

**ZARZĄDZENIE NR 0050.53.2018**  
**Wójta w Urzędzie Gminy w Bojadłach**  
**z dnia 16 lipca 2018**

Na podstawie Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) zarządzam co następuje:

§1

W celu ochrony i zabezpieczenia danych osobowych przetwarzanych w Urzędzie Gminy Bojadłach wprowadzam:

1. Politykę ochrony danych osobowych będący załącznikiem nr 1 do niniejszego zarządzenia
2. Instrukcję zarządzania procedurami i systemami informatycznymi stanowiącą załącznik nr 2 do niniejszego zarządzenia
3. Regulamin ochrony danych osobowych stanowiący załącznik nr 3 do niniejszego zarządzenia

§2

Z chwilą wejścia zarządzenia traci moc zarządzenie 0050.33.2017 z dnia 24 maja 2017r.

§3

Zobowiązuje:

1. Inspektora danych osobowych do wdrożenia zasad wynikających z polityki ochrony danych osobowych i instrukcji zarządzania w Urzędzie Gminy w Bojadłach

§4

Zarządzenie obowiązuje od dnia 25 maja 2018 r.

  
**WÓJT**  
*mgr inż. Grzegorz Doszel*



**Załącznik nr 1 do zarządzenia nr 0050.53.2018**

**Wojta w Urzędzie Gminy w Bojadłach**

**z dnia 16 lipca 2018**

**Polityka ochrony danych osobowych w Urzędzie Gminy w Bojadłach**

WSTĘP .....	3
ANALIZA RYZYKA .....	3
DEFINICJE .....	3
REJESTR CZYNNOŚCI PRZETWARZANIA (INWENTARYZACJA DANYCH OSOBOWYCH) .....	3
WYZNACZENIE ZAGROŻEŃ .....	4
WYLICZENIE RYZYKA DLA ZAGROŻEŃ .....	4
PLAN POSTĘPOWANIA Z RYZYKIEM .....	5
UPOWAŻNIENIA .....	5
ŚRODKI TECHNICZNE I ORGANIZACYJNE ZABEZPIECZAJĄCE DANE OSOBOWE .....	6
REGULAMIN OCHRONY DANYCH OSOBOWYCH .....	6
INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI .....	6

## WSTĘP

---

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

## ANALIZA RYZYKA

---

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów (kategorii osób) lub dla procesów przetwarzania

## DEFINICJE

1. Aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych
1. Naruszenie (Incident) ochrony danych osobowych - to 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
2. Zagrożenie - potencjalne naruszenie (potencjalny incydent)
3. Skutki - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia)
4. Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie aktywów

## REJESTR CZYNNOŚCI PRZETWARZANIA (INWENTARYZACJA DANYCH OSOBOWYCH)

Administrator jest zobowiązany zgodnie z art. 30 RODO do prowadzenia rejestru czynności przetwarzania. Rejestr stanowi podstawę do przeprowadzenia analizy ryzyka.

1. Administrator prowadzi rejestr zgodnie z załącznikiem [01a Rejestr czynności przetwarzania \(wykaz zbiorów danych osobowych\)](#)
1. Podmiot przetwarzający prowadzi rejestr zgodnie z załącznikiem [06b Rejestr czynności prowadzony przez Podmiot przetwarzający](#)

## WYZNACZENIE ZAGROZEŃ

1. Administrator jest odpowiedzialny za określenie listy zagrożeń naruszenia poufności, dostępności i integralności, które mogą wystąpić podczas przetwarzania danych osobowych

1. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zinwentaryzowanych zbiorów (kategorii osób), aktywów oraz procesów przetwarzania

## WYLICZENIE RYZYKA DLA ZAGROŻEŃ

1. Administrator określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze (dla kategorii osób) lub w procesie przetwarzania  
Proponowaną skalę prawdopodobieństwa prezentuje Tabela A  
Administrator określa Skutki (**S**) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne  
Proponowaną Skalę skutków prezentuje Tabela B  
Administrator wylicza Ryzyka (**R**) dla wszystkich zagrożeń i ich skutków w/g formuły:  $R = P * S$

Tabela A PRAWDOPODOBIENSTWO WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
małe (do 10000 PLN, incydent prasowy lokalny)	1
średnie (10000-100000 PLN, incydent prasowy ogólnopolski)	2
duże (od 100000 PLN, naruszenie prawa)	3

Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem

1. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem
1. Proponowaną skalę Ryzyka prezentuje Tabela C

Tabela C POZIOM RYZYKA	WARTOŚĆ [R = P*S]
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

Reakcja na wartość ryzyka

1. Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń
1. Działania obniżające ryzyko, które może zastosować Administrator:
  - a. Przeniesienie –przerzucenie ryzyka (outsourcing, ubezpieczenie)
  - b. Unikanie – eliminacja działań powodujących ryzyko
2. Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka
3. Analizę ryzyka przeprowadza się w specjalnym szablonie załącznik [02e Arkusz analizy ryzyka RODO](#)

Ponowna analiza ryzyka

Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne)

## PLAN POSTĘPOWANIA Z RYZYKIEM

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne, patrz załącznik [02f Plan postępowania z ryzykiem](#)
1. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń

## UPOWAŻNIENIA

---

1. Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach (dla kategorii osób) w postaci papierowej oraz w systemach informatycznych
1. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa
2. Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Ewidencja ma charakter pomocniczy i nie jest wymagana przepisami RODO. Patrz [załącznik 01c Ewidencja osób upoważnionych](#)
3. W przypadku powierzenia przetwarzania danych do Podmiotu przetwarzającego, Administrator jest zobowiązany do sporządzenia z nim umowy powierzenia, stanowiącą podstawę upoważnienia dla osób z Podmiotu przetwarzającego - patrz załącznik [01f Umowa powierzenia](#)

## ŚRODKI TECHNICZNE I ORGANIZACYJNE ZABEZPIECZAJĄCE DANE OSOBOWE

---

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych, patrz [załącznik Instrukcja zarządzania RODO](#)
1. W instrukcji wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne i organizacyjne
2. Instrukcja jest aktualizowana, jeśli zajdzie taka potrzeba po przeprowadzeniu analizy ryzyka

## REGULAMIN OCHRONY DANYCH OSOBOWYCH

---

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania. Patrz załącznik - [04 Regulamin Ochrony Danych Osobowych](#)

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania poprzez podpisanie oświadczenia o poufności zawartego w arkuszu [01c Ewidencja osób upoważnionych](#)

Klauzula informacyjna jest określona dla petenów. Patrz [załącznik 1a do Polityki Ochrony Danych Osobowych](#)

## INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI

---

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego (lub jeśli jest powołany – Inspektora Ochrony Danych)
1. Do typowych podatności bezpieczeństwa danych osobowych należą:
  - a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
  - b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekami, kradzieżami i utratą danych osobowych



- c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)
2. Do typowych incydentów bezpieczeństwa danych osobowych należą:
  - a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
  - b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardej 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)
3. W przypadku stwierdzenia wystąpienia incydu, Administrator (lub w przypadku powołania – IOD) prowadzi postępowanie wyjaśniające w toku, którego:
  - a. ustala zakres i przyczyny incydu oraz jego ewentualne skutki
  - b. inicjuje ewentualne działania dyscyplinarne
  - c. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydu
  - d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia
4. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze - załącznik [03 Formularz rejestracji incydu](#)
5. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych
6. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.



**Załącznik nr 2 do zarządzenia nr 0050.53.2018**

**Wójta w Urzędzie Gminy w Bojadłach**

**z dnia 16 lipca 2018**

**Instrukcja zarządzania procedurami i systemami informatycznymi**

**w Urzędzie Gminy w Bojadłach**

1.	Wstęp .....	3
2.	Zabezpieczenia fizyczne .....	3
3.	Zabezpieczenia techniczne .....	3
4.	Procedura nadawania uprawnień do przetwarzania danych osobowych. ....	3
5.	Metody i środki uwierzytelnienia (polityka haseł) .....	4
6.	Procedura tworzenia kopii zapasowych .....	4
7.	Utylizacja elektronicznych nośników i wydruków oraz czyszczenie danych .....	4
8.	Procedura zabezpieczenia systemu informatycznego .....	4
8.1.	Bezpieczeństwo przetwarzania danych poza organizacją .....	4
8.2.	Ochrona przed nieautoryzowanym dostępem do sieci lokalnej.....	5
8.3.	Zabezpieczenia infrastruktury IT.....	5
8.4.	Zabezpieczenia aplikacji.....	5
9.	Procedura wykonywania przeglądów i konserwacji .....	5

## **1. WSTĘP**

Instrukcja stanowi wykaz procedur oraz stosowanych środków technicznych i organizacyjnych mających na celu, zgodnie z Art. 32 RODO, zabezpieczyć przetwarzane dane osobowe przed: przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych oraz nieuprawnionym dostępem do danych osobowych

## **2. ZABEZPIECZENIA FIZYCZNE**

1. drzwi do pomieszczeń biurowych, archiwów zamykane są na klucz
2. drzwi do serwerowni zamykane są na klucz
3. dokumentację papierową i nośniki elektroniczne przechowywaną w pomieszczeniach zabezpieczono w szafach zamykanych na klucz
4. stosowany jest system alarmowy/ kraty okienne
5. wdrożono system kontroli dostępu

## **3. ZABEZPIECZENIA TECHNICZNE**

1. zastosowano UPS do serwera, sieć stabilizowana
2. zastosowano monitoring wizyjny w obrębie obiektu i w otoczeniu
3. serwerownia wyposażona w gaśnice
4. powiadamianie administratora systemu informatycznego o alertach temperatury serwerowni
5. system gaszenia pożaru
6. klimatyzacja w serwerowni

## **4. PROCEDURA NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH**

Celem procedury jest minimalizacja ryzyka przetwarzania danych przez osoby nieupoważnione.

1. Dostęp do systemów informatycznych nadawany jest każdemu użytkownikowi w formie indywidualnego identyfikatora (loginu)
2. Nadawanie, zmiana, odbieranie uprawnień użytkownika do systemów informatycznych odbywa się na polecenie przełożonych (lub innych osób upoważnionych) w formie maila od przełożonego / z użyciem formularza nadawana uprawnień
3. Za wykonanie czynności nadawania, zmiany, odbierania uprawnień użytkownikowi odpowiada informatyk
4. Obowiązuje zasada minimalizacji uprawnień
5. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika. Zasada ta obowiązuje również administratorów systemów.

## **5. METODY I ŚRODKI UWIERZYTELNIANIA (POLITYKA HASEŁ)**

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

1. Standard hasła: (hasło min 8 – znakowe, zmieniane co 60 dni. Zmiana hasła jest wymuszana przez system
2. Zastosowano mechanizm blokady dostępu po 3 próbach nieudanego logowania się
3. Hasła administracyjne zdeponowane są w sejfie (lub w innym bezpiecznym miejscu)
4. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp

5. W przypadkach awaryjnych (np. nieobecność administratora) hasło może być przekazane decyzją informatyka osobie zastępującej administratora
6. Po ustaniu sytuacji awaryjnej, Administrator jest zobowiązany do zmiany hasła

## 6. PROCEDURA TWORZENIA KOPII ZAPASOWYCH

1. Kopie zapasowe serwera (z zawartością plików i baz danych) tworzone są w sposób zautomatyzowany w oparciu o (specjalne oprogramowanie / skrypt / wykorzystanie programowej funkcji serwera)
2. Kopie bezpieczeństwa sporządzane są także dla dokumentacji gromadzonej na dyskach stacji roboczych użytkowników w wybranym katalogu (np. w katalogu C:/Dokumenty)
3. Kopie przyrostowe tworzy się codziennie o g. 22.00
4. Kopie całościowe sporządzane są raz w miesiącu
5. Przechowywanych jest 12 kopii miesięcznych przez okres roku. Najstarsze kopie są nadpisywane w cyklu rotacyjnym
6. Kopie sporządzane są na wydzielonym serwerze NAS
7. Informatyk sprawuje nadzór nad poprawnością wykonania kopii zapasowych NAS
8. Niszczenie dysków z kopiami odbywa się komisyjnie. Nośniki niszczone są przez fizyczne zniszczenie, pocięcie po wymontowaniu z obudowy

## 7. UTYLIZACJA ELEKTRONICZNYCH NOŚNIKÓW I WYDRUKÓW ORAZ CZYSZCZENIE DANYCH

1. Podlegające likwidacji uszkodzone lub przestarzałe nośniki są niszczone w sposób fizyczny / zutylizowane w specjalistycznej firmie
2. Nośniki informacji muszą być wyczyszczone specjalistycznym oprogramowaniem zanim zostaną przekazane poza obszar organizacji
3. Dokumentacja papierowa niszczona jest w niszcarkach

## 8. PROCEDURA ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO

### 8.1. BEZPIECZEŃSTWO PRZETWARZANIA DANYCH POZA ORGANIZACJĄ

1. Stosuje się szyfrowanie (**bitlocker / veracrypt**) dysków komputerów przenośnych zawierających dane osobowe, jeśli wnoszone są poza obszar organizacji
2. Dane osobowe na komputerach przenośnych wnoszonych poza obszar organizacji muszą być przechowywane na zaszyfrowanych partycjach
3. Dyski przenośne / pendrive wnoszone poza organizację muszą być zaszyfrowane
4. W przypadku użycia komputerów przenośnych lub sprzętu mobilnego do zdalnego dostępu do zasobów wewnętrznej sieci przez Internet, stosuje się szyfrowanie tego połączenia z użyciem VPN (np. przez Informatyka / Księgową)

### 8.2. OCHRONA PRZED NIEAUTORYZOWANYM DOSTĘPEM DO SIECI LOKALNEJ

Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów

1. Dokonuje się konfiguracji urządzeń sieciowych oraz sprzętu IT w celu zabezpieczenia przed nieuprawnionym dostępem do nich
2. Dokonuje się aktualizacji oprogramowania systemów i aplikacji.
3. Stosowany jest monitoring usług sieciowych w celu deaktywacji nieużywanych
4. Zastosowano system antywirusowy i filtr antyspamowy
5. Stosowany jest Firewall
6. Zastosowano mechanizmy kontroli dostępu do sieci w postaci: (IDS/IPS do wykrywania i blokowania ataków do sieci komputerowej, technikę NAT

7. Separacja sieci wewnętrznej od sieci przeznaczonej dla gości (dla wifi i dla Ethernet) np. w salach konferencyjnych
8. Zabezpieczenie baz i katalogów webowych przed indeksacją wyszukiwarek

### **8.3. ZABEZPIECZENIA INFRASTRUKTURY IT**

1. Serwer wyposażono w macierz dyskową
2. Zastosowano wirtualizację serwera
3. Zastosowano redundantny serwer
4. Zabezpieczono hasłem dostęp do portów fizycznych
5. Dokonano dezaktywacji nieużywanych gniazd sieciowych
6. Stosuje się drukarki z funkcją kontroli wydruków (PIN)
7. Dopuszczono do użycia wyłącznie zakwalifikowane pendrive wraz z blokadą dopuszczenia pozostałych
8. Na stacjach roboczych zastosowano „zahasłowane wygaszacze ekranu”, aktywowane po 15 minutach nieaktywności użytkownika
9. Ustawienie monitorów uniemożliwiający wgląd w dane przez osoby postronne

### **8.4. ZABEZPIECZENIA APLIKACJI**

1. W kluczowych aplikacjach stosuje się terminację sesji
2. Stosuje się szyfrowanie poczty wychodzącej(SSL)
3. Dla aplikacji webowych stosowane jest szyfrowanie z użyciem protokołu SSL
4. Formularze kontaktowe na stronach www zabezpieczono protokołem SSL

## **9. PROCEDURA WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI**

1. Administrator / Informatyk odpowiada za optymalizację zasobów IT
2. Administrator / Informatyk odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach oraz za poprawność działania zasobów IT
3. W przypadku napraw dokonywanych na zewnątrz, z komputerów i urządzeń mobilnych należy usunąć nośniki danych lub usunąć te dane
4. W przypadku naprawy sprzętu z danymi osobowymi na nośniku wymaga się „usługi bezpiecznej naprawy”
5. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw on-site
6. Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych) muszą być wykonywane pod nadzorem osób upoważnionych





## **Załącznik nr 3 do zarządzenia nr 0050.53.2018**

**Wójta w Urzędzie Gminy w Bojadłach**

**z dnia 16 lipca 2018**

### **Regulamin Ochrony Danych Osobowych Urzędu Gminy w Bojadłach**

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO 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

**Załącznik 1a Wykaz pracowników zapoznanych z regulaminem**

**Załącznik 1b Oświadczenie pracownika**

## SPIS TREŚCI

1. Zasady bezpiecznego użytkowania sprzętu IT, dysków, programów .....	3
2. Zarządzanie uprawnieniami - procedura rozpoczęcia, zawieszenia i zakończenia pracy.....	3
3. Polityka haseł .....	3
4. Zabezpieczenie dokumentacji papierowej z danymi osobowymi .....	3
5. Zasady wnoszenia nośników z danymi poza firmę/organizację.....	4
6. Zasady korzystania z internetu.....	4
7. Zasady korzystania z poczty elektronicznej.....	4
8. Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych .....	4
9. Obowiązek zachowania poufności i ochrony danych osobowych.....	5
10. Postępowanie dyscyplinarne.....	5

## ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, PROGRAMÓW

---

1. Użytkownik odpowiada za zabezpieczenie przed zniszczeniem, uszkodzeniem oraz utratą sprzętu IT (komputerów, urządzeń biurowych, tabletów i smartfonów)
2. Demontaż, instalowanie lub podłączanie dodatkowych urządzeń jest zabronione
3. Użytkownik jest zobowiązany do usuwania tymczasowych plików z nośników/dysków z miejsc, gdzie dostęp do nich miałyby osoby nieupoważnione
4. Użytkownik jest zobowiązany do przekazania informatykowi nośników przeznaczonych do zniszczenia

## ZARZĄDZANIE UPRAWNIENIAMI - PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

---

1. Każdy użytkownik komputerów, programów i systemu operacyjnego zobowiązany jest do pracy na własnym koncie. Zabronione jest udostępnianie konta innemu użytkownikowi
2. Użytkownik nie może zmieniać swoich uprawnień, np. zostać Administratorem na swoim komputerze
3. Użytkownik komputera oraz programów rozpoczyna i kończy pracę logowaniem i wylogowaniem się
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach – tzw. **Polityka czystego ekranu**
5. Użytkownik przed tymczasowym odejściem od komputera musi włączyć wygaszacz ekranu (**WINDOWS + L**) lub wylogować się z systemu bądź z programu.
6. Zabrania się uruchamiania jakiegokolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana jako pracownik działu informatyki. Dotyczy to zwłaszcza programów przestanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
7. Po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego oraz zabezpieczyć nośniki elektroniczne, magnetyczne i optyczne na których znajdują się dane osobowe

## POLITYKA HASEŁ

---

1. Hasła powinny składać się z min. 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.
4. Hasła nie powinny być ujawniane innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie

5. W przypadku ujawnienia hasła – należy natychmiast go zmienić
6. Hasła muszą być zmieniane co 60 / 90 dni
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła

## ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANymi OSOBOWymi

---

1. Pracownicy są zobowiązani do stosowania tzw. „**Polityki czystego biurka**”. Polega ona na zabezpieczeniu (zamykaniu na klucz) dokumentów oraz nośników np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób postronnych
2. Pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach
3. Zabrania się pozostawiania dokumentów w miejscach dostępnych dla osób postronnych
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik

## ZASADY WYNOszENIA NOŚNIKÓw Z DANymi POZA FIRME/ORGANIZACJĘ

---

1. Użytkownicy nie mogą wnosić na zewnątrz niezasyfrowanych nośników z danymi osobowymi (np. przenośnych dysków twardych, pen-drive, płyt CD, DVD, pamięci typu Flash)
2. Dane osobowe wynoszone poza organizację muszą być zasyfrowane (szyfrowane dyski przenośne, zahasłowane pliki, zabezpieczone smartfony)
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach w celu zabezpieczenia ich przed zagubieniem i kradzieżą

## ZASADY KORZYSTANIA Z INTERNETU

---

1. Zabrania się instalowania programów z Internetu bez konsultacji z 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

## 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. 8**) 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, .xism, .pdf, .exe) w mailach!!!! Są to zwykle „wirusy”, które infekują komputer oraz często pozostałe komputery w sieci. **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 komputer oraz inne komputery w sieci. **WYSOKIE RYZYKO UTRATY BEZPOWROTNEJ UTRATY DANYCH**
6. Należy zgłaszać informatykowi przypadki podejrzanых emaili
7. Użytkownicy nie powinni rozsyłać „niezawodowych” emaili 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

11. Użytkownik bez zgody Pracodawcy / Zleceniodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy / Zleceniodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej

## SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

---

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Pracodawcy / Zleceniodawcy 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 wyciekami, kradzieżami i utratą danych osobowych
  - c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony hasła, 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, twarde 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 niszczone 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. wnoszenie 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, twarde 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

## OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

---

1. Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana do:
  - a. przetwarzania danych osobowych wyłącznie w celu i zakresie powierzonych jej zadań
  - b. zachowania w tajemnicy danych osobowych do których ma
  - c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych jej zadań
  - d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych

2. 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
3. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych
4. Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana zabezpieczenia danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem

## 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 ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.

