacji należącej do osoby nieposiadającej statusu osoby zatrudnionej u ADO, ale upoważnionej do przetwarzania danych osobowych, należy sprawdzić czy na stacji:
 - 1) zainstalowany został aktualny, wspierany przez producenta system operacyjny;
 - 2) funkcjonuje aktualna aplikacja chroniąca przed szkodliwym oprogramowaniem;
 - 3) funkcjonuje konto użytkownika standardowego z ograniczonymi do minimum możliwościami administrowania;
 - 4) uruchomiony został wygaszacz ekranu, skonfigurowany w identyczny sposób jak na stacjach roboczych należących do ADO.
3. W miarę możliwości technicznych ADO powinien stworzyć odseparowaną sieć dla urządzeń prywatnych.
4. Dodatkowo przed podłączeniem stacji zewnętrznej należy wykonać jej pełne skanowanie oprogramowaniem antywirusowym.
5. W przypadku konieczności przechowywania na zewnętrznej stacji roboczej danych osobowych należących do ADO, powinny zostać zastosowane środki kryptograficzne w celu ich zabezpieczenia.
6. Właściciel zewnętrznej stacji roboczej powinien wyrazić zgodę na możliwość dostępu do niej ADO w celu realizacji działań zabezpieczających, o którym mowa w niniejszym rozdziale.

10. Zasady dostępu zdalnego do infrastruktury ADO

1. Zdalny dostęp do sieci lokalnej ADO powinien być zabezpieczony poprzez uwierzytelnianie za pomocą identyfikatora i hasła lub innych metod uwierzytelnienia, nieopartych na hasle.
2. Zabronione jest korzystanie z rozwiązania posiadającego znane podatności bezpieczeństwa, które nie zostały naprawione przez producenta.
3. Aplikacja przeznaczona do zdalnego dostępu powinna zostać skonfigurowana w taki sposób, aby nieaktywne sesje były zamykane po przekroczeniu zdefiniowanego limitu czasu.
4. W celu ponownego nawiązania sesji zdalnego połączenia, użytkownik powinien ponownie się uwierzytelnić.

5. Jeżeli zamknięcie sesji może mieć negatywny wpływ na przetwarzane dane lub w znacznym stopniu utrudni pracę użytkownikom, ADO może odstąpić od zastosowania mechanizmu zamykającego nieaktywne sesje.
6. Rozwiązanie realizujące zdalny dostęp do sieci lokalnej ADO powinno:
 - 1) zapewniać poufność połączenia (szyfrowanie);
 - 2) zapobiegać nieautoryzowanemu i nienadzorowanemu przez ADO nawiązaniu połączenia;
 - 3) ograniczać dostęp do konkretnych elementów infrastruktury informatycznej ADO.
7. W miarę możliwości działanie użytkowników korzystających z dostępu zdalnego, a w szczególności pracowników podmiotów zewnętrznych, powinno być monitorowane przez ADO lub osobę przez niego wyznaczoną.
8. W przypadku pracowników podmiotów zewnętrznych zdalny dostęp powinien być przyznany tylko na podstawie umowy.
9. Umowa z podmiotem zewnętrznym powinna określać zasady związane ze zdalnym dostępem, które w szczególności powinny ustalać:
 - 1) zakres i okres dostępu;
 - 2) dane kontaktowe do osób, które będą wykonywać prace serwisowe;
 - 3) sposób komunikacji w ramach zgłaszania zadań serwisowych wykonywanych na odległość;
 - 4) nazwę oprogramowania, jakie będzie wykorzystywane do zdalnego połączenia;
 - 5) niezbędne wymagania bezpieczeństwa przetwarzania danych osobowych.
10. ADO powinien posiadać dostęp do rejestru prac wykonywanych przez pracowników podmiotów zewnętrznych z wykorzystaniem dostępu zdalnego.

11. Zasady zarządzania infrastrukturą sieciową

1. Połączenia pomiędzy siecią lokalną ADO a innymi sieciami:
 - 1) muszą zostać zatwierdzone przez ADO;
 - 2) powinny być realizowane w sposób zapewniający poufność przesyłanych danych osobowych.
 - 3) powinny być realizowane w sposób, który nie zagraża bezpieczeństwu infrastruktury ADO.
2. Miejsce styku sieci lokalnej ADO z innymi sieciami powinno zostać zabezpieczone zaporą sieciową, urządzeniem typu IDS/IPS.
3. W miarę możliwości należy zastosować segmentację sieć lokalnej.
4. Zmiany konfiguracyjne elementów lokalnej infrastruktury sieciowej powinny zostać zatwierdzone przez ADO.
5. Zmiany konfiguracyjne elementów lokalnej infrastruktury sieciowej powinien przeprowadzać tylko wykwalifikowany personel.
6. ADO powinien wykonywać kopię zapasową konfiguracji elementów sieci lokalnej.
7. ADO powinien prowadzić działania mające na celu inwentaryzację elementów sieci lokalnej wraz z oprogramowaniem zainstalowanym na takich elementach.
8. Inwentaryzacja elementów sieci lokalnej może polegać na prowadzeniu spisu sprzętu lub uruchomieniu oprogramowania, które umożliwi przeprowadzenie inwentaryzacji.
9. Dostęp do informacji dotyczących konfiguracji sprzętu sieciowego powinien zostać udostępniony wyłącznie upoważnionym osobom.
10. Konfiguracja elementów sieciowych powinna uwzględniać rejestrowanie najważniejszych zdarzeń, w szczególności należy rejestrować:
 - 1) wszelkie błędy i informacje o awariach;

- 2) nieudane próby logowania;
- 3) nieudane próby uzyskania dostępu do danych zasobów.

12. Zasady aktualizacji elementów środowiska informatycznego

1. Aktualizacja oprogramowania służącego do przetwarzania danych osobowych, jak i oprogramowania wspierającego przetwarzanie danych osobowych, powinna być wykonywana przez wykwalifikowany personel IT.
2. W miarę możliwości aktualizacja oprogramowania służącego do bezpośredniego przetwarzania danych osobowych powinna zostać poprzedzona testami wykluczającymi ich negatywny wpływ na proces przetwarzania danych osobowych.
3. W przypadku uzasadnionych wątpliwości świadczących o negatywnym wpływie aktualizacji na środowisko informatyczne odpowiedzialne za bezpośrednie przetwarzanie danych osobowych, ADO może podjąć decyzję o rezygnacji z wprowadzenia aktualizacji. Należy też podjąć kroki w celu zgłoszenia odpowiedniej poprawki do producenta oprogramowania.
4. W przypadku braku możliwości instalacji aktualizacji dotyczącej bezpieczeństwa, należy zastosować rozwiązania mających na celu minimalizację ryzyka związanego z wykorzystaniem podatności.
5. W przypadku braku przesłanek związanych z negatywnym wpływem aktualizacji na środowisko informatyczne odpowiedzialne za bezpośrednie przetwarzanie danych osobowych, aktualizacja powinna zostać wdrożona bez zbędnej zwłoki.
6. Przed aktualizacją systemu służącego do bezpośredniego przetwarzania danych osobowych, należy bezwarunkowo wykonać kopie, które zapewnią możliwość przywrócenia poprzedniej wersji oprogramowania w przypadku niepowodzenia aktualizacji.
7. Kopia wykonana przed aktualizacją systemu informatycznego powinna w szczególności obejmować:
 - 1) kopię danych osobowych;
 - 2) kopię konfiguracji systemu.
8. Oprogramowanie użytkowane przez ADO powinno mieć wsparcie producenta w zakresie udostępniania aktualizacji, a w szczególności poprawek związanych z bezpieczeństwem.
9. W miarę możliwości aktualizacja systemów operacyjnych powinna odbywać się automatycznie.

13. Zasady postępowania z nośnikami danych

1. ADO powinien podjąć działania mające na celu zmniejszenia do minimum wykorzystywania nośników do przenoszenia danych osobowych.
2. W celu zmniejszenia do minimum wykorzystywania nośników danych ADO powinien udostępnić użytkownikom zasoby sieciowe, które będą wykorzystywane zarówno do przekazywania, jak i magazynowania danych osobowych.
3. W miarę możliwości na stacjach roboczych, szczególnie narażonych na ryzyko dostępu osób nieupoważnionych (np. kontuar rejestracji lub recepcji) powinno się wyłączyć możliwość podłączenia i uruchomienia zewnętrznych nośników danych.
4. Z wymiennych nośników danych powinni korzystać tylko ci użytkownicy, którym nośniki niezbędne są do wykonania obowiązków służbowych.
5. W miarę możliwości ADO powinien specjalnie oznaczyć wymienne nośniki będące jego własnością tak, aby nie doszło do pomyłki z innym urządzeniem tego typu.

6. Wszystkie wymienne nośniki przed ich użytkowaniem powinny zostać sprawdzone za pomocą aktualnego oprogramowania antywirusowego zawierającego najnowsze bazy sygnatur wirusów.
7. ADO powinien zapewnić warunki gwarantujące bezpieczne przechowywanie nośników danych w czasie, gdy nie są wykorzystywane.
8. O ile ADO nie wyrazi zgody, żaden nośnik danych nie będący własnością ADO nie może zostać podłączony do stacji końcowych funkcjonujących w sieci ADO.
9. Wyrażenie zgody na wykorzystywanie wymiennych nośników danych niebędących własnością ADO powinno wiązać się z zapewnieniem dodatkowych środków bezpieczeństwa.
10. Osobom zatrudnionym, korzystającym z nośników danych, powinna zostać udostępniona instrukcja informująca o zasadach bezpiecznego korzystania z nośników, w szczególności uwzględniająca:
 - 1) skanowania nośnika programem antywirusowym;
 - 2) szyfrowania danych osobowych przechowywanych na nośniku;
 - 3) trwałego usuwania danych z nośnika.
11. W przypadku podjęcia decyzji o wykorzystywaniu prywatnych nośników danych, osoba zatrudniona powinna:
 - 1) wyrazić zgodę na wykorzystywanie prywatnego nośnika danych;
 - 2) zostać zobowiązana do dostarczenia nośnika do działu IT celem jego sprawdzenia i zabezpieczenia przed dostępem osób nieupoważnionych, m.in. poprzez zastosowanie środków kryptograficznych.
12. Osoby zatrudnione, wykorzystujące prywatne nośniki:
 - 1) w chwili cofnięcia przez ADO zgody na ich wykorzystywanie;
 - 2) w chwili, w której wykorzystywanie prywatnych nośników nie będzie już konieczne.- powinni zostać zobowiązani do przekazania nośników do działu IT celem usunięcia danych przetwarzanych w związku z wykonywaniem obowiązków służbowych.
13. Usuwanie danych powinno być realizowane przy użyciu oprogramowania, które uniemożliwi ich odtworzenie.
14. Dane osobowe znajdujące się na nośnikach powinny zostać niezwłocznie usunięte w przypadku:
 - 1) ustania przydatności danych (zakończył się czas ich przetwarzania);
 - 2) utylizacji nośników;
 - 3) sprzedaży urządzeń, w których znajdują się nośniki z danymi osobowymi.
15. Uszkodzone nośniki danych, w przypadku których nie można zastosować oprogramowania, które zapewni nieodwracalne wymazanie danych, powinny być niszczone fizycznie.
16. ADO powinien dysponować procedurą utylizacji nośników danych, precyzyjnie regulującą:
 - 1) zasady postępowania z różnymi rodzajami danych,
 - 2) zasady odpowiedniego bezpiecznego kasowania (jeśli to możliwe),
 - 3) zasady współpracy z podmiotami zewnętrznymi w zakresie utylizacji nośników lub urządzeń elektronicznych przetwarzających dane osobowe.
17. Jeżeli w procesie kasowania lub utylizacji nośników lub urządzeń zawierających dane osobowe uczestniczy podmiot zewnętrzny, współpraca z tym podmiotem powinna być oparta o odpowiednie uregulowanie prawne.
18. Proces utylizacji oraz trwałe usuwanie danych osobowych powinny zostać udokumentowane zgodnie z zasadą rozliczalności, wynikającą z RODO.

13. Zasady dotyczące przeglądów, konserwacji, modernizacji lub naprawy elementów środowiska informatycznego

1. Funkcjonujące elementy środowiska informatycznego powinny podlegać regularnym przeglądom i konserwacji.
2. Wszelkie czynności mające na celu przegląd, konserwację lub modernizację elementów infrastruktury informatycznej, powinny być przeprowadzone przez wykwalifikowany personel IT.
3. Wszelkie czynności, mające na celu przegląd, konserwację lub modernizację elementów infrastruktury informatycznej, powinny być realizowane zgodnie z instrukcjami producentów.
4. Wszelkie wykryte nieprawidłowości w działaniu sprzętu informatycznego lub oprogramowania wykorzystywanego do przetwarzania danych osobowych, należy niezwłocznie usunąć i zgłosić ADO.
5. Fakt przeprowadzenia przeglądu i działań mających na celu konserwację, powinien zostać udokumentowany.
6. W miarę możliwości wszelkie czynności mające na celu przeglądy, konserwacje lub modernizację powinny odbywać się w obszarze przetwarzania danych osobowych.
7. W wyjątkowych sytuacjach ADO może podjąć decyzję o przekazaniu sprzętu poza obszar przetwarzania danych, ale powinien wówczas wykonać działania mające na celu zabezpieczenie danych osobowych.
8. W sytuacji przekazania sprzętu poza obszar przetwarzania danych należy wymontować nośniki danych, usunąć z nich dane bądź zastosować środki ochrony kryptograficznej.
9. Nośniki z danymi, które zostały wymontowane na czas udostępnienia sprzętu poza obszar przetwarzania, należy przechowywać w bezpiecznym miejscu.
10. W przypadku konieczności przekazania nośników, na których znajdują się dane osobowe, poza obszar przetwarzania, należy podpisać stosowną umowę z podmiotem zewnętrznym.
11. W przypadku przekazania do naprawy lub konserwacji urządzenia, przed ponownym jego podłączeniem do sieci lokalnej ADO zawartość nośników danych powinna zostać sprawdzona za pomocą aktualnego oprogramowania antywirusowego, zawierającego najnowsze bazy sygnatur wirusów.

14. Zasady zabezpieczenia infrastruktury przed skutkami utraty zasilania

1. ADO powinien zastosować rozwiązania zapewniające ochronę przetwarzanych danych przed ich utratą, w przypadku wystąpienia nagłego zaniku napięcia w sieci energetycznej.
2. Elementy infrastruktury informatycznej odpowiedzialne za awaryjne zasilanie powinny zapewniać bezpieczne zakończenie pracy i umożliwić poprawne wyłączenie urządzeń.
3. W miarę możliwości ADO powinien ustanowić czynności mające na celu regularną kontrolę urządzeń zapewniających ochronę w przypadku nagłego zaniku zasilania.

15. Zasady współpracy z podmiotami zewnętrznymi, świadczącymi usługi informatyczne

1. W przypadku ograniczonych zasobów własnych, ADO powinien korzystać z usług podmiotów zewnętrznych.

2. ADO nie powinien traktować zlecenia jakichkolwiek usług podmiotowi zewnętrznemu jako zwolnienia z odpowiedzialności za bezpieczeństwo danych osobowych.
3. ADO powinien:
 - 1) regularnie weryfikować czynności wykonywane przez podmioty zewnętrzne.
 - 2) zawierać umowy określające odpowiedzialność podmiotów zewnętrznych oraz regulujące kwestie związane z dostępem do danych osobowych,
 - 3) współpracować z podmiotami, których kompetencje nie budzą wątpliwości co do jakości wykonanych usług.
4. Umowy zawierane przez ADO z zewnętrznymi dostawcami usług powinny zapewniać, że świadczenie usług odbywać się będzie zgodnie z wymaganiami prawnymi oraz standardami bezpieczeństwa przyjętymi przez ADO.
5. Pracownicy podmiotów zewnętrznych, wykonujący czynności na obszarze przetwarzania danych osobowych, przed rozpoczęciem prac powinni zostać poddani weryfikacji tożsamości.
6. Wszelkie czynności wykonywane przez podmiot zewnętrzny na obszarze przetwarzania danych osobowych, powinny odbywać się pod nadzorem ADO, a także powinny kończyć się podpisaniem protokołu z wykonania czynności lub ewentualnie raportem z wykonanej czynności.

16. Postanowienia końcowe

1. Nieprzestrzeganie zasad niniejszego dokumentu może być traktowane będzie jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku zatrudnienia na podstawie innej niż stosunek pracy.
2. ADO może dopuścić odstępstwo od zasad opisanych w niniejszym dokumencie pod warunkiem przeprowadzenia wcześniejszej analizy ryzyka związanego z takim odstępstwem.