ZARZĄDZENIE NR 31/2018
DYREKTORA CENTRUM USŁUG WSPÓLNYCH W NOWEJ SARZYNIE
z dnia 19 listopada 2018 r.

w sprawie wprowadzenia Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Centrum Usług Wspólnych w Nowej Sarzynie

Na podstawie art. 32 Rozporządzenia 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,

zarządzam, co następuje:

§ 1

Wprowadza się Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Centrum Usług Wspólnych w Nowej Sarzynie, stanowiącą załącznik do zarządzenia.

§ 2

Traci moc zarządzenie Nr 10/2017 z dnia 31 maja 2017 r. Dyrektora Centrum Usług Wspólnych w Nowej Sarzynie w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych przetwarzanych w Centrum Usług Wspólnych w Nowej Sarzynie oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Centrum Usług Wspólnych w Nowej Sarzynie.

§ 3

Nadzór nad realizacją zarządzenia powierza się Dyrektorowi Centrum Usług Wspólnych w Nowej Sarzynie.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Centrum Usług Wspólnych w Nowej Sarzynie
Józef Dziurdź

Załącznik do zarządzenia Nr 31/2018
Dyrektora Centrum usług Wspólnych
w Nowej Sarzynie
z dnia 19 listopada 2018 r .

Zatwierdzam:

.....

ADO
Inspektor Ochrony Danych Osobowych
Iwona Wysocka

.....

IOD

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W CENTRUM USŁUG WSPÓLNYCH W NOWEJ SARZYNIE

Nowa Sarzyna 2018

SPIS TREŚCI

1. Postanowienia ogólne

1.1 Podstawa prawna

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE nakłada na administratora danych osobowych następujące obowiązki:

a) pseudonimizację i szyfrowanie danych osobowych,
b) zapewnienie poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
c) zapewnienie szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydenty fizycznego lub technicznego,
d) zapewnienie regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić skuteczność przetwarzania.
e) zabezpieczenie danych przed nieuprawnionym dostępem,
f) zabezpieczenie danych przed udostępnieniem osobom nieupoważnionym (nieuprawnionym pozyskaniem),
g) zabezpieczenie przed utratą danych,
h) zabezpieczenie przed uszkodzeniem lub zniszczeniem danych oraz przed ich nielegalną modyfikacją.

1.2 Definicje

Ilekroć w niniejszym dokumencie jest mowa o:

1) CUW – należy przez to rozumieć Centrum Usług Wspólnych w Nowej Sarzynie,
2) Administratorze Danych Osobowych (ADO) – należy przez to rozumieć Dyrektora Centrum Usług Wspólnych w Nowej Sarzynie,
3) Inspektorze Ochrony Danych Osobowych (IOD) – rozumie się przez to Inspektora Ochrony Danych wyznaczonego przez ADO;
4) Administratorze Systemu Informatycznego (ASI) – należy przez to rozumieć pracownika CUW zatrudnionego na stanowisku specjalisty ds. obsługi i konserwacji i konserwacji urządzeń audiowizualnych, akustycznych i komputerowych,
5) danych osobowych – należy przez to rozumieć informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub

pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

6) zgodzie osoby, której dane dotyczą - należy przez to rozumieć dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
7) naruszeniu ochrony danych osobowych - należy przez to rozumieć naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
8) pseudonimizacji - należy przez to rozumieć przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
9) zbiorze danych - należy przez to rozumieć uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
10) udostępnieniu danych osobowych – należy przez to rozumieć jedną z operacji wykonywanych na danych osobowych, polegającą na przekazaniu lub okazaniu ich treści podmiotowi lub osobie będącej odbiorcą danych osobowych;
11) utrwalaniu danych – należy przez to rozumieć zapisywanie danych w sposób trwały na wszelkiego rodzaju nośnikach papierowych lub elektronicznych;
12) usuwaniu danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
13) uwierzytelnianiu (autentykacji) – należy przez to rozumieć proces, celem którego jest zweryfikowanie zadeklarowanej tożsamości osoby, urządzenia lub usługi biorącej udział w wymianie danych;

14) użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym CUW. Użytkownikiem może być pracownik CUW, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w CUW,

15) zabezpieczeniu danych w systemie informatycznym – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

16) systemie informatycznym – jest to zbiór powiązanych ze sobą elementów, którego funkcją jest przetwarzanie danych przy użyciu techniki komputerowej w CUW.

1.3 Cel

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Centrum Usług Wspólnych w Nowej Sarzynie zwana dalej „Instrukcją" jest wewnętrznym dokumentem CUW i określa sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w zbiorach danych.

2. Instrukcja odnosi się do organizacji, metod i trybu przetwarzania danych osobowych oraz konserwacji systemu informatycznego oraz użytych w tym celu środków organizacyjnych i technicznych, ustanawianych przez Administratora Danych Osobowych, a także określa tryb dopuszczania do zasobów systemu informatycznego użytkowników oraz specjalistów z zakresu konserwacji sprzętu i oprogramowania.

3. Instrukcja ma zapewnić zabezpieczenie zasobów technicznych systemu informatycznego, ochronę oprogramowania i danych osobowych przed nieuprawnionymi działaniami (wgląd, modyfikacja, pozyskanie i dalsze ujawnienie), a także przed ich utratą.

4. Instrukcja przeznaczona jest dla pracowników CUW upoważnionych do przetwarzania danych osobowych przez Administratora Danych Osobowych.

2. Nadawanie/odbieranie uprawnień do przetwarzania danych w systemie informatycznym

Dane osobowe w systemie informatycznym w CUW może przetwarzać wyłącznie osoba posiadająca aktualne, ważne pisemne upoważnienie do przetwarzania danych osobowych.
W przypadku ustania stosunku pracy/zmiany zakresu obowiązków użytkownika, następuje odebranie użytkownikowi praw dostępu do systemu informatycznego.

TRYB POSTĘPOWANIA

1. Dane osobowe w systemie informatycznym może przetwarzać wyłącznie osoba posiadająca aktualne, ważne, pisemne upoważnienie do przetwarzania danych osobowych.
2. Zarejestrowanie użytkownika w systemie informatycznym i nadanie mu upoważnienia do przetwarzania danych osobowych następuje na wniosek kierownika administracyjnego, którego wzór stanowi **Załącznik nr 1** do niniejszego opracowania.
3. Dla każdej osoby upoważnionej do przetwarzania danych osobowych IOD tworzy indywidualny zakres czynności, którego wzór stanowi **Załącznik nr 2** do niniejszego opracowania.
4. ASI rejestruje użytkownika w systemie i konfiguruje jego konto, nadając mu uprawnienia do pracy w systemie informatycznym na podstawie upoważnienia do przetwarzania danych osobowych wydanego przez ADO oraz nadaje do osobistego i wyłącznego użytku, unikalny identyfikator.
5. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, nie może być przydzielony innej osobie.
6. Zmiana uprawnień w zasobach informatycznych służących do przetwarzania danych osobowych, następuje na wniosek przełożonego. W procesie zmiany uprawnień mają zastosowanie postanowienia dotyczące nadawania uprawnień w zasobach informatycznych.
7. Odebranie uprawnień użytkownika następuje w przypadku zaistnienia okoliczności, warunkujących wyrejestrowanie użytkownika z systemu i blokadę jego konta.
8. Takimi okolicznościami są m.in.:
   1) zwolnienie z pracy;
   2) zmiana zakresu obowiązków powodująca, że pracownik nie będzie już przetwarzał

danych osobowych w systemie informatycznym,

9. Użytkownik systemu informatycznego ponosi odpowiedzialność za powierzony mu sprzęt komputerowy i wykonywane w nim czynności, aż do momentu rozliczenia się ze sprzętu komputerowego.

Nadawanie uprawnień do przetwarzania danych osobowych w zasobach informatycznych przebiega według następującej procedury:

1) Kierownik administracyjny składa wniosek o nadanie uprawnień w zasobie informatycznym, do ASI;

2) ASI, na podstawie otrzymanego wniosku, rejestruje użytkownika w systemie/aplikacji i nadaje mu wymagane uprawnienia oraz unikalne hasło;

3) Użytkownik, po otrzymaniu informacji o nadaniu uprawnień:

   a) loguje się do systemu/aplikacji w celu sprawdzenia poprawności konta i uprawnień,

   b) przy pierwszym logowaniu się do systemu/aplikacji, użytkownik zobowiązany do zapamiętania hasła i zniszczenia dokumentu zawierającego hasło.

3. Metody uwierzytelniania użytkowników systemu informatycznego przetwarzającego dane osobowe

Każdy użytkownik systemu musi posiadać indywidualny identyfikator oraz hasło dostępu do systemu.

Główną zasadą bezpieczeństwa systemu/aplikacji i sieci informatycznej jest ochrona informacji przed nieuprawnionym dostępem, ujawnieniem, przypadkowym lub nieautoryzowanym zniszczeniem lub modyfikacją danych. Stosowanie zasad uwierzytelniania użytkowników systemów/aplikacji (w tym sieci LAN/WAN) ma bezpośredni wpływ na zachowanie poufności, integralności oraz rozliczalności przetwarzanych danych.

TRYB POSTĘPOWANIA

Logowanie się do systemu

1. Zadaniem logowania jest uniemożliwienie niepowołanego dostępu do systemu informatycznego.
2. Każdy użytkownik systemu informatycznego posiada indywidualny identyfikator oraz hasło dostępu do systemu co jest niezbędne do jego uwierzytelnienia w systemie.
3. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który będzie przetwarzał dane osobowe w systemie informatycznym, odpowiada ASI.
4. Użytkownicy systemu są identyfikowani poprzez tzw. login (krótka nazwa użytkownika – ogólnie znana) i hasło (znane tylko użytkownikowi, IOD oraz ASI).
5. Użytkownik systemu, któremu nie udało się poprawnie zalogować, może po sprawdzeniu poprawności wpisywanych danych ponowić próbę zalogowania.

Hasła dostępu do systemu informatycznego przetwarzającego dane osobowe

1. Każdy użytkownik systemu posiada własne hasło dostępu.
2. Hasło powinno być unikatowe, a jego treść nie powinna umożliwiać identyfikacji użytkownika systemu i musi być zastrzeżona.
3. Użytkownik zobowiązany jest do zachowania w tajemnicy swojego hasła dostępu i nie udostępniania go innym współpracownikom. Zabrania się przechowywania go w postaci zapisanej, w szczególności niedozwolone jest przechowywanie hasła zapisanego np. na obudowie komputera, monitora lub na odwrocie klawiatury.

4. Przy wyborze hasła obowiązują następujące zasady:
    a) minimalna długość hasła – 8 znaków,
    b) zakazuje się stosować:
        a) haseł, które użytkownik stosował uprzednio w okresie minionego roku,
        b) swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.),
        c) ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego,
        d) nazwa ulicy na której mieszka lub pracuje, itp.
        e) wyrazów słownikowych,
        f) przewidywalnych sekwencji znaków z klawiatury np.: „QWERTY", „12345678",itp.
    c) należy stosować:
        a) hasła zawierające kombinacje liter i cyfr,
        b) hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, #, &, itp. o ile system informatyczny na to pozwala
        c) hasła, które można zapamiętać bez zapisywania,
        d) hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim,
5. Zabronione jest podejmowanie jakichkolwiek prób przywłaszczenia lub rozszyfrowania hasła innego użytkownika.
6. Hasła użytkownika, umożliwiające dostęp do systemu informatycznego, utrzymuje się w tajemnicy również po upływie ich ważności.

4. Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemu informatycznego przetwarzającego dane osobowe

Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik obowiązany jest do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych.

TRYB POSTĘPOWANIA

1. Każdy użytkownik musi przestrzegać warunków i zasad podłączenia sprzętu do sieci, gniazd elektrycznych i logicznych itp. określonych przez ASI.
2. Wszelkie zmiany w istniejących podłączeniach bez uprzedniego zezwolenia są niedozwolone.
3. Każdy użytkownik stacji roboczej jest odpowiedzialny za jej stan i bieżącą eksploatację.
4. Przed rozpoczęciem przetwarzania danych użytkownik zobowiązany jest sprawdzić, czy stan pomieszczenia i elementów systemu informatycznego nie wskazuje na możliwość naruszenia bezpieczeństwa danych osobowych, w szczególności:
   1) sprawdzić czy na drzwiach i zamkach nie ma widocznych śladów prób niepowołanego ich otwarcia,
   2) sprawdzić stan okien i innych zabezpieczeń oraz ocenić czy w pomieszczeniach nie ma znaków wskazujących na przebywanie w osób nieuprawnionych,
   3) sprawdzić stan sprzętu informatycznego.
5. Jeśli mogło mieć miejsce naruszenie ochrony danych osobowych, to użytkownik podejmuje działania zgodnie z „Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych".
6. Jeśli użytkownik nie wykrył naruszenia zabezpieczeń danych osobowych, to loguje się do systemu za pomocą własnego identyfikatora i hasła.
7. Obowiązkiem użytkownika jest śledzenie reakcji poszczególnych urządzeń i komunikatów pojawiających się na monitorze podczas uruchamiania komputera (stacji roboczej) i bieżącej eksploatacji.
8. W razie wystąpienia nieprawidłowości należy powiadomić IOD.
9. Przed zakończeniem pracy albo przerwą w przetwarzaniu danych użytkownik blokuje dostęp do systemu w sposób uniemożliwiający dostęp do danych bez podania prawidłowego identyfikatora i hasła.

10. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.
11. W przypadku przerwy w pracy użytkownika stacji roboczej przez okres dłuższy niż 10 minut automatycznie włączany jest wygaszacz ekranu.
12. Niedopuszczalne jest, aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jedno konto użytkownika.
13. W pomieszczeniach, w których przetwarzane są dane, przebywanie osób nieuprawnionych jest dopuszczalne za zgodą Administratora Danych Osobowych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
14. Po zakończeniu pracy użytkownik zobowiązany jest do przestrzegania poniższych zasad:
    1) wylogować się z systemu i poczekać na jego wyłączenie,
    2) sprawdzić czy nie zostały pozostawione bez nadzoru nośniki informacji,
    3) upewnić się że szafy i biurka z dokumentacją zostały zamknięte.

5. Tworzenie kopii zapasowych zbiorów danych osobowych oraz sposób, miejsce i okres przechowywania elektronicznych nośników informacji

ASI zobowiązany jest do wykonywania kopii awaryjnych zabezpieczających system informatyczny służący do przetwarzania danych osobowych i danych w nim przetwarzanych

TRYB POSTĘPOWANIA

1. Kopie awaryjne danych wykonuje ASI lub osoba przez niego upoważniona.
2. Wzór dziennika ewidencji kopii bezpieczeństwa stanowi **Załącznik nr 3** do niniejszego opracowania.
3. Kopie awaryjne usuwa się niezwłocznie po ustaniu ich użyteczności.
4. Wzór protokołu zniszczenia stanowi **Załącznik nr 4** do niniejszego opracowania.
5. Dane, w szczególności w postaci elektronicznej, przetwarzane w systemach CUW, zapisane na nośnikach informacji są własnością CUW.
6. Nośniki informacji, zawierające dane osobowe są przechowywane w pomieszczeniach stanowiących obszar przetwarzania danych, w meblach biurowych zamykanych na klucz. Nośniki nie mogą być wynoszone poza obszar przetwarzania bez zgody przełożonego.
7. Nośniki informacji, zawierające dane osobowe, można przekazywać tylko podmiotom lub osobom uprawnionym na podstawie przepisów prawa.
8. Dane osobowe na każdym elektronicznym nośniku informacji powinny być zabezpieczone przed odczytem, w szczególności spakowane do archiwum zabezpieczonego hasłem. Hasło powinno zostać przekazane odrębnym kanałem informacyjnym.
9. Dane osobowe przenoszone za pomocą nośników informacji, po poprawnym ich przeniesieniu na docelowy sprzęt komputerowy i do docelowej bazy danych lub zbioru danych, powinny być z nich trwale usunięte.
10. W przypadku, gdy dane powinny zostać usunięte, są one kasowane z wykorzystaniem dedykowanego oprogramowania i odpowiedniego, bezpiecznego algorytmu. Po usunięciu danych wymagane jest przeprowadzenie weryfikacji, czy dane zostały usunięte skutecznie.

11. W przypadku, gdy dane nie mogą być usunięte w sposób wskazany w pkt 10 (w szczególności nośniki optyczne) podlegają one skasowaniu poprzez fizyczne zniszczenie nośnika, na którym się znajdują.

12. Manualne kopie zapasowe zbioru danych oraz programów, oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w przeznaczonych do tego celu szafach biurowych zamykanych na klucz znajdujących się w wyznaczonym pomieszczeniu, które zapewnia właściwą ochronę przed nieuprawnionym dostępem, modyfikacją, uszkodzeniem lub zniszczeniem. Zaleca się, aby pomieszczenie to było zlokalizowane w strefie bezpieczeństwa zapewniającej ograniczony do nich dostęp.

6. Zabezpieczenie systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu

Do ochrony sieci wewnętrznej CUW wykorzystywane jest urządzenie Firewall z funkcjonalnością UTM oraz oprogramowanie antywirusowe

TRYB POSTĘPOWANIA

1. Do ochrony sieci wewnętrznej CUW wykorzystywane jest urządzenie Firewall z funkcjonalnością UTM (zintegrowane zarządzanie zagrożeniami) oferujące ochronę antyspamową, antywirusową, wykrywanie intruzów, zapobieganie wtargnięciu intruzów, filtrowanie treści internetowych oraz posiadające funkcje zapory ogniowych.

2. Na wszystkich stacjach roboczych zainstalowano oprogramowanie antywirusowe.

3. Dostęp do programu konfiguracyjnego BIOS zabezpieczony jest hasłem.

7. Procedury wykonywania przeglądów oraz konserwacji systemu i nośników informacji służących do przetwarzania danych

Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

TRYB POSTĘPOWANIA

1. Wszelkie prace związane z naprawami urządzeń wchodzących w skład systemu informatycznego i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
2. W przypadku uszkodzenia zestawu komputerowego nośnik informacji danych, na których są przechowywane dane osobowe zostaje zabezpieczony przez ASI przed dostępem osób nieuprawnionych.
3. Prace serwisowe na terenie CUW prowadzone w tym zakresie mogą być wykonywane wyłącznie przez pracowników lub przez upoważnionych przedstawicieli wykonawców (serwisantów) zewnętrznych znajdujących się w towarzystwie pracowników CUW.
4. Przedstawiciele wykonawców zewnętrznych muszą posiadać stosowne upoważnienie od ADO.
5. Przed rozpoczęciem prac serwisowych przez osoby spoza CUW konieczne jest potwierdzenie ich tożsamości.
6. W przypadku konieczności przeprowadzenia prac serwisowych poza siedzibą CUW dane z naprawianego urządzenia muszą zostać w sposób trwały usunięte. Od poniższego wymagania możliwe jest odstępstwo, jeżeli urządzenie, podczas przechowywania poza siedzibą CUW, będzie pod stałym nadzorem osoby upoważnionej do dostępu do danych na nim przetwarzanych.

8. Załączniki:

1. Wzór wniosku o nadanie uprawnień dla użytkownika w systemach informatycznych
2. Wzór indywidualnego zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych.
3. Wzór dziennika ewidencji kopii bezpieczeństwa.
4. Wzór protokołu zniszczenia.

Załącznik Nr 1 do Instrukcji

WZÓR WNIOSKU O NADANIE UPRAWNIEŃ DLA UŻYTKOWNIKA W SYSTEMACH INFORMATYCZNYCH

Imię i nazwisko użytkownika:	☐ Nowy użytkownik	☐ Modyfikacja uprawnień
Referat:	Adres budynku, piętro i nr pomieszczenia:	
Stanowisko:	Numery telefonów służbowych:	
Nr aktualnego upoważnienia do przetwarzania danych osobowych:	Okres ważności upoważnienia do przetwarzania danych osobowych:	

OPIS ZAKRESU UPRAWNIEŃ UŻYTKOWNIKA DO SYSTEMÓW INFORMATYCZNYCH

Lp.	Typ systemu, aplikacji, udziału sieciowego, usługi	Nazwa systemu, aplikacji, modułu, udziału sieciowego, usługi	Zakres uprawnień[1]	Identyfikator użytkownika w systemie
1				

Data i podpis przełożonego:	Data i podpis ASI:

[1] niepotrzebne skreślić

Załącznik Nr 2 do Instrukcji

WZÓR INDYWIDUALNEGO ZAKRESU CZYNNOŚCI OSOBY ZATRUDNIONEJ PRZY PRZETWARZANIU DANYCH OSOBOWYCH

Nazwa i adres pracodawcy: Centrum Usług Wspólnych w Nowej Sarzynie

Imię i nazwisko pracownika: .....

Stanowisko: .....

Przetwarzanie danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

Dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej; *(art. 4 pkt 1 Rozporządzenia 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.).*

1) Obowiązkiem każdego pracownika CUW jest zachowanie tajemnicy państwowej i służbowej, również w zakresie ochrony danych osobowych gromadzonych i przetwarzanych przez CUW. Obowiązek ten istnieje również po ustaniu zatrudnienia.
2) Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
3) Dokumentów materialnych (w formie elektronicznej, papierowej itp.) z danymi osobowymi nie można pozostawiać bez dozoru, ani udostępniać osobom nieupoważnionym.
4) Dokumentacji z danymi nie wolno wykorzystywać do innych celów niż służbowe.
5) Dokumentację z danymi nie wolno udostępniać nieuprawnionym.
6) Użytkownik systemu informatycznego musi dopilnować, aby monitor usytuowany był tak, by ekran był niewidoczny dla osób wchodzących do pomieszczenia.
7) Przy krótkotrwałych przerwach w pracy należy stosować blokady stacji roboczych.
8) Pracownik może uzyskać dostęp do systemu informatycznego tylko i wyłącznie jako użytkownik podając swój indywidualny login i hasło.
9) Oprogramowanie wgrywa tylko i wyłącznie Informatyk CUW, nie wolno tego robić samodzielnie.
10) Wydrukowane nadmiarowe, niepotrzebne lub błędne dokumenty należy niezwłocznie, trwale zniszczyć.

Oświadczam, że treść niniejszego zakresu jest mi znana

i zobowiązuję się do jego przestrzegania

Wykonano w 3 egzemplarzach

Potwierdzam odbiór 1 egzemplarza

Nowa Sarzyna, dnia .....

.....

(imię i nazwisko)

Załącznik Nr 3 do Instrukcji

WZÓR DZIENNIKA EWIDENCJI KOPII BEZPECZEŃSTWA

Lp.	Oznaczenie systemu / zbioru danych	Określenie metody (całościowa przyrostowa)	Oznaczenie nośnika, na którym utworzono kopię awaryjną	Kopię bezpieczeństwa utworzył:		
				Nazwisko i imię administratora	Data	Podpis
1	2	3	4	5	6	7

Załącznik Nr 4 do Instrukcji

.....
(miejscowość, data)

WZÓR PROTOKOŁU ZNISZCZENIA

Kopii bezpieczeństwa*/ innych nośników zawierających dane osobowe*

Nr: .....

Komisja w składzie:

1. .....
2. .....
3. .....

Oświadczam, iż kopie bezpieczeństwa* / inne nośniki* otrzymane z .....
(nazwa komórki organizacyjnej)

zostały w dniu ..... komisyjne zniszczone .....

....
(opis procesu zniszczenia)

Rodzaj i oznaczenie nośników:.....

Ilość sztuk: .....

Uwagi: .....

Podpisy komisji:

1. .....
2. .....
3. .....

* niepotrzebne skreślić