# INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Administrator danych:

Urząd Gminy w Domaniowie

adres:

55-261 Domaniów 56

## Spis treści

## Wprowadzenie

Instrukcja stanowi wykaz procedur oraz stosowanych środków technicznych i organizacyjnych mających na celu, zgodnie z art. 32 RODO, zabezpieczyć przetwarzane dane osobowe. Administrator danych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator danych zobowiązany jest zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. W tym celu prowadzona jest dokumentacja opisująca sposób przetwarzania danych oraz środki zapewniające należytą ochronę.

**Administrator danych** – Urząd Gminy Domaniów z siedzibą w Domaniowie, 55-261 Domaniów 56, REGON 931934851, NIP 912-17-16-512, reprezentowany przez Wojciecha Głogulskiego – Wójta Gminy.

**Administrator systemów informatycznych** – administrator danych sam wykonuje czynności administratora systemów informatycznych.

**Inspektor ochrony danych (IOD)** – Krzysztof Petrykiewicz, kontakt: iod.lege.olawa@gmail.com faks: (71) 303 32 72

## Rozdział I – Definicje

1. **identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
2. **Integralność danych** – właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
3. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
4. **Osoba upoważniona** – użytkownik systemu informatycznego uprawnionego do przetwarzania danych osobowych.
5. **Odbiorca danych** – osoba fizyczna lub prawna, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.
6. **Obszar przetwarzania danych** – wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

7. **Opis przepływu danych** – opis sposobu przepływu danych pomiędzy poszczególnymi systemami informatycznymi.
8. **Opis struktury zbiorów** – opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.
9. **Państwo trzecie** – to państwo nienależące do Europejskiego Obszaru Gospodarczego.
10. **Poufność danych** – to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.
11. **Przetwarzanie danych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
12. **Rozliczalność** – to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
13. **Raport** – to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.
14. **Sieć publiczna** – to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.).
15. **Sieć telekomunikacyjna** – to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.).
16. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
17. **Środki techniczne i organizacyjne** – środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.
18. **Teletransmisja** – to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.
19. **Ustawa** – rozumie się przez to ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000).
20. **Usuwanie danych** – to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
21. **Użytkownik systemu** – to osoba, której został przydzielony przez administratora systemów informatycznych indywidualny identyfikator w systemie informatycznym w powiązaniu z niezbędnymi uprawnieniami dostępowymi w tym systemie.
22. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości.
23. **Wykaz zbiorów** – wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.
24. **Zabezpieczenie danych w systemie informatycznym** – to wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

25. **Zbiór danych** – to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
26. **Zgoda osoby, której dane dotyczą** – to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie.

## Rozdział II – Zabezpieczenia systemów informatycznych

1. Użytkownicy systemu informatycznego niezwłocznie informują administratora systemu o zagrożeniach wskazywanych przez oprogramowanie antywirusowe.
2. Każdy zbiór wczytywany do komputera, w tym także wiadomości email, musi być przetestowany programem antywirusowym. Niedopuszczalne jest stosowanie dostępu do sieci internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.
3. Użytkownicy urządzeń/komputerów przenośnych wynoszonych poza obszar organizacji, na których są przetwarzane dane osobowe są zobowiązani do przestrzegania zasad bezpieczeństwa i podpisania regulaminu użytkowania urządzeń/komputerów przenośnych.
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.
5. W przypadku użycia komputerów przenośnych lub sprzętu mobilnego do zdalnego dostępu do zasobów wewnętrznej sieci przez Internet dokonuje się uwierzytelnienia: z użyciem loginu i hasła, dwuetapowe (np. weryfikacja SMS, token) / poprzez autoryzację adresu IP.
6. Zapewniono rozliczalność operacji dla pracy w kluczowych aplikacjach, bazach i serwerach plików.
7. W ramach rozliczalności logowane są operacje tworzenia, modyfikacji, usuwania, wglądu, eksportu do plików.
8. Kluczowe aplikacje i bazy zawierające dane osobowe zabezpieczono przed eksportem danych do plików.
9. Zabezpieczono interfejsy programistyczne poprzez zmianę domyślnych loginów i haseł / wyłączenie dostępu zdalnego, gdy nie jest wymagany.
10. Zabezpieczenie testowych wersji aplikacji poprzez zmianę domyślnych loginów i haseł / wyłączenie dostępu zdalnego, gdy nie jest wymagany.
11. Zastosowano szyfrowanie / tokenizację baz danych.
12. Zastosowano szyfrowanie danych przechowywanych w chmurze.
13. Stosuje się szyfrowanie poczty wychodzącej (SSL/TLS).
14. Na stronach www stosowane jest szyfrowanie połączeń internetowych z użyciem protokołu SSL.
15. Formularze kontaktowe na stronach www zabezpieczono protokołem SSL.
16. Formularze logowania na stronach www zabezpieczono protokołem SSL.
17. Dokonuje się aktualizacji oprogramowania (firmware / sterowniki) urządzeń sieciowych oraz innych (np. w urządzeniach jak: routery, switche, access pointy, firewalle, macierze, dyski NAS, drukarki, skanery).

18. Dokonywana jest konfiguracja urządzeń sieciowych (routery, switche, access pointy, firewalle, macierze, dyski NAS, drukarki, skanery i inne) w celu zabezpieczenia przed nieuprawnionym dostępem do nich (np. zmiana domyślnych haseł na urządzeniach, zmiana domyślnych nazw kont administratora w urządzeniach, konfiguracja portów na routerze).
19. Dokonuje się aktualizacji oprogramowania systemów i aplikacji (systemy operacyjne na stacjach roboczych / systemy operacyjne serwerów / przeglądarki www / CMS (Wordpress, Drupal, Joomla, Prestashop,) / Dedykowany CMS / Adobe / Flash / Java / inne). Aktualizacja dokonywana jest zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service packi, łatki).
20. Monitorowane są usług sieciowe na serwerach i stacjach roboczych (np. DHCP, DNS, SSH, http, telnet, FTP, SMTP, SNMP) oraz utrzymuje się niezbędne usługi oraz dezaktywuje pozostałe.
21. Zastosowano system antywirusowy na serwerze.
22. Zastosowano filtr antyspamowy.
23. Stosowany jest Firewall/NGFirewall (sprzętowy zintegrowany z routerem / programowy na serwerze, na stacjach roboczych, na wirtualnym serwerze)
24. Zastosowano mechanizmy kontroli dostępu do sieci w postaci: (IDS/IPS do wykrywania i blokowania ataków do sieci komputerowej, technikę NAT.
25. Zastosowano sewery proxy i bramki filtrujące (blokada ruchu na podstawie bazy reputacji, blokada dostępu do określonych stron)
26. Zastosowano mechanizmy monitorujące przeglądanie Internetu przez użytkowników (blokowanie stron internetowych określonego typu, blokowanie określonych stron internetowych, analizę przesyłanych informacji pod kątem niebezpiecznego oprogramowania)* - niepotrzebne skreślić
27. Sieć bezprzewodową zabezpieczono (protokołem WEP, uwierzytelnianiem EAP, uwierzytelnianiem EAP – TLS, uwierzytelnianiem EAP-MS-CHAP v.2, uwierzytelnianiem PEAP, technologią WPA)
28. Separacja sieci wewnętrznej od sieci przeznaczonej dla gości (dla WiFi i dla Ethernet).
29. Zastosowano specjalistyczne oprogramowanie monitorujące wymianę danych na styku sieci lokalnej i sieci internet.
30. Zabezpieczenie baz i katalogów dostępnych z poziomu sieci przed indeksacją wyszukiwarek.
31. Pozostałe środki zabezpieczeń zostały określone w rejestrze obszarów przetwarzania danych osobowych.

## Rozdział III – Procedura tworzenia kopii zapasowych

1. Kopie zapasowe powinny być kontrolowane przez administratora systemów informatycznych, w szczególności pod kątem prawidłowości ich wykonania poprzez częściowe lub całkowite odtworzenie.
2. W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.
3. Rejestr kopii zapasowych powinien zawierać:

a) rodzaj kopii (kopia całego serwera, kopia bazy, kopia danych, obraz serwera wirtualnego),
b) typ kopii (całościowa, przyrostowa),
c) rodzaj nośnika (CD, DVD, przenośny dysk HDD, pendrive, serwer NAS, cloud, streamer, mirror),
d) częstotliwości wykonywania kopii,
e) czas przechowywania,
f) miejsca przechowywania, sposobu transportu i przekazywania kopii zabezpieczonych przed kradzieżą, utratą, modyfikacją, uszkodzeniem, zniszczeniem,
g) rejestr osób uprawnionych do dostępu do kopii,

4. Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.
5. W systemach informatycznych zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych przetwarzanych przy użyciu systemów informatycznych.
6. Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.
7. Kopie zapasowe serwera (z zawartością plików i baz danych) tworzone są w sposób zautomatyzowany w oparciu o (specjalne oprogramowanie / skrypt / wykorzystanie programowej funkcji serwera).
8. Kopie bezpieczeństwa sporządzane są także dla dokumentacji gromadzonej na dyskach stacji roboczych użytkowników w wybranym katalogu (np. w katalogu C:/Dokumenty)
9. Kopie przyrostowe tworzy się codziennie o godzinie: 15.30.
10. Kopie całościowe sporządzane są min. raz w miesiącu.
11. Przechowywanych jest do 12 kopii miesięcznych przez okres roku. Najstarsze kopie są nadpisywane w cyklu rotacyjnym.
12. Kopie sporządzane są na: przenośnym dysku HDD / pendrive / wydzielonym serwerze NAS / w chmurze (cloud).
13. Co miesiąc sporządzana jest kopia przenośnego dysku HDD / pendrive / wydzielonego serwera NAS / chmury (cloud) na przenośnym dysku HDD / pendrive / wydzielonym serwerze NAS / w chmurze (cloud)
14. Przenośny dysk HDD / Pendrive / Wydzielony serwer NAS przechowywany jest w zamykanym pomieszczeniu.
15. Dostęp do przenośnego dysku HDD / pendrive / wydzielonego serwera NAS / chmury (cloud) mają wyłącznie osoby upoważnione.
16. Administrator systemów informatycznych sprawuje nadzór nad poprawnością wykonania kopii zapasowych.

## Rozdział IV – Przechowywanie elektronicznych nośników

1. Nie należy przechowywać zbędnych nośników informacji zawierających dane oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane. Po upływie okresu ich

użyteczności lub przechowywania, dane powinny zostać skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie.

2. Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe nie mogą być przemieszczane poza pomieszczenia stanowiące obszar przetwarzania danych.
3. W przypadku korzystania z elektronicznych nośników zawierających dane, w szczególności takich jak płyty CD / DVD / Blu-ray, pendrive, karty SD, zewnętrzne dyski, taśmy magnetyczne, są one przechowywane w sposób uniemożliwiający do nich dostęp osobom nieupoważnionym.
4. W celu usunięcia danych z elektronicznego nośnika danych użytkownicy stosują metodę trzykrotnego nadpisania pełnej zawartości nośnika danymi niezawierającymi danych osobowych.

## Rozdział V – Procedura utylizacji nośników

1. Podlegające likwidacji uszkodzone lub przestarzałe nośniki a szczególności macierze dyskowe / twarde dyski z danymi osobowymi ze stacji roboczych i laptopów / pendrive / pamięci flash / dyski SSD / płyty DVD / telefony komórkowe / smartfony są niszczone komisyjnie w sposób fizyczny. Stosowana metoda niszczenia, to fizyczne niszczenie (pocięcie, nawiercenie, młotkowanie) wymontowanych nośników / użycie degaussera / zmielenie w specjalistycznej firmie potwierdzone protokołem zniszczenia lub certyfikatem bezpieczeństwa firmy utylizacyjnej lub nagraniem z procesu transportu i utylizacji.
2. Nośniki informacji zamontowane w sprzęcie IT a w szczególności twarde dyski muszą być wyczyszczone specjalistycznym oprogramowaniem zanim zostaną przekazane poza obszar firmy (np. sprzedaż lub darowizna komputerów stacjonarnych / laptopów / smartfonów).
3. Dokumentacja papierowa niszczona jest w niszczarkach paskowych oraz tam, gdzie to wymagane w niszczarkach o podwyższonym standardzie.
4. Dokumentacja papierowa niszczona jest za pośrednictwem firmy niszczącej dokumenty. Firma zobowiązana jest do wykazania się bezpieczną procedurą utylizacji (np. posiadać certyfikat ISO27001, nagrania z procesu transportu i utylizacji.

## Rozdział VI – Procedura przeglądów i konserwacji

1. Administrator systemów informatycznych prowadzi okresowe przeglądy systemów informatycznych w celu określania ich poziomu sprawności, biorąc pod uwagę racjonalne wykorzystanie sprzętu oraz bezpieczeństwo danych przetwarzanych z jego wykorzystaniem.
2. Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych, przeprowadzane są w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, przez: administratora systemów informatycznych / firmy zewnętrzne na podstawie zawartych umów. W umowach powinno znajdować się postanowienie o powierzeniu danych osobowych. W przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności administratora systemów informatycznych.

3. W przypadku konieczności dokonania naprawy elementu infrastruktury systemu informatycznego przez osobę nieupoważnioną (np. zewnętrzny serwis informatyczny) w obszarze przetwarzania danych, wszelkie czynności dokonywane są pod bezpośrednim nadzorem osób upoważnionych lub administratora systemów informatycznych.
4. Administrator systemów informatycznych przeprowadza ww. przegląd nie rzadziej niż raz na 12 miesięcy.
5. Nadzór nad przeprowadzaniem przeglądów technicznych, konserwacji i napraw sprzętu komputerowego, na którym zainstalowano system informatyczny służący do przetwarzania danych osobowych, systemu informatycznego służącego do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych pełni administrator danych.

## Rozdział VII – Procedura polityki haseł

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

1. Pierwsze (pierwotne) hasło użytkownika nadawane jest przez administratora systemów informatycznych i przekazywane użytkownikowi w poufny sposób.
2. Hasła administracyjne zdeponowane są w: sejfie (lub w innym bezpiecznym miejscu), do których dostęp posiada: administrator danych / administrator systemów informatycznych.
3. W przypadku utraty uprawnień przez osobę administrującą systemami informatycznymi należy niezwłocznie zmienić hasła, do których miała dostęp (administratorów, użytkowników, urządzeń, dostępu do pomieszczeń, itp.)
4. W sytuacjach awaryjnych (np. nieobecność administratora systemów informatycznych) hasło może być przekazane decyzją administratora danych osobie zastępującej administratora systemów informatycznych.
5. Po ustaniu sytuacji awaryjnej, administrator systemów informatycznych jest zobowiązany do zmiany haseł administracyjnych oraz tych do których osoba zastępująca mogła uzyskać dostęp podczas zastępstwa.
6. Hasło zastosowane do uwierzytelnienia użytkownika w systemie informatycznym składa się z określonej liczby znaków (co najmniej 8), w tym musi zawierać małe i duże litery oraz liczbę i znak specjalny. Hasło jest zmieniane w cyklach nie dłuższych niż 30 dni.
7. Hasło nie może składać się z danych personalnych (tj. imion, nazwisk, adresów zamieszkania użytkownika, jak również najbliższych dla niego osób) lub ich fragmentów.
8. Hasło nie może składać się z identycznych znaków lub ciągu znaków z klawiatury.
9. Hasło nie może być tożsame z identyfikatorem użytkownika.
10. Hasło musi być za każdym razem nowe, tzn. takie, które nie było poprzednio stosowane przez użytkownika.
11. Zmiana hasła dokonywana jest przez użytkownika manualnie.
12. Hasło zastosowane do uwierzytelnienia administratora systemu w systemie informatycznym składa się z określonej liczby znaków, w tym musi zawierać małe i duże litery oraz liczbę i znak specjalny.

13. Hasło, w trakcie wpisywania, nie może być wyświetlane na ekranie. Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności.
14. W przypadku złamania zasady poufności hasła, użytkownik zobowiązany jest niezwłocznie zmienić hasło i poinformować o tym fakcie administratora systemów informatycznych.
15. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego służącego do przetwarzania danych nie powinien być przydzielany innej osobie.
16. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, należy niezwłocznie zablokować w systemie informatycznym służącym do przetwarzania danych oraz unieważnić przypisane mu hasło.
17. Użytkownicy systemów informatycznych są zapoznawani z zagrożeniami wynikającymi ze stosowania haseł jako formy ich uwierzytelniania w systemie informatycznym.
18. Przed rozpoczęciem przetwarzania danych osobowych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić administratora danych.
19. Przed rozpoczęciem pracy w systemie informatycznym użytkownik weryfikuje bezpieczeństwo treści wyświetlanych na ekranie ze względu na przebywanie osób nieupoważnionych w obszarze przetwarzania.
20. Niedozwolone jest wykonywanie jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.
21. Przed przerwaniem pracy w systemie informatycznym i tymczasowym odejściem od punktu dostępowego systemu informatycznego użytkownik blokuje swój dostęp poprzez manualne uruchomienie wygaszacza ekranu chronionego hasłem.
22. Po zakończeniu pracy w systemie informatycznym użytkownik zamyka system informatyczny, do którego ma dostęp.

## Rozdział VIII – Procedura uprawnień do systemów informatycznych

Celem procedury jest minimalizacja ryzyka przetwarzania danych w systemach informatycznych przez osoby nieupoważnione.

1. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych, zastosowano wysoki poziom bezpieczeństwa.
2. Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.
3. Osobą odpowiedzialną za nadawanie uprawnień w systemach informatycznych jest administrator systemu informatycznego.
4. Procedura nadawania, modyfikowania i odbierania uprawnień użytkownikowi w systemach informatycznych obejmuje w kolejności:
   a) nadanie przez administratora danych upoważnienia do przetwarzania danych oraz odebranie oświadczenia o zachowaniu poufności i przestrzeganiu wewnętrznej dokumentacji ochrony danych, w tym regulaminu ochrony danych,

b) przy nadawaniu przez administratora danych upoważnienia do systemów informatycznych użytkownikowi, obowiązuje zasada minimalizacji uprawnień w niezbędnym do wykonywania czynności zakresie,
c) zwrócenie się administratora danych lub innej upoważnionej przez niego osoby z wnioskiem do administratora systemów informatycznych o nadanie uprawnień w systemach,
d) przed nadaniem uprawnień użytkownikowi upoważnionemu do przetwarzania danych administrator systemów informatycznych zapoznaje użytkownika z przepisami dotyczącymi ochrony danych w systemach informatycznych oraz procedurami bezpieczeństwa tych systemów,
e) nadanie, zmodyfikowanie lub odbieranie uprawnień użytkownika w systemach informatycznych w niezbędnym zakresie, odbywa się po zweryfikowaniu przez administratora systemów informatycznych treści upoważnienia do przetwarzania danych osobowych lub innej podstawy prawnej pozwalającej na wykonanie czynności zgodnie z:
   - upoważnieniem do przetwarzania danych wydanym przez administratora danych
   - załącznikiem do zlecenia nadania / modyfikacji / odebrania uprawnień

5. Procedura nadania uprawnień użytkownikowi w systemach informatycznych np. w stacji roboczej, terminalu, komputerze stacjonarnym, komputerze przenośnym, tablecie, telefonie komórkowym, dysku sieciowym, programie lub aplikacji, poczcie elektronicznej, nadawany jest konkretnej osobie jako unikalnemu użytkownikowi i obejmuje w kolejności:
   a) przypisanie indywidualnego identyfikatora użytkownika w systemach informatycznych przy zapewnieniu, że identyfikator ten nie był wcześniej przydzielony innemu użytkownikowi,
   b) przypisanie zakresu przydzielonych uprawnień w systemach informatycznych do konkretnego identyfikatora użytkownika,
6. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
7. Użytkowników obowiązuje zasada pracy na własnym unikalnym koncie użytkownika. Zabronione jest umożliwianie, udostępnianie, przekazywanie innym osobom pracy na koncie innego użytkownika. Zasada ta obowiązuje wszystkie osoby bez wyjątków w tym administratorów.
8. Każdemu użytkownikowi uprzywilejowanemu (administratorowi) nadawane jest indywidualne konto administracyjne.
9. W przypadku pracy z uprawnieniami użytkownika uprzywilejowanego, każdy administrator systemu informatycznego zobowiązany jest do bieżącej pracy na koncie roboczym. Użycie tzw. konta administracyjnego (np. root, admin, administrator, itp.) dopuszczalne jest jedynie w sytuacjach awaryjnych lub podczas poważnych zmian wprowadzanych w administrowanym systemie.

## Rozdział IX – Postanowienia końcowe

1. W przypadku stwierdzenia uchybień dotyczących przetwarzania danych każda osoba powinna o tym fakcie niezwłocznie powiadomić administratora danych. Następnie administrator danych wprowadza takie zabezpieczenia i procedury, które w przyszłości wyeliminują takie zdarzenia.

2. Administrator danych ma prawo do kontroli stanu zabezpieczeń oraz przestrzegania zasad ochrony danych osobowych w dowolnym terminie.
3. Należy zainstalować zalecane przez producentów oprogramowania aktualizacje systemu informatycznego służącego do przetwarzania danych osobowych celem wyeliminowania błędów w działaniu lub poprawienia wydajności działania.
4. Wszelkie zasady opisane w niniejszej Instrukcji są przestrzegane przez użytkowników i administratorów systemów ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą.
5. Instrukcja obowiązuje od dnia jej zatwierdzenia przez administratora danych.

**Wykaz załączników:**

1. Regulamin użytkowania komputerów przenośnych.

| _____ | _____ | _____ |
|---|---|---|
| Pieczęć firmowa | Podpis administratora danych | Data |