	Gminny Ośrodek Pomocy Społecznej w Mirczu
	Dokument Polityki Ochrony Danych Osobowych

Regulamin Ochrony Danych Osobowych

w Gminnym Ośrodku Pomocy Społecznej w Mirczu

Sporządził:	**Przyjął i zatwierdził:**	
ADIGAN Ewa Nowak TARNOSZYN 109, 22-678 ULHÓWEK tel. 506 575 235 REGON 061456177 NIP 922-173-73-[illegible] e-mail: szkolenia@adigan.pl INSPEKTOR OCHRONY DANYCH (data protection officer) mgr Adam Jan SKORNIEWSKI	KIEROWNIK mgr [illegible] Administrator Danych	
Nr dok. Załącznik nr 15 do Polityki Ochrony Danych Osobowych Gminnego Ośrodka Pomocy Społecznej w Mirczu	**Data wydania**	**Wersja:** 1
Niniejszy dokument wraz z załącznikami jest własnością Gminnego Ośrodka Pomocy Społecznej w Mirczu. Prawa zastrzeżone. Kopiowanie i rozpowszechnianie całości lub części dokumentu wyłącznie za zgodą Kierownika Gminnego Ośrodka Pomocy Społecznej w Mirczu.		

Poniższe zapisy stanowią wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (EU) 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 (ogólne rozporządzenie o ochronie danych) dla:

- Pracowników
- Współpracowników
- Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający
- Użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający

Każda z wyżej wymienionych osób ma obowiązek zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych.

Spis treści:

1. Zasady zarządzania oraz bezpiecznego używania sprzętem i oprogramowaniem informatycznym.

1. Pracownicy Gminnego Ośrodka Pomocy Społecznej w Mirczu, wykonujący prace na sprzęcie informatycznym będącym na wyposażeniu Ośrodka, mogą korzystać wyłącznie z komputerów oraz oprogramowania, na które Ośrodek posiada aktualne licencje i które ujęte są w metrykach komputerów **(załącznik Nr 15a)** określających oprogramowanie oraz sprzęt informatyczny przydzielony pracownikowi. Metryki prowadzi Administrator Systemów Informatycznych.
2. Pracownicy, o których mowa w pkt. 1, ponoszą odpowiedzialność przewidzianą w obowiązujących przepisach prawa w przypadku korzystania z nielegalnego oprogramowania oraz naruszania praw autorskich i zasad zarządzania oprogramowaniem. Pracownicy korzystający z w/w oprogramowania zobowiązani są do podpisania oświadczenia w sprawie korzystania ze sprzętu informatycznego i oprogramowania **(załącznik nr 15b).**
3. Decyzja o zakupie nowego oprogramowania na potrzeby Ośrodka wymaga opinii Kierownika Ośrodka oraz Administratora Systemu Informatycznego.
4. Instalacji zakupionego oprogramowania może dokonywać osobiście Administrator Systemów Informatycznych lub osoby upoważnione przez Kierownika Ośrodka.
5. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu informatycznego zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem. W postaci sprzętu informatycznego rozumiemy: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, zewnętrzne nośniki pamięci (pendrive, dysk zewnętrzny, itp.), służbowe tablety i smartfony.
6. Samowolne otwieranie (demontaż) sprzętu IT, instalacja dodatkowych urządzeń (np. twardych dysków, pamięci)lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
7. Obowiązkiem użytkownika w razie zagubienia, utraty lub zniszczenia powierzonego mu sprzętu jest natychmiastowe zgłoszenie Kierownikowi Ośrodka i Inspektorowi ochrony danych.
8. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych wydziałów) wgląd do danych wyświetlanych na monitorach komputerowych – tzw. polityka czystego ekranu.
9. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wylogować się z systemu bądź z programu i wywołać blokowany hasłem wygaszacz ekranu (WINDOS + L).
10. Po zakończeniu pracy, użytkownik zobowiązany jest:
    a. wylogować się z systemu informatycznego, a jeśli to wymagane - następnie wyłączyć sprzęt komputerowy,
    b. zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne na których znajdują się dane osobowe.
11. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów).

12. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien **TRWALE** zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD w niszczarce, zniszczenie twardego dysku). Kwestie szczegółowe reguluje Polityka niszczenia danych **(załącznik Nr 15c).**
13. Użytkownicy komputerów przenośnych na których znajdują się dane osobowe lub z dostępem do danych osobowych przez Internet zobowiązani są do stosowania zasad bezpieczeństwa zawartych w Polityce komputerów przenośnych, urządzeń mobilnych oraz nośników zewnętrznych **(załącznik nr 15d).**
14. Zabrania się umieszczania w urządzeniach odczytujących dane na stanowisku (stacje dyskietek, czytniki CD-ROM, DVD, porty USB itp.) nośników rozprowadzanych z różnego rodzaju czasopismami, materiałami reklamowymi oraz niewiadomego pochodzenia (znalezione) itp.
15. Zabrania się używania na stanowisku pracy urządzeń do gromadzenia i przenoszenia danych, takich jak pamięci „flash" dołączane przez porty USB, karty radiowe, urządzenia „bluetooth", dyski wymienne, modemy nie będących własnością Ośrodka. Wykaz dopuszczonych do używania w Ośrodku nośników zawiera Ewidencja komputerów przenośnych, urządzeń mobilnych oraz nośników zewnętrznych.
16. Zabrania się wykorzystywania do celów służbowych bez zgody Administratora Danych, innych niż dopuszczony w Ośrodku, systemu poczty elektronicznej.
17. **Z uwagi na próby ataków na systemy użytkowników poprzez zainfekowanie poczty elektronicznej zaleca się zachowanie szczególnej ostrożności przy otwieraniu otrzymanych tą drogą załączników. W przypadku otrzymania nieoczekiwanej przesyłki pocztowej, która zawiera załącznik lub odsyła do treści bezpośrednio do strony internetowej zaleca się aby nie otwierać załącznika ani nie korzystać bezpośrednio z przesłanych odnośników i poinformować o takim przypadku Administratora Danych.**
18. Zaleca się wyłączenie opcji auto podglądu załącznika w programie pocztowym.
19. Korzystając z programów MS Office (Word, Excel itp.) i podobnych należy, jeśli to możliwe, uaktywnić ich wewnętrzny system ochrony przed wirusami MAKRO.
20. Każdy nośnik danych, używany do przenoszenia danych pomiędzy stanowiskami komputerowymi, przed odczytaniem danych należy sprawdzić programem antywirusowym.

2. Zasoby

1. Ośrodek jest właścicielem treści wszystkich zasobów i aktywów, włączając: sprzęt komputerowy, oprogramowanie, sieci, system telefoniczny, dane, jak i wszystkie dane przepływające przez sieć Ośrodka. Do tych danych zalicza się wiadomości poczty elektronicznej i głosowej (włączając osobiste wiadomości przesyłane na służbowy adres) oraz wszystkie dane elektroniczne przechowywane w jakiejkolwiek formie na jakimkolwiek nośniku.
2. ASI ma dostęp do wszystkich zasobów informatycznych będących własnością Ośrodka, w celu ich ochrony, konserwacji lub z innych powodów ważnych dla funkcjonowania Ośrodka. W szczególności ASI ma dostęp do każdej informacji zawartej w tych zasobach i może ją ujawnić Kierownikowi Ośrodka lub osobie

upoważnionej przez niego.

3. W Ośrodku prowadzony jest Rejestr Licencji i Instalacji Oprogramowania oraz sprzętu IT zwany dalej „Rejestrem". Prowadzenie Rejestru zleca się Administratorowi Systemów Informatycznych.
4. Oryginalna dokumentacja licencyjna będąca w dyspozycji Ośrodka przechowywana jest w jednym miejscu, w zamkniętym pomieszczeniu, do którego mają dostęp osoby upoważnione przez Administratora Danych.
5. W Ośrodku dokonuje się przynajmniej raz w roku kontroli zgodności sprzętu IT oraz zainstalowanego oprogramowania z oprogramowaniem zawartym w „Metryce komputera". Kontrola należy do zadań Administratora systemów informatycznych.
6. Od pracowników Ośrodka wymaga się, aby – na wniosek ASI, zaakceptowany przez Kierownika Ośrodka – udostępnili wszelkie dane zapisane na powierzonym im przez Ośrodka nośniku.

3. Zgłaszanie i usuwanie usterek

1. Problemy ze sprzętem komputerowym lub systemem informatycznym należy zgłosić go do ASI
2. Zgłaszając usterkę należy podać:
    - lokalizację w której usterka wystąpiła,
    - w miarę dokładny opis problemu.

4. Zarządzanie uprawnieniami.

1. Administrator systemów informatycznych dla każdego upoważnionego przez Administratora danych użytkownika ustanawia parametry stanowiska roboczego oraz udostępnia zasoby, a następnie dokonuje konfiguracji stanowiska roboczego.
2. Administrator systemów informatycznych zakłada konto lub zmienia parametry konta i przekazuje użytkownikowi wszystkie dane niezbędne do korzystania z niego, w tym hasło do pierwszego zalogowania się. W przypadku likwidacji konta administrator usuwa lub blokuje konto w terminie określonym w upoważnieniu Administratora danych.
3. Administrator systemów informatycznych ma prawo zablokować dostęp do funkcji i zasobów systemu w przypadku stwierdzenia niewłaściwego, niezgodnego z treścią upoważnienia wykorzystywania stanowiska roboczego.
4. Każdy użytkownik z dostępem do danych osobowych (np. na swoim komputerze, na dysku sieciowym, w programie lub aplikacji, w poczcie elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się.
5. Użytkownicy nie mają prawa do samodzielnej zmiany uprawnień, np. przydzielenia sobie uprawnień administratora w Windows.
6. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest zatem umożliwianie innym osobom praca na koncie innego użytkownika

7. Posługiwanie się danymi identyfikującymi lub uwierzytelniającymi należącymi do innego użytkownika w celu dostępu do zasobów sieci komputerowej Ośrodka na jego konto lub podejmowania jakichkolwiek innych działań, a zwłaszcza wykorzystanie podpisu elektronicznego w jego imieniu jest zabronione
8. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
9. Obszar, w którym są przetwarzane dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne za zgodą Administratora Danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
10. W systemie informatycznym służącym do przetwarzania danych osobowych, przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie nadane przez Administratora Danych.
11. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
12. W przypadku, gdy pracownicy Ośrodka używają w pracy systemu informatycznego udostępnianego przez zewnętrzną instytucję (np.: ministerstwo) ochronie podlegają jedynie dane i programy umożliwiające uwierzytelnienie i dostęp do ww. systemu (np.: loginy, hasła, certyfikaty). Należy wtedy oprócz stosowania się do zasad opisanych w niniejszej instrukcji, stosować się do zaleceń i polityki bezpieczeństwa instytucji udostępniającej system. Pracownicy Ośrodka korzystają z systemu udostępnionego przez zewnętrzne instytucje wyłącznie w siedzibie Ośrodka i w godzinach pracy Ośrodka, na sprzęcie komputerowym przeznaczonym do celów służbowych, chyba, że ustalenia z instytucją udostępniającą system stanowią inaczej lub specyfika pracy w tym systemie wymaga odstąpienia od tej zasady.

5. Polityka haseł

1. **Minimalna długość hasła powinna wynosić 8 znaków .**
2. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne).
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami czyli słownikowe. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów.
4. Nie należy używać haseł wynikających z układu klawiatury (np. qwerty, 12345678 itp.).
5. Hasło nie może się powtarzać.
6. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach
   i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
7. W przypadku ujawnienia hasła –należy natychmiast go zmienić.

8. Hasła muszą być zmieniane co 90 dni.
9. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.
10. Hasła do kont o wysokich uprawnieniach są przechowywane w zamkniętej kopercie w Ośrodku - Karta haseł **(Załącznik nr 15e).** Dostęp do karty mają upoważnione osoby.
11. Uprawnionymi do otwarcia karty są Administrator Danych oraz Administrator Systemów Informatycznych.

6. Zabezpieczenie dokumentacji papierowej z danymi osobowymi.

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „Polityki czystego biurka". Polega ona na zabezpieczaniu (zamykaniu) dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji - szczegółowe informacje zawarte są Polityce niszczenia danych.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych miejskich lub w lesie.
5. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach.
6. Należy korzystać ze sprawdzonych firm kurierskich.
7. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.

7. Zasady korzystania z Internetu

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT (Administrator Systemów Informatycznych) i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo.

5. Nie należy w opcjach przeglądarki internetowej włączać opcji auto uzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

8. Zasady korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania danych osobowych poza organizację należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych, podpis elektroniczny).
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 12 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. **WAŻNE:** Nie należy otwierać załączników (plików) w mailach nawet od rzekomo znanych nam nadawców bez weryfikacji tegoż nadawcy. Tego typu maile większości przypadków zawierają załączniki ze szkodliwymi programami, które po „kliknięciu" infekują komputer użytkownika oraz często pozostałe komputery w sieci. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy.
7. **WAŻNE:** Bez weryfikacji wiarygodności nadawcy, nie należy „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych. Użytkownik „klikając" na taki hiperlink bezwiednie infekuje swój komputer oraz często pozostałe komputery w sieci. W wyniku takiej infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy
8. Należy zgłaszać ASI przypadki podejrzanych emaili.
9. 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"!
10. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.

11. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
12. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
13. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.
14. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
15. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
16. Użytkownik bez zgody Administrator Danych nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Administratora Danych, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.
17. Podczas wymiany korespondencji e-mail między kontrahentami szczególnie w księgowości należy zachować nadzwyczajną czujność w przypadku prośby o zmianę np. konta bankowego, adresu itp. Informacje te należy potwierdzić innymi środkami kontaktu (telefon, poczta tradycyjna, osobisty kontakt).

9. Ochrona antywirusowa

W zakresie profilaktyki antywirusowej wprowadza się metody i działania związane z profilaktyką antywirusową w systemach informatycznych użytkowanych w sieci komputerowej Ośrodka. Osobą prowadzącą działania profilaktyczne mające na celu ochronę zasobów sieci komputerowej Ośrodka przed atakami wirusów komputerowych jest Administrator Systemów Informatycznych.

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym.
2. Zabronione jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, zainstaluj program antywirusowy", użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie ASI lub osobę upoważnioną.
4. Jeśli program antywirusowy stwierdził istnienie wirusa na nośniku danych, taki nośnik należy natychmiast wyjąć z czytnika (stacji dyskietek, czytnika DVD-ROM, USB itp.), wyraźnie oznaczyć i przekazać nośnik administratorowi bezpieczeństwa informacji. Następnie należy sporządzić notatkę służbową ze zdarzenia i przeprowadzić kontrolę antywirusową całego systemu.
5. Po stwierdzeniu obecności wirusa w systemie przez program antywirusowy, jeśli to możliwe, należy zezwolić programowi antywirusowemu na usunięcie wirusów. Jeśli program antywirusowy nie będzie mógł usunąć wirusów nie niszcząc części lub

całości zbioru zainfekowanego wirusem, należy przerwać działanie programu antywirusowego i natychmiast zgłosić ten fakt administratorowi bezpieczeństwa informacji.

6. Użytkownik ma obowiązek zgłaszania do ASI wszelkich zauważonych niestandardowych zachowań systemu antywirusowego.

10. Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

1. Każda osoba upoważniona do przetwarzania danych osobowych lub której została udzielona zgoda na przebywanie w miejscu przetwarzania danych zobowiązana jest do powiadomienia bezpośredniego przełożonego, Inspektora ochrony danych osobowych lub Administratora Danych w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.

2. Do sytuacji wymagających powiadomienia, należą:
   a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą
      i utratą danych osobowych,
   c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do incydentów wymagających powiadomienia, należą:
   a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych),
   c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
4. Typowe przykłady incydentów wymagające reakcji:
   a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
   b. dokumentacja jest niszczona bez użycia niszczarki,
   c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie ,
   d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
   e. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe,
   f. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia Pracodawcy / Zleceniodawcy,
   g. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,

h. telefoniczne próby wyłudzenia danych osobowych,
i. kradzież, zagubienie komputerów lub CD, twardych dysków, Pen-drive z danymi osobowymi,
j. maile zachęcające do ujawnienia identyfikatora i/lub hasła,
k. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
l. hasła do systemów przyklejone są w pobliżu komputera .

Szczegółowe informacje zawarte są w Instrukcji postępowania z incydentami **(Załącznik nr 19).** Niepoinformowanie natychmiastowe bezpośredniego przełożonego, Administratora Danych lub Inspektora ochrony danych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.

11. Obowiązek zachowania poufności i ochrony danych osobowych

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora Danych zadaniach,
   b. zachowania w tajemnicy danych osobowych do których mam lub będzie miał/a dostęp w związku z wykonywaniem obowiązków służbowych powierzonych przez Administratora Danych,
   c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora Danych,
   d. zabezpieczenia tych danych przed dostępem osób nieupoważnionych, a następnie przekazanie ich do dyspozycji osób upoważnionych,
   e. zgłaszania sytuacji (incydentów) naruszenia zasad ochrony danych osobowych Inspektorowi Ochrony Danych lub bezpośredniemu przełożonemu,
   f. do zachowania w tajemnicy wszelkich informacji na temat sposobów zabezpieczeń danych osobowych przetwarzanych w Ośrodka,
   g. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.
2. Jeśli jest to przewidziane, osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych.
3. Osoby zapoznane z treścią niniejszego Regulaminu i przeszkolone zobowiązane są podpisać Oświadczenie o poufności.
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.
5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.

12. Procedura napraw w serwisach zewnętrznych

1. Komputery przeznaczone do naprawy należy wysyłać bez dysków a urządzenia mobilne
   bez kart pamięci.
2. W przypadku naprawy sprzętu z danymi osobowymi na nośniku należy je wpierw trwale usunąć z użyciem specjalistycznego oprogramowania.
3. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest zawarcie specjalnego zapisu w umowie serwisowej, gwarantującego bezpieczną naprawę (należy na to zwrócić uwagę przy zakupach sprzętu).
4. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku / karcie pamięci. Sprzęt przekazywany jest do serwisu bez podania hasła.
5. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta (umowy gwarancyjne on-site).

13. Postępowanie dyscyplinarne

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Pracodawcę/Zleceniodawcę za naruszenie przepisów karnych zawartych w Rozporządzeniu 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 (ogólne rozporządzenie o ochronie danych), a także Ustawy o Ochronie Danych Osobowych z dnia 10 maja 2018 roku (Dz. U. poz. 1000).

Administrator Danych

KIEROWNIK
mgr Katarzyna Górniak-Kudełka