Instrukcja informatyczna

w ŚCZ SPZOZ w Środzie Śląskiej

Niniejszy instrukcja stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych w systemach informatycznych:

* Pracowników
* Współpracowników
* Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora danych osobowych (ADO)/ Podmiot przetwarzający
* Użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez ADO/ Podmiot przetwarzający.

Każda z w/w osób powinna zapoznać się z poniższą instrukcją oraz zobowiązać się do stosowania zasad w niej zawartych.

1. POSTANOWIENIA OGÓLNE

Do pracy w sieci informatycznej służącej do przetwarzania danych osobowych może zostać dopuszczona tylko i wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych wydane przez ADO.

2. ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, PROGRAMÓW

1. Użytkownik przestrzega opracowane dla systemu zasady przetwarzania danych osobowych oraz procedury bezpieczeństwa.
2. Użytkownik dba, aby uniemożliwić dostęp do danych osobowych w systemie lub ich podgląd przez osoby nieupoważnione.
3. Użytkownik informuje ADO/ Administratora Systemu Informatycznego (ASI)/ Informatyka/ firmę zewnętrzną o wszelkich naruszeniach, podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych.
4. Użytkownik odpowiada za zabezpieczenie przed zniszczeniem, uszkodzeniem oraz utratą sprzętu IT (laptopów, urządzeń biurowych, smartfonów).
5. Użytkownik jest zobowiązany do usuwania tymczasowych plików z nośników/dysków z miejsc, gdzie dostęp do nich miałyby osoby nieupoważnione.
6. Użytkownik jest zobowiązany do przekazania ASI/ Informatyka/ firmy zewnętrznej i lub ADO nośniki przeznaczone do zniszczenia.

3. Do zadań ASI/ Informatyka/ firmy zewnętrzne w zakresie bezpieczeństwa należy dbanie, aby:

1. dyski twarde uszkodzone lub wyłączone z eksploatacji przed oddaniem do utylizacji trwale pozbawić zapisu lub zniszczyć dysk twardy w ten sposób, aby niemożliwym stało się odzyskanie informacji z niego.
2. uniemożliwić montaż/ demontaż, instalowanie lub podłączanie dodatkowych urządzeń do sieci informatycznej.
3. komputery zabezpieczyć przed skutkami awarii, bądź niestabilnego napięcia z sieci elektrycznej poprzez podłączenie UPS.
4. sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie przy wykorzystaniu oprogramowania zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych, bądź ustawienie automatyczne.
5. monitorowanie aktualizacji oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów, dokonywanych przez to oprogramowanie.
6. w dziennikach systemów odnotowane były działania użytkowników, lub obiektów systemowych – informacje te przechowywane są przez okres 6 miesięcy.
7. programy zainstalowane na stacjach roboczych i na komputerach przenośnych były użytkowane z zachowaniem praw autorskich oraz zgodnie z posiadanymi licencjami.
8. oprogramowanie typu Freeware, Shareware lub inne oprogramowanie dostarczane bez opłat (uznawane było jako nieautoryzowane), jeżeli nie otrzyma stosownej aprobaty ASI/ Informatyka/ firmy zewnętrznej.
9. zapewnienie synchronizacji zegarów wszystkich stosowanych systemów służących do przetwarzania danych osobowych z uzgodnionym, dokładnym źródłem czasu.
10. usługi, które nie są wykorzystywane były zablokowane.
11. Firma zewnętrzna/ informatyczna zapewnia opiekę informatyczną.

4. POZIOM BEZPIECZEŃSTWA

1. Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym połączonym z siecią publiczną, wprowadza się wysoki poziom bezpieczeństwa.
2. Środki bezpieczeństwa:
3. Obszar przetwarzania danych zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych;
4. Przebywanie osób nieuprawnionych w obszarze przetwarzania danych jest dopuszczalne za zgodą, w obecności osoby upoważnionej do przetwarzania danych osobowych;
5. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych;
6. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:
7. w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator,
8. dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia;
9. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
10. działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
11. utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej;
12. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie;
13. Obowiązek stosowania haseł o wymaganej składni leży po stronie użytkownika;
14. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych;
15. ASI/ Informatyk monitoruje wdrożone zabezpieczenia systemu informatycznego;
16. System informatyczny, służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem;
17. W przypadku zastosowania logicznych zabezpieczeń obejmują one:
18. kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych, a siecią publiczną,
19. kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych;
20. Wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej stosuje się środki kryptograficznej ochrony.

5. OCHRONA PRZED ZŁOŚLIWYM OPROGRAMOWANIEM

1. Na wszystkich komputerach został zainstalowany program antywirusowy ESET Endpoint, który chroni je przed zagrożeniami wynikającymi z działania złośliwego kodu. Za zarządzanie programem antywirusowym odpowiedzialny jest ASI/ Informatyk/ firma zewnętrzna.
2. Dostęp do systemu operacyjnego w którym przetwarzane są dane osobowe komputera posiadają wyłącznie osoby upoważnione; dostęp zabezpieczony jest za pomocą procesu uwierzytelniania z wykorzystaniem identyfikatora oraz hasła,

6. ZARZĄDZANIE UPRAWNIENIAMI - PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. Każdy użytkownik laptopów, komputerów, programów i systemu operacyjnego zobowiązany jest do pracy na własnym koncie (poprzez wpisanie identyfikatora i hasła). Zabronione jest udostępnianie konta innemu użytkownikowi.
2. Użytkownik nie może zmieniać swoich uprawnień, np. zostać Administratorem na swoim laptopie/ komputerze.
3. Użytkownik laptopa/ komputera oraz programów rozpoczyna i kończy pracę logowaniem i wylogowaniem się.
4. Odpowiednie ustawienie monitorów powinno uniemożliwiać podgląd wyświetlanych danych bądź poprzez stosowanie filtrów zabezpieczających.
5. W monitorach zastosowano wygaszacze ekranu, ustawione na 15 minut. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła.
6. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom) wglądu do danych wyświetlanych na monitorach – tzw. **Polityka czystego ekranu.**
7. Użytkownik przed tymczasowym odejściem od laptopa/ komputera musi włączyć wygaszacz ekranu lub wylogować się z systemu, bądź z programu.
8. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
9. Na zakończenie pracy, po wylogowaniu się użytkownik zobowiązany jest dodatkowo zabezpieczyć nośniki magnetyczne, na których znajdują się dane osobowe.

7. POLITYKA HASEŁ

1. ADO/ ASI ustala hasło administracyjne dla sieci komputerowej zarządzanej w jednostce.
2. Hasło do systemu informatycznego (tzn. dla użytkowników posiadających uprawnienia na poziomie administratorów systemów informatycznych) jest zabezpieczone u ADO na wypadek sytuacji awaryjnych, szczególnie w przypadku nieobecności ASI/ Informatyka.
3. Hasła użytkowników powinny składać się minimum z 8 znaków.
4. Hasła te powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne).
5. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami.
6. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na laptopie, nie trzymać pod klawiaturą lub w szufladzie.
7. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.
8. Użytkownik wprowadza swoje hasło w sposób uniemożliwiający innym osobom jego poznanie.
9. W przypadku ujawnienia hasła – należy natychmiast go zmienić.
10. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.
11. ASI/ Informatyk usuwa lub blokuje zbędne identyfikatory użytkowników oraz kont w systemach informatycznych.
12. Należy unikać ponownego lub cyklicznego używania starych haseł.
13. Zmiana haseł dostępowych następuję przynajmniej raz na 30 dni.

8. PROCEDURA TWORZENIA KOPII ZAPASOWYCH

1. Kopie bezpieczeństwa powinny być wykonywane regularnie, według wcześniej ustalonych zasad. Serwery – 2 razy dziennie.
2. W celu zapewnienia poprawności wykonywania kopii bezpieczeństwa należy regularnie poddawać testowi wybraną kopię. Informacja zwrotna w programie beckapowym o prawidłowości kopii. Weryfikacja, czy dany dokument się otwiera, ręczna.
3. Kopie bezpieczeństwa powinny być wykonywane w taki sposób by zminimalizować koszty ewentualnej awarii.
4. Zabrania się przechowywania kopii zapasowych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.
5. W miarę możliwości zbiorcze kopie zapasowe przechowywane są w innej lokalizacji. Za bezpieczne przechowywanie kopii ich oznakowanie oraz regularne sprawdzanie przydatności odpowiada ASI/ Informatyk/ firma zewnętrzna.
6. Kopie zapasowe:
7. przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
8. usuwa się niezwłocznie po ustaniu ich użyteczności.

9. PRZECHOWYWANIE ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

1. Decyzję o likwidacji zbiorów danych osobowych, przetwarzanych w systemach informatycznych podejmuje ADO.
2. Zbiory danych w formie elektronicznej przechowywane są na macierzy i serwerze.
3. Elektroniczne nośniki danych (pamięci flash, nośniki optyczne, itp.), na których znajdują się dane osobowe muszą być przechowywane w miejscach, do których dostęp jest ograniczony.
4. Po wykorzystaniu danych z elektronicznego nośnika informacji, nośnik ten należy zniszczyć lub trwale usunąć z niego dane.
5. Pracownik bierze odpowiedzialność za korzystanie z prywatnych nośników magnetycznych, optycznych oraz pamięci przenośnych.
6. Pracownik jest zobowiązany do odpowiedniego zabezpieczenia danych przechowywanych na powierzonym mu sprzęcie.

10. ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI POZA FIRMĘ/ORGANIZACJĘ

1. Użytkownicy nie mogą wynosić na zewnątrz niezaszyfrowanych nośników z danymi osobowymi (np. laptopów, smartfonów, przenośnych dysków twardych).
2. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski przenośne, zahasłowane pliki, zabezpieczone laptopy i smartfony).
3. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych;
4. Urządzenia mobilne są chronione za pomocą programu zabezpieczającego przed szkodliwą działalnością (programy antywirusowe).
5. Tylko osoby upoważnione mają możliwość pracy na komputerach przenośnych poza jednostką.
6. Należy w miarę posiadanych możliwości zabezpieczać sprzęt przed kradzieżą.
7. Zabrania się:
8. Pozostawiania sprzętu bez nadzoru w przestrzeni publicznej.
9. Pozostawiania sprzętu w samochodzie w widocznym miejscu.
10. Użyczania sprzętu osobom trzecim.
11. Pozostawiania sprzętu pod nadzorem osób trzecich.
12. Użytkownicy przetwarzający dane osobowe na komputerach przenośnych obowiązani są do systematycznego wprowadzania tych danych w określone miejsca na zasobach sieciowych administratora danych, a następnie do trwałego usuwania ich z pamięci powierzonych komputerów przenośnych.
13. Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach przenośnych. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zgłosić to do ASI/ Informatykowi.

11. ZASADY KORZYSTANIA Z INTERNETU

1. Zabrania się instalowania programów z Internetu bez konsultacji z ASI/ Informatykiem.
2. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez takie oprogramowanie.
3. Zabrania się wchodzenia na strony z nielegalnym oprogramowaniem do pobrania oraz na hackerskie.
4. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.

12. ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Pliki w danymi osobowymi w Wordzie, Excelu, w Pdf lub spakowane (7zip), przed wysłaniem ich do osób trzecich powinny być zahasłowane, a hasło powinno być przesłane do odbiorcy telefonicznie lub SMS.
2. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum (np. 6) znaków: duże i małe litery i cyfry lub znaki specjalne.
3. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
4. **WAŻNE:** Nie otwierać załączników (.zip, .rar, .xlsm, .pdf, .exe) w mailach!!!!! Są to zwykle „wirusy”, które infekują laptop oraz sieć. WYSOKIE RYZYKO UTRATY BEZPOWROTNEJ UTRATY DANYCH.
5. **WAŻNE:** Nie wolno „klikać” na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron z „wirusami”. Użytkownik „klikając” na taki hiperlink infekuje laptop oraz inne komputery w sieci. WYSOKIE RYZYKO UTRATY BEZPOWROTNEJ UTRATY DANYCH.
6. Należy zgłaszać ASI przypadki podejrzanych e-maili.
7. Użytkownicy nie powinni rozsyłać „niezawodowych” e-maili w formie „łańcuszków szczęścia”.
8. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „**Ukryte do wiadomości** **– UDW**”. Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości”!.
9. Użytkownicy powinni okresowo kasować niepotrzebne maile.
10. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób, bez zgody ADO.
11. Użytkownik bez zgody ADO nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące ADO, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

13. PRZEGLĄDY I KONSERWACJE Sprzętu, w tym NOŚNIKÓW INFORMACJI

1. Osobą odpowiedzialną za prawidłowe działanie sieci informatycznej jest ASI/ Informatyk, firma informatyczna.
2. ASI/ Informatyk/ firma zewnętrzna dokonuje napraw i konserwacji sieci informatycznej.
3. Gdy naprawa sprzętu komputerowego znajdującego się w jednostce musi odbyć się w serwisie zewnętrznym lub przez osobę niebędącą upoważnioną do przetwarzania danych osobowych, ASI/ Informatyk/ firma zewnętrzna zobowiązany jest do odpowiedniego zabezpieczenia danych znajdujących się na dyskach urządzenia.
4. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
5. likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
6. przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
7. naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez ADO;

14. SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Procedura postępowania w przypadku naruszenia ochrony danych osobowych opisana w Polityce bezpieczeństwa.

15. SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY SYSTEMAMI

Opis struktury danych w poszczególnych systemach informatycznych oraz sposób połączeń z innymi systemami przedstawione są w dokumentacjach technicznych programów.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| L.p. | Nazwa systemu eksportującego dane | Nazwa systemu importującego dane | Kategorie danych osobowych podlegające eksportowi do drugiego systemu | Sieć wykorzystana do transmisji danych. Technologia wymiany danych (automatyczna, półautomatyczna, ręczna) |
| PŁATNIK | ZUS | Zarejestrowanie i wyrejestrowanie pracowników płatnika składek i członków ich rodzin, zmiana ich danych, rozliczenia miesięczne itp. Zakres danych określają przepisy prawa. | Sieć INTERNET. Technologia półautomatyczna | Sieć Internet. Technologia półautomatyczna. |
| ZUS | PŁATNIK | Potwierdzenie wykonanej operacji | INTERNET. Technologia automatyczna | Wewnętrzna sieć. Technologia półautomatyczna. |

Bankowość elektroniczna – logowanie on-line.

16. POSTANOWIENIA KOŃCOWE

Niezastosowanie się do procedur określonych w niniejszej instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane, jako ciężkie naruszenie obowiązków pracowniczych i obciążone odpowiedzialnością dyscyplinarną, zgodnie z przepisami prawa pracy.