OR.120.19.2016

ZARZĄDZENIE Nr ...19...../2016
STAROSTY TURECKIEGO
z dnia ...23. lutego..... 2016 r.

w sprawie Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz Polityki bezpieczeństwa danych osobowych w Starostwie Powiatowym w Turku

Na podstawie art. 34 ust 1 i art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2015 r. poz. 1445 i 1890), art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135 i 2281) oraz § 3, § 4 i § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) zarządza się, co następuje:

§ 1. 1. Wprowadza się Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Turku, stanowiącą załącznik Nr 1 do niniejszego zarządzenia.

2. Wprowadza się Politykę bezpieczeństwa danych osobowych w Starostwie Powiatowym w Turku, stanowiącą załącznik Nr 2 do niniejszego zarządzenia.

§ 2. Zobowiązuje się pracowników Starostwa Powiatowego w Turku do zapoznania się z Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz Polityką bezpieczeństwa danych osobowych, o których mowa w § 1.

§ 3. Wykonanie zarządzenia powierza się Sekretarzowi Powiatu, Dyrektorom Wydziałów Starostwa Powiatowego w Turku oraz Administratorowi Bezpieczeństwa Informacji w Starostwie Powiatowym w Turku.

§ 4. 1. Traci moc zarządzenie Nr 55/2011 Starosty Tureckiego z dnia 3 października 2011 r. w sprawie wprowadzenia w Starostwie Powiatowym w Truku Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Starostwa Powiatowego w Truku oraz Polityki bezpieczeństwa danych osobowych Starostwa Powiatowego w Turku.

2. Dotychczasowe upoważnienia do przetwarzania danych osobowych wydane na podstawie dokumentów wskazanych w ust. 1 wygasają z chwilą podjęcia niniejszego zarządzenia.

STAROSTA
Mariusz Leńko

SEKRETARZ
Roman Kacprzak

Przemysław Jandy
Radca prawny
Pzkn-2777

ZATWIERDZAM

STAROSTA

Mariusz Seńko

.....

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W STAROSTWIE POWIATOWYM W TURKU

Opracował
Robert Wojdyła
Administrator Bezpieczeństwa Informacji
w Starostwie Powiatowym w Turku

Rozdział I

Postanowienia ogólne.

§ 1.
POSTANOWIENIA OGÓLNE

Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Turku, zwana dalej „Instrukcją", określa:

1. Zasady, tryb postępowania i zalecenia Administratora Danych Osobowych , które należy stosować w trakcie przetwarzania danych osobowych w systemach informatycznych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.
2. Sposób rejestrowania i wyrejestrowywania użytkowników oraz osoby odpowiedzialne za te czynności,
3. Sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności,
4. Procedury i zasady rozpoczynania i kończenia pracy,
5. Metody i częstotliwość kontroli pod kątem obecności wirusów komputerowych oraz sposobów ich usuwania,
6. Zasady i częstotliwość tworzenia kopii bezpieczeństwa,
7. Zasady i czas przechowywania nośników informacji, w tym kopii informatycznych,
8. Zasady dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych,
9. Zasady postępowania w zakresie komunikacji w sieci komputerowej,
10. Instrukcja została opracowana zgodnie z wymogami § 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych w systemach informatycznych.

§ 2.
DEFINICJE

Ilekroć w instrukcji jest mowa o:

1. **Ustawa** - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. , poz. 1182), zwaną dalej „ustawą";
2. **Staroście** - rozumie się przez to Starostę Tureckiego,

3. **Zbiorze danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
4. **Przetwarzaniu 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,
5. **Kartotece** - rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierającej dane osobowe,
6. **Komórce organizacyjnej** - rozumie się przez to każdą wydzieloną organizacyjnie i funkcjonalnie komórkę wewnętrzną, zgodnie z regulaminem organizacyjnym,
7. **Systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji programowych zastosowanych w celu przetwarzania danych,
8. **Identyfikator użytkownika** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
9. **Hasło** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
10. **Sieć telekomunikacyjna** - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.)
11. **Sieć publiczna** - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne;
12. **Teletransmisja** - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
13. **Rozliczalność** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
14. **Integralność danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
15. **Raport** - rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
16. **Poufność danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
17. **Uwierzytelnianie** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
18. **Administrator Danych (AD)** - w świetle przepisów ustawy o ochronie danych osobowych , art. 3 i 7 pkt 4, rozumie się przez to Starostę Tureckiego, który decyduje o celach i środkach przetwarzania danych osobowych,
19. **Administrator Bezpieczeństwa Informacji (ABI)** - rozumie się przez to osobę wyznaczoną przez Administratora Danych, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
20. **Administrator Systemu Informatycznego (ASI)** - rozumie się przez to osobę zatrudnioną przez Starostę Tureckiego, upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;

21. **Użytkownik systemu informatycznego** - rozumie się przez to upoważnioną przez kierownika Starostę Tureckiego, pracownika do przetwarzania danych osobowych w systemie informatycznym, który odbył stosowne szkolenie w zakresie ochrony danych,
22. **Pracowniku ochrony** - rozumie się przez to osobę wykonującą zadania z zakresu ochrony osób i mienia na rzecz Administratora Danych,
23. **Pomieszczeniach** - rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem sprzętu komputerowego lub gromadzone w kartotekach.

§ 3.

1. Podstawowym celem zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych jest zapewnienie jak najwyższego standardu bezpieczeństwa tych danych. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania, charakteru poufnego wraz z zachowaniem ich integralności oraz integralności systemu informatycznego.
2. Ochrona danych osobowych jest realizowana poprzez zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.
3. Zastosowane zabezpieczenia mają zapewnić poufność, integralność, rozliczalność danych oraz integralność systemu rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.
4. Za przestrzeganie zasad ochrony i bezpieczeństwa danych w komórkach organizacyjnych odpowiedzialni są kierownicy tych komórek oraz osoby na stanowiskach samodzielnych.

§ 4.

Realizację zamierzeń określonych w § 3 powinny zagwarantować następujące założenia:

1. Wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania danych osobowych oraz ich odpowiedzialność za ochronę tych danych,
2. Przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych,
3. Przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory) oraz zapewniających dostęp użytkowników do różnych poziomów zbiorów danych osobowych - stosownie do indywidualnego zakresu upoważnienia,
4. Okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych,
5. Opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii,
6. Wdrażanie nowych narzędzi metod pracy oraz sposobów zarządzania systemem informatycznym, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych i dostosowania go do najnowszych standardów

Rozdział II

Zasady dostępu użytkownika do systemu.

§ 1.

1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, zwanego dalej „systemem" może uzyskać wyłącznie osoba (użytkownik) zarejestrowana w tym systemie przez Administratora Systemu na wniosek kierownika komórki organizacyjnej i po akceptacji Administratora Bezpieczeństwa Informacji.
2. Rejestracja, o której mowa w punkcie 1, polega na nadaniu identyfikatora i przydziale hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu. Identyfikator umożliwia wykonywanie czynności zgodnie z zakresem powierzonych obowiązków, które wyznaczają poziom uprawnień.
3. Każdy użytkownik dopuszczony do przetwarzania danych osobowych posiada stosowne upoważnienie.
4. Administrator Systemu Informatycznego na wniosek kierownika komórki organizacyjnej właściwej dla użytkownika definiuje poziom uprawnień użytkownika określony w punkcie 2 niniejszego paragrafu.
5. Administrator Systemu Informatycznego zobowiązany jest do prowadzenia ewidencji przyznanych poszczególnym użytkownikom uprawnień związanych z dostępem do danych osobowych przetwarzanych w systemie informatycznym oraz zmian w zakresie przyznanych uprawnień.

§ 2.

1. Użytkownik systemu informatycznego przetwarzającego dane osobowe powinien posiadać umiejętność bezpiecznej obsługi komputera i dobrą znajomość oprogramowania systemowego z którego będzie korzystał.
2. Każdy użytkownik - przed dopuszczeniem do obsługi systemu informatycznego, w którym przetwarzane są dane osobowe - podlega przeszkoleniu w zakresie:
    a. obsługi komputera, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, które będzie wykorzystywał,
    b. przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków.
3. Wszyscy użytkownicy podlegają okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.
4. Za organizację szkoleń, o których mowa w punkcie 2, odpowiedzialny jest Administrator Bezpieczeństwa Informacji .
5. Szkolenia odbywają się na wniosek kierowników komórek organizacyjnych.

§ 3.

IDENTYFIKATOR

1. Identyfikator składa się z minimum sześciu znaków.
2. W identyfikatorze pomija się polskie znaki diakrytyczne.
3. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika Administrator Systemu po uzgodnieniu z ABI nadaje inny identyfikator.
4. Identyfikator użytkownika podlega rejestracji w systemie informatycznym.

§ 4.

H A S Ł A

Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

Hasło nie może być identyczne z identyfikatorem użytkownika, ani z jego imieniem lub nazwiskiem. Nie mogą zostać użyte kombinacje znaków mogące doprowadzić do łatwego rozszyfrowania haseł przez osoby nieupoważnione,

Nie mogą być w nich stosowane znaki następujące po sobie na klawiaturze bądź te same litery czy cyfry,

Zmiana hasła następuje nie rzadziej niż co 30 dni.

Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom.

Pierwsze hasło dla użytkownika ustala Administrator Systemu Informatycznego lub upoważniona przez niego osoba przy wprowadzaniu identyfikatora użytkownika do systemu.

Po otrzymaniu pierwszego hasła użytkownik zobowiązany jest zalogować się do systemu i zmienić hasło. Przy wpisywaniu hasło nie może być wyświetlane na ekranie.

Hasło podlega natychmiastowej zmianie w przypadku podejrzenia jego odkrycia przez nieupoważnioną osobę.

Hasła nie mogą być nigdzie zapisywane, z wyjątkiem haseł Administratora Systemu Informatycznego, które przechowywane są w opieczętowanych kopertach, w miejscu wyznaczonym przez Administratora Bezpieczeństwa Informacji.

§ 5.

Tryb przechowywania i udostępniania haseł Administratora Systemu Informatycznego:

1. Hasła Administratora Systemu Informatycznego przechowywane są w formie pisemnej w zapieczętowanej kopercie.
2. Koperta złożona jest w specjalnej szafie, do której dostęp posiada wyłącznie Starosta i osoby przez niego upoważnione.
3. Hasła, o którym mowa w pkt 1 dają najwyższe uprawnienia administracyjne do korzystania i obsługi systemu informatycznego.
4. Hasła zmieniane są co najmniej co 30 dni bądź natychmiast w przypadku podejrzenia odkrycia przez inną, nieupoważnioną osobę.
5. Nowe, aktualne hasło zabezpiecza się według procedur opisanych w pkt 1 i 2.
6. Koperta wraz z hasłem, które straciło ważność podlega zniszczeniu przy użyciu niszczarki dokumentów.
7. Niszczenia, o którym mowa w pkt 6 dokonuje Administrator Systemu Informatycznego w obecności Starosty lub osoby przez niego upoważnionej.
8. W sytuacjach awaryjnych zaistniałych pod nieobecność Administratora Systemu Informatycznego lub w razie jego niedyspozycji Starosta udostępnia hasło osobie przez siebie wyznaczonej.

Rozdział III

Rejestrowanie i wyrejestrowanie użytkowników.

---

§ 1.

1. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi osoba odpowiedzialna za sprawy kadrowe wyznaczona przez Administratora Danych.
2. Ewidencja zawiera:
    a. imię i nazwisko użytkownika,
    b. datę nadania i ustania upoważnienia,
    c. zakres upoważnienia,
    d. identyfikator użytkownika.
3. Postanowienia z punktu podpunkt d, nie dotyczą użytkowników, którzy mają dostęp wyłącznie do danych osobowych gromadzonych w kartotekach.
4. Ewidencja osób upoważnionych do przetwarzania danych osobowych może być prowadzona w systemie informatycznym i jest dostępna dla wszystkich użytkowników.
5. Nośniki magnetyczne (optyczne), na których gromadzone są kopie wykazów zawierających ewidencję przyznanych poszczególnym użytkownikom uprawnień przechowywane są w wyznaczonych szafach lub sejfach, do których ma dostęp wyłącznie Administrator Systemu Informatycznego oraz osoby upoważnione przez Administratora Danych.
6. Zmiany dotyczące użytkownika, takie jak, zmiana imienia lub nazwiska czy zmiana zakresu upoważnienia, podlegają niezwłocznemu odnotowaniu w ewidencji.

§ 2.

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemu.
2. Kierownicy komórek organizacyjnych oraz osoba odpowiedzialna za sprawy kadrowe w przypadku osób na samodzielnych stanowiskach odpowiadają za natychmiastowe zgłoszenie do Administratora Systemu Informatycznego, użytkowników, którzy utracili uprawnienia do dostępu do danych osobowych, celem zablokowania im dostępu do systemu informatycznego poprzez zablokowanie identyfikatora i wyrejestrowanie z ewidencji użytkowników
3. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.
4. Wyrejestrowanie następuje poprzez:
    a. zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
    b. usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).
5. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego jest:
    a. nieobecność w pracy trwająca dłużej niż 31 dni kalendarzowych,
    b. zawieszenie w pełnieniu obowiązków służbowych,
    c. zwolnienie z pełnienia obowiązków służbowych.
6. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.
7. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi .
8. Osoba prowadząca ewidencję osób upoważnionych do przetwarzania danych osobowych, obowiązana jest odrębnie gromadzić identyfikatory, które utraciły ważność lub też stosować odpowiednie ich oznaczenia.

Rozdział IV

Rozpoczęcie i zakończenie pracy w systemie.

---

§ 1.

1. Przed przystąpieniem do pracy z systemem informatycznym lub kartotekami, użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz dokonać oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie poufności danych osobowych.
2. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie systemu, użytkownik obowiązany jest postępować zgodnie z zasadami określonymi w Polityce bezpieczeństwa.

3. Rozpoczynając pracę na komputerze użytkownik loguje się do systemu informatycznego poprzez wprowadzenie swojego identyfikatora i hasła dokonując w ten sposób uwierzytelnienia.
4. Po przekroczeniu ustalonej liczby prób logowania system blokuje dostęp do systemu informatycznego na poziomie danego użytkownika .
5. Administrator Systemu Informatycznego ustala przyczyny zablokowania systemu oraz w zależności od zaistniałej sytuacji podejmuje odpowiednie działania. W uzasadnionych przypadkach o zaistniałym incydencie powiadamia Administratora Bezpieczeństwa Informacji lub osobę przez niego wyznaczoną.

§ 2.

1. Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest:
   a. wylogować się z systemu informatycznego lub,
   b. zablokować dostęp do konta.
2. Zakończenie pracy w systemie odbywa się poprzez:
   a. zamknięcie aplikacji,
   b. odłączenie się od zasobów systemowych,
   c. zamknięcie systemu operacyjnego,
   d. wyłączenie stacji roboczej,
   e. zabezpieczenie stanowiska pracy, w szczególności wszelkiej dokumentacji oraz nośników magnetycznych i optycznych, na których znajdują się dane osobowe, przed dostępem osób nieuprawnionych.

§ 3.

ZASADY PRACY W SYSTEMIE

Zabrania się użytkownikom pracującym w systemie:

1. udostępniania stacji roboczej osobom niezarejestrowanym z zastrzeżeniem pkt 2,
2. udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z Administratorem Systemu Informatycznego,
3. używania nielicencjonowanego oprogramowania.

Rozdział V

Zabezpieczenie systemu informatycznego.

§ 1.

System informatyczny zabezpiecza się przed:

1. działaniem, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
2. utratą danych spowodowaną:
3. działaniem nieautoryzowanego oprogramowania,
4. awarią zasilania łub zakłóceniami w sieci zasilającej.

§ 2.

1. Administrator Systemu Informatycznego odpowiada za niezwłoczne instalowanie na sprzęcie najnowszych wersji oprogramowania zabezpieczającego system informatyczny .
2. Nowe wersje oprogramowania instaluje wyłącznie Administrator Systemu Informatycznego lub upoważnione przez niego osoby niezwłocznie po ich otrzymaniu lub osoba upoważniona przez Administratora Systemu Informatycznego.
3. Okresowych kontroli w zakresie instalowania najnowszych wersji oprogramowania zabezpieczającego system informatyczny dokonuje Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona.
4. Na serwerach i stacjach roboczych używanych przez Administratora Danych powinno instalować się przynajmniej jeden program antywirusowy.
5. W komputerach przenośnych zawierających dane osobowe stosuje się środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

§ 3.

Zabezpieczenie antywirusowe

1. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie informatycznym, jak i do celów instalacyjnych.
2. Na serwerach, w miarę możliwości technicznych, oprogramowanie antywirusowe powinno być aktywne cały czas.

3. Na stacjach roboczych oprogramowanie antywirusowe powinno być aktywne cały czas i powinno dokonywać sprawdzenia każdego otwieranego lub uruchamianego pliku .
4. Użytkownicy są zobowiązani do dokonywania kontroli antywirusowej wszystkich nośników magnetycznych lub optycznych przychodzących z zewnątrz oraz okresowo nośników własnych .
5. W razie stwierdzenia zainfekowania systemu, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Administratora Systemu Informatycznego.
6. Administrator Systemu Informatycznego usuwa wirusa, jeśli automatycznie nie dokonał tego program antywirusowy oraz informuje Administratora Bezpieczeństwa Informacji lub osobę przez niego upoważnioną o dokonanych czynnościach i rodzaju wirusa.
7. W razie niemożności usunięcia wirusa, Administrator Systemu Informatycznego za zgodą Administratora Bezpieczeństwa Informacji, korzysta z usług zewnętrznych specjalistów w tej dziedzinie.
8. W sytuacji korzystania z usług zewnętrznych specjalistów, należy podjąć działania uniemożliwiające tym osobom dostęp do danych osobowych.
9. Administrator systemu informatycznego jest odpowiedzialny za kontrolę antywirusową serwerów i zasobów sieciowych.
10. Użytkownicy są odpowiedzialni za kontrolę antywirusową na dyskach lokalnych i używanych nośnikach danych.
11. Po usunięciu wirusa Administrator Systemu Informatycznego sprawdza zainfekowany system informatyczny oraz przywraca go do pełnej sprawności i funkcjonalności.
12. Administrator Systemu Informatycznego po usunięciu wirusa, sporządza raport o wystąpieniu wirusa. Raport winien zawierać następujące informacje:
    a. nazwę wirusa,
    b. datę wykrycia wirusa,
    c. miejsce zainfekowania,
    d. źródło infekcji.
13. Raport, o którym mowa w punkcie 12 przekazywany jest Administratorowi Bezpieczeństwa Informacji lub osobie przez niego wyznaczonej wraz z wnioskami, stosownymi do zaistniałej sytuacji.
14. Administrator Systemu Informatycznego prowadzi wykaz przypadków zainfekowania komputerów i nośników wykorzystywanych do przetwarzania danych osobowych w systemie oraz przechowuje kopie raportów.

§ 4.

Bezpieczeństwo komunikacji.

1. Bezpieczeństwo komunikacji w obrębie systemów przetwarzających dane osobowe Administrator Systemu zapewnia przy użyciu narzędzi w obrębie systemu.
2. W systemach działających sieciowo, na zasadzie udostępnienia zasobów na serwerze, Administrator Systemu powinien uwzględniać dedykowane przyzwolenia dostępu.

§ 5.

Komunikacja wewnętrzna.

1. Przesyłanie danych osobowych w komunikacji wewnętrznej (LAN) musi być oznaczone w sposób dostępny jedynie dla uprawnionych użytkowników przy użyciu narzędzi zabezpieczeń w obrębie systemu informatycznego.
2. W sytuacji, gdy dostępne narzędzia informatyczne nie będą wystarczające do działania w komunikacji wewnętrznej, użytkownik systemu wyznacza sposób postępowania, mając w szczególności na uwadze ochronę danych osobowych.
3. Do przesyłania danych przy połączeniach w sieci publicznej (Internet), z uwagi na przekazywane dane osobowe, powinny być wykorzystywane tylko kanały transmisji wykorzystywane przez autoryzowane programy wykorzystywane również w innych urzędach oraz instytucjach państwowych i w oparciu o przepisy prawne regulujące sposób wysyłania tych danych.

§ 6.

Bezpieczeństwo nośników i urządzeń.

1. Nośniki informatyczne zawierające dane osobowe powinny być opisane w sposób czytelny i zrozumiały dla użytkownika, a zarazem nie powinny ułatwiać rozpoznania zawartości przez osoby nieupoważnione.
2. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione.
3. W pomieszczeniach, gdzie nie jest możliwe ograniczenie dostępu osób postronnych, monitory stanowisk dostępu do danych osobowych ustawia się w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
4. Ekrany monitorów stanowisk dostępu do danych osobowych są zaopatrzone w wygaszacze z ustawioną opcją wymagania hasła, które po upływie maksymalnie 10 minut nieaktywności użytkownika automatycznie wyłączają możliwość eksploracji ekranu.
5. Osoby użytkujące przenośne nośniki informatyczne, służące do przetwarzania danych osobowych, obowiązane są niezwłocznie informować na piśmie Administratora Bezpieczeństwa Informacji o zakresie, rodzaju zbieranych danych osobowych oraz celu ich przetwarzania. Administrator Bezpieczeństwa Informacji może żądać usunięcia danych, co do których zachodzi uzasadnione podejrzenie, że nie są przetwarzane zgodnie z zasadami określonymi w przepisach o ochronie danych osobowych.
6. Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem ochrony danych w celu zapobieżenia dostępowi do tych danych osobie niepowołanej.

§ 7.

Wydruki.

1. Użytkownik sporządzający wydruki, które zawierają dane osobowe jest odpowiedzialny za zachowanie szczególnej ostrożności przy korzystaniu z nich, a zwłaszcza za zabezpieczenie ich przed dostępem osób nie posiadających imiennego upoważnienia oraz nieuprawnionych do wglądu.
2. Wydruki zawierające dane osobowe, które są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§ 8.

Zasilanie awaryjne i zasilanie energetyczne systemu informatycznego.

1. System i urządzenia informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, zabezpiecza się przed utratą danych osobowych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
2. Minimalne zabezpieczenie systemu i urządzeń informatycznych, o których mowa w punkcie 1, polega na wyposażeniu serwera (serwerów) oraz stacji roboczych w zasilacze awaryjne (UPS).
3. Serwer sieci powinien być zasilany przez UPS o odpowiednich parametrach, pozwalających na podtrzymanie napięcia przez minimum 15 minut oraz na wykonanie, bezpiecznego wyłączenia serwera, tak aby przed zanikiem zasilania zostały prawidłowo zakończone operacje rozpoczęte na zbiorze danych osobowych.
4. Zasilaczem awaryjnym powinna być zabezpieczona, co najmniej jedna stacja robocza.

Rozdział VI

Naruszenie bezpieczeństwa systemu.

---

§ 1.

1. Każdy przypadek naruszenia ochrony danych osobowych, które mogą wskazywać na naruszenie bezpieczeństwa podlega zgłoszeniu do Administratora Bezpieczeństwa Informacji, a w szczególności:
   a. naruszenia bezpieczeństwa systemu informatycznego,
   b. stwierdzenia objawów (stanu urządzeń, sposobu działania programu lub jakości komunikacji w sieci).
2. Administratorowi Bezpieczeństwa Informacji zgłasza się w szczególności przypadki:

a. użytkowania stacji roboczej przez osobę nie będącą użytkownikiem systemu,
b. usiłowania logowania się do systemu (sieci) przez osobę nieuprawnioną,
c. usuwania, dodawania lub modyfikowania bez wiedzy i zgody użytkownika jego dokumentów (rekordów),
d. przebywania osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe, w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych i bez zgody Administratora Danych, pozostawiania bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe,
e. udostępniania osobom nieuprawnionym stacji roboczej lub komputera przenośnego, służących do przetwarzania danych osobowych,
f. niezabezpieczenia hasłem dostępu do komputera służącego do przetwarzania danych osobowych,
g. przechowywania kopii awaryjnych w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco,
h. przechowywania nośników informacji oraz wydruków z danymi osobowymi, nieprzeznaczonymi do udostępniania, w warunkach umożliwiających do nich dostęp osobom nieuprawnionym.

3. Obowiązek dokonania zgłoszenia, o którym mowa w punkcie 1, spoczywa na każdym użytkowniku, który powziął podejrzenie o naruszeniu ochrony danych osobowych.
4. W przypadku naruszenia integralności bezpieczeństwa sieciowego, obowiązkiem Administratora Systemu jest natychmiastowe wstrzymanie udostępniania zasobów dla użytkowników i odłączenie serwerów od sieci.
5. Użytkownik sieci i Administrator Systemu w porozumieniu z Administratorem Bezpieczeństwa Informacji ustalają przyczyny naruszenia integralności bezpieczeństwa sieciowego.
6. Przywrócenie udostępniania zasobów użytkownikom może nastąpić dopiero po ustaleniu i usunięciu przyczyny naruszenia integralności bezpieczeństwa sieciowego.

Rozdział VII

Kopie zapasowe.

---

§ 1.

1. Kopie awaryjne tworzy się z następującą częstotliwością:
   a. kopie systemu finansowo - księgowego – dwa razy w miesiącu,
   b. kopie pozostałe - nie rzadziej niż raz na miesiąc.
2. Każdą kopię tworzy się na oddzielnym nośniku informatycznym.
3. Zabrania się przechowywania kopii awaryjnych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.

4. Za prawidłowe sporządzanie kopii zapasowych, ich oznakowanie i przechowywanie, odpowiedzialny jest Administrator Systemu Informatycznego.
5. Administrator Systemu przegląda okresowo kopie awaryjne i ocenia ich przydatność do odtworzenia zasobów systemu w przypadku jego awarii.
6. Stwierdzenie utraty przez kopie awaryjne waloru przydatności do celu, o którym mowa w punkcie 5, upoważnia Administratora Systemu do ich zniszczenia.
7. Użytkownicy obowiązani są przestrzegać terminów tworzenia doraźnych kopii zapasowych, o ile zostali do tego upoważnieni przez Administratora Systemu Informatycznego.
8. Użytkownicy określeni w punkcie 7 są odpowiedzialni za prawidłowe sporządzanie kopii zapasowych, ich oznakowanie i przechowywanie.
9. Zniszczenia kopii zapasowych, na nośnikach magnetycznych i optycznych dokonuje Administrator Systemu Informatycznego w obecności Administratora Bezpieczeństwa Informacji lub osoby przez niego wyznaczonej.
10. Z nośników magnetycznych i optycznych wielokrotnego użytku, np. CDRW dane należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku , gdy usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym odzyskanie danych.
11. Dane zawarte na nośnikach optycznych jednokrotnego użytku, np. CDR należy usuwać poprzez całkowite zniszczenie nośnika.

Rozdział VIII

Sprzęt i oprogramowanie.

§ 1.

1. Sprzęt obsługujący zbiór danych osobowych składa się z komputerów stacjonarnych klasy PC.
2. Komputery przenośne mogą być używane do przetwarzania danych osobowych po odpowiednim ich zabezpieczeniu.
3. Użytkownik korzystający z komputera przenośnego jest zobowiązany do zachowania szczególnej ostrożności podczas transportu komputera oraz nie może udostępnić komputera osobom nieupoważnionym.
4. Sieć komputerowa służąca do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu komputerowego.
5. Sieć komputerowa powinna być podłączona do zasilania zapasowego (zasilanie dwustronne, agregat prądotwórczy lub UPS). Oprogramowanie powinno zapewnić bezpieczne wyłączanie systemu informatycznego, po dokonaniu operacji zamknięcia w pracujących aplikacjach i oprogramowaniu systemowym.
6. Za prawidłowe zasilanie energetyczne sieci komputerowej odpowiedzialny jest Administrator Systemu Informatycznego.

7. Infrastruktura techniczna związana z siecią komputerową i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych .
8. Wszystkie urządzenia w sieci komputerowej (pozostałe stacje robocze, drukarki, modemy itd.) powinny być w miarę możliwości technicznych, włączone do wydzielonej sieci energetycznej zapewniającej odpowiednie i zabezpieczenie przed przepięciami.
9. Gniazda zasilania sieci komputerowej powinny być odpowiednio oznakowane, zabezpieczone przed włączeniem do nich innych odbiorników lub wykonane w specjalnym standardzie.

§ 2.

1. Dane osobowe przesyłane na nośnikach magnetycznych i optycznych oraz za pomocą systemów teleinformatycznych powinny być zabezpieczone w sposób uniemożliwiający dostęp do nich osób nieupoważnionych .
2. Dane osobowe przesyłane po łączach telekomunikacyjnych wewnątrz danej sieci powinny być dodatkowo zabezpieczone w sposób uniemożliwiający dostęp do danej sieci LAN z innej sieci.
3. Dane osobowe przesyłane po łączach telekomunikacyjnych na zewnątrz powinny być w miarę możliwości technicznych szyfrowane za pomocą algorytmu kryptograficznego.
4. Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje.
5. Administrator Systemu Informatycznego odpowiada za audyt oprogramowania i prowadzenie dokładnego zestawienia zainstalowanych programów, ich lokalizacji i licencji.

§ 3.

1. Administrator Systemu Informatycznego odpowiada za wyposażenie systemu informatycznego w mechanizmy uwierzytelniania użytkownika oraz za sprawowanie kontroli dostępu do danych osobowych jedynie osób upoważnionych.
2. System informatyczny wykorzystywany jest przez użytkowników wyłącznie w celach służbowych. Wyjątki od powyższej reguły możliwe są jedynie za wyraźną zgodą Administratora Danych.
3. System informatyczny może być monitorowany, w tym również z zastosowaniem specjalistycznego oprogramowania lub sprzętu, w celu rejestracji aktywności użytkowników oraz sposobu wykorzystywania systemu informatycznego przez użytkowników .
4. Ekrany monitorów powinny być wyposażone w wygaszacze zabezpieczone hasłem, które aktywują się automatycznie po upływie określonego czasu od ostatniego użycia komputera.
5. Ekrany monitorów, powinny być ustawione w taki sposób, żeby w miarę możliwości uniemożliwić odczyt wyświetlanych informacji osobom nieupoważnionym.
6. Za spełnienie obowiązku określonego w punkcie 2 odpowiadają użytkownicy i kierownicy komórek organizacyjnych .

§ 4.

1. Administrator Systemu Informatycznego jest odpowiedzialny za to, aby dla każdej osoby, której dane osobowe są przetwarzane, system informatyczny zapewniał odnotowanie:
    a. daty pierwszego wprowadzenia danych do systemu,
    b. identyfikatora użytkownika wprowadzającego dane, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba,
    c. źródła danych, w przypadku zbierania danych nie od osoby, której one dotyczą,
    d. informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych,
    e. sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 7, po jego uwzględnieniu oraz sprzeciwu określonego w art. 32 ust. 1 pkt 8, ustawy o ochronie danych osobowych.
2. Wymagania określone w niniejszym ustępie nie dotyczą systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie.
3. Odnotowanie informacji, o których mowa w punkcie 1 podpunkt a i b, następuje automatycznie po zatwierdzeniu przez użytkowni ka operacji wprowadzania danych.
4. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w punkcie 1.
5. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w punkcie 1 podpunkt d, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.
6. Do czasu spełnienia przez system informatyczny wszystkich wyżej wymienionych wymogów, system informatyczny powinien zapewnić odnotowanie:
    a. daty pierwszego wprowadzenia danych do użytku wewnętrznego
    b. identyfikatora użytkownika wprowadzającego dane, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba.
7. Do chwili spełnienia przez system informatyczny wszystkich wymogów określonych w niniejszym paragrafie, odnotowanie informacji określonych w punkcie 1 podpunkt c, d, e należy prowadzić w formie tradycyjnej (papierowej) lub komputerowo poza systemem.

Rozdział IX

Serwis, przegląd i konserwacje.

---

§ 1.

1. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać do naprawy, do likwidacji dopiero po uprzednim uzyskaniu zgody Administratora Bezpieczeństwa Informacji.
2. Urządzenia, o których mowa w punkcie 1 przed ich przekazaniem pozbawia się zapisu danych osobowych poprzez wymontowanie dysku twardego z zastrzeżeniem punkt 3.
3. Jeżeli nie jest to możliwe, urządzenie to może być naprawiane wyłącznie pod nadzorem Administratora Systemu.
4. Jeżeli nie jest możliwe pozbawienie urządzenia przekazywanego do likwidacji zapisu danych osobowych, urządzenie - przed przekazaniem - uszkadza się w sposób uniemożliwiający odczytanie tych danych.

§ 2.

1. Przeglądu i konserwacji systemu dokonuje Administrator Systemu doraźnie.
2. Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) Administrator Systemu dokonuje nie rzadziej niż raz na dwa tygodnie.
3. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale Administratora Systemu nie rzadziej niż raz na dwa tygodnie.

Rozdział X

Przetwarzanie danych osobowych.

§ 1.

1. Dane osobowe przetwarzane są w kartotekach oraz w komputerach do tego przeznaczonych (serwerach, stacjach roboczych) zlokalizowanych w obszarach przetwarzania danych osobowych.
2. W wypadku przekazywania urządzeń lub nośników zawierających dane osobowe, zwłaszcza tzw. „wrażliwe", o których mowa w art. 27 ust. 1 ustawy o ochronie danych osobowych, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność i integralność tych danych, przez co rozumie się:
    a. ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi, lub
    b. stosowanie metod kryptograficznych, lub
    c. stosowanie odpowiednich zabezpieczeń fizycznych, lub
    d. w zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń.
3. Dane osobowe zapisywane na nośnikach zewnętrznych (streamer, dyski: wymienne, magnetyczne, optyczne) tworzące kopie zapasowe kolejnych okresów, powinny być przechowywane w wyznaczonych, odpowiednio zabezpieczonych, pomieszczeniach.
4. Kartoteki powinny być przechowywane w szafach, znajdujących się w wyznaczonych, odpowiednio zabezpieczonych, pomieszczeniach.
5. Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.
6. Szczegółowy opis obszaru przetwarzania danych osobowych oraz środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności danych osobowych określony jest w Polityce bezpieczeństwa.

§ 2.

1. Kartoteka przekazywana jest do archiwum zgodnie z procedurami archiwizacji dokumentów.
2. Likwidacji zbiorów archiwalnych dokonuje się przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie.
3. Decyzję o likwidacji zbiorów danych osobowych, przetwarzanych w kartotekach oraz systemach informatycznych podejmuje Administrator Danych lub osoby przez niego upoważnione na wniosek Administratora Bezpieczeństwa Informacji.

4. Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów danych osobowych, Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona sporządza protokół, w którym zamieszcza następujące informacje:
    a. datę dokonania likwidacji,
    b. przedmiot likwidacji (nośniki, kartoteka),
    c. przedział czasowy likwidowanych zbiorów danych osobowych,
    d. podpisy osób dokonujących i obecnych przy likwidacji zbiorów danych osobowych.

Rozdział XI

Podsumowanie i przepisy końcowe.

---

§ 1.

Odpowiedzialność

Naruszenie obowiązków wynikających z niniejszej Polityki Bezpieczeństwa oraz przepisów ustawy o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym w szczególności wynikającym z przepisów tejże ustawy.

§ 2.

Obowiązki Administratora Bezpieczeństwa Informacji

Do obowiązków Administratora Bezpieczeństwa Informacji w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

nadzór nad stosowaniem środków ochrony,

nadzór nad przestrzeganiem przez Administratora Systemów Informatycznych i użytkowników systemu - procedur bezpieczeństwa,

wskazywanie zagrożeń oraz reagowanie na naruszenia ochrony danych osobowych i usuwanie ich skutków,

prowadzenie ewidencji użytkowników systemów informatycznych, w których przetwarzane są dane osobowe, która jest częścią ewidencji osób upoważnionych do przetwarzania danych osobowych oraz wszelkiej dokumentacji opisującej sposób realizacji i zasady ochrony danych osobowych w Starostwie Powiatowym w Turku,

kontrolowanie nadanych w systemach informatycznych uprawnień do przetwarzania danych osobowych pod kątem ich zgodności z wpisami umieszczonymi w ewidencji osób upoważnionych do przetwarzania danych osobowych.

prowadzenie szkoleń dla użytkowników w zakresie stosowanych w systemach informatycznych środków ochrony danych osobowych,

prowadzenie rejestru zbiorów będących w zasobach Administratora danych,

współdziałanie z Generalnym Inspektorem Ochrony Danych Osobowych w zakresie sprawdzeń zleconych przez GIODO,

uzgadnianie z Administratorem Systemów Informatycznych procedur regulujących wykonywanie czynności w systemach lub aplikacjach służących do przetwarzania danych osobowych.

§ 3.

Obowiązki Administratora Systemów Informatycznych

Do obowiązków Administratora Systemów Informatycznych w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

realizacja zadań związanych z przeszkoleniem użytkowników w zakresie obsługi sprzętu informatycznego, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji , którą będą wykorzystywali,

zapoznanie użytkowników z treścią Instrukcji,

operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę danych osobowych w nich przetwarzanych,

przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa,

kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym,

zarządzanie stosowanymi w systemach informatycznym środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień,

utrzymanie systemu w należytej sprawności technicznej,

regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych,

wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami, sprzętu IT, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których przetwarzane są dane osobowe.

§ 4.

Przepisy końcowe.

W sprawach nieuregulowanych w niniejszej Instrukcji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r. poz. 1182, z późn. zm.) oraz rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).

ZATWIERDZAM

STAROSTA

Maxius Seńko

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W STAROSTWIE POWIATOWYM W TURKU

Opracował
Robert Wojdyła
Administrator Bezpieczeństwa Informacji
w Starostwie Powiatowym w Turku

Rozdział I

Postanowienia ogólne.

§ 1.

Polityka bezpieczeństwa została opracowana w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182) oraz rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024). Dokument został opracowany zgodnie z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osób oraz ochrony prywatności w sektorze komunikacji elektronicznej.

§ 2.

Polityka określa tryb i zasady ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Turku.

§ 3.

Ilekroć w Polityce jest mowa o:

1. **Staroście** - rozumie się przez to Starostę Tureckiego,
2. **zbiorze danych osobowych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
3. **danych osobowych** - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
4. **przetwarzaniu 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;
5. **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

6. **systemie tradycyjnym** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
7. **zabezpieczeniu danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
8. **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
9. **Administratorze Danych Osobowych zwanym też Administratorem Danych (ADO)** - w świetle art. 3 i 7 pkt 4 ustawy o ochronie danych osobowych rozumie się przez to Starostę Tureckiego, który decyduje o celach i środkach przetwarzania danych osobowych;
10. **Administratorze Bezpieczeństwa Informacji zwanym też Administratorem Bezpieczeństwa (ABI)**- rozumie się przez to osobę wyznaczoną przez Starostę Tureckiego, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
11. **Administratorze Systemu Informatycznego zwanym też Administratorem Systemu (ASI)** - rozumie się przez to osobę zatrudnioną przez kierownika jednostki upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;
12. **kierownik komórki organizacyjnej** – rozumie się również samodzielne stanowisko pracy,
13. **komórce organizacyjnej** - rozumie się przez to każdą wydzieloną organizacyjnie i funkcjonalnie komórkę wewnętrzną, zgodnie z regulaminem organizacyjnym,
14. **użytkowniku systemu zwanym też użytkownikiem systemu informatycznego** - rozumie się przez to upoważnionego przez Starostę Tureckiego, wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika, który odbył szkolenie prowadzone przez ABI w zakresie ochrony tych danych;
15. **zgodzie osoby, której te dane dotyczą** - rozumie się przez 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.
16. **kartotece** - rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierającej dane osobowe,
17. **pracowniku ochrony** - rozumie się przez to osobę wykonującą zadania z zakresu ochrony osób i mienia na rzecz Administratora Danych,
18. **pomieszczeniach** - rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz gromadzone w kartotekach .

§ 4.

W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.

Rozdział II

Cele i zasady.

§ 1.

1. Celem opracowania Polityki bezpieczeństwa jest ochrona danych osobowych przed niepowołanym dostępem do zgromadzonych i przetwarzanych danych.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów i zapewnić:
    a. poufność danych - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
    b. integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
    c. rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
    d. integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej .
3. Za przestrzeganie zasad ochrony i bezpieczeństwa danych w komórkach organizacyjnych odpowiedzialni są kierownicy tych komórek oraz osoby na stanowiskach samodzielnych.

§ 2.

1. Realizację zamierzeń określonych w § 1 powinny zagwarantować następujące założenia:
2. wdrożenie procedur określających postępowanie osób upoważnionych do przetwarzania danych osobowych oraz ich odpowiedzialność za ochronę tych danych,
3. przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych,
4. przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory) oraz zapewniających dostęp użytkowników do różnych poziomów zbiorów danych osobowych - stosownie do indywidualnego zakresu upoważnienia,
5. podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń,
6. okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych,
7. opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii,
8. śledzenie osiągnięć w dziedzinie zabezpieczania systemów informatycznych i w miarę możliwości organizacyjnych i techniczno-finansowych - wdrażanie nowych rozwiązań oraz sposobów zarządzania systemem informatycznym, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

§ 3.

Dane osobowe w Starostwie Powiatowym w Turku są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach ,zestawieniach oraz w innych zestawach i zbiorach ewidencyjnych poszczególnych komórek organizacyjnych Starostwa Powiatowego w Turku na dokumentach papierowych, jak również w systemach informatycznych na elektronicznych nośnikach informacji.

§ 4.

Polityka bezpieczeństwa wprowadza regulacje w zakresie zasad organizacji procesu przetwarzania danych osobowych i odnosi się swoją treścią do informacji:

1. w formie papierowej - przetwarzanej w ramach systemu tradycyjnego;
2. w formie elektronicznej - przetwarzanej w ramach systemu informatycznego.

§ 5.

Procedury i zasady określone w niniejszej Polityce bezpieczeństwa stosuje się do wszystkich pracowników Starostwa Powiatowego w Turku, jak i innych osób mających dostęp do danych osobowych przetwarzanych w Starostwie Powiatowym w Turku (np. osób realizujących zadania na podstawie umów zlecenia lub o dzieło, wolontariuszy, stażystów, praktykantów, serwisantów).

§ 6.

1. Przetwarzanie danych osobowych do celów związanych z działalnością Administratora Danych jest zgodne z prawem w sytuacji, gdy dane te zostały uzyskane od osoby, której dotyczą i wyraziła ona na ich przetwarzanie zgodę.
2. W sytuacji, gdy dane osobowe nie zostały uzyskane od osoby, której dotyczą, to ich przetwarzanie jest zgodne z prawem, gdy przepis szczególny tak stanowi.
3. Usunięcie danych nie wymaga zgody osoby, której dotyczą.
4. Ocena niezbędności przetwarzania danych do wypełnienia usprawiedliwionych celów Administratora Danych powinna być dokonywana indywidualnie w każdej sytuacji.

§ 7.

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, w wypadkach przewidzianych ustawą należy poinformować tę osobę o:
    a. adresie swojej siedziby i pełnej nazwie,
    b. celu zbierania danych, a w szczególności o znanych w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,

c. prawie dostępu do treści swoich danych oraz ich poprawiania,
d. dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

2. Powyższy obowiązek Administrator Danych nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych.

§ 8.

1. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, Administrator Danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:
   a. adresie swojej siedziby i pełnej nazwie,
   b. celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
   c. źródle danych,
   d. prawie dostępu do treści swoich danych oraz ich poprawiania,
   e. prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, jeżeli nawet przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą,
   f. prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.
2. Powyższy obowiązek Administrator Danych nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych.

§ 9.

Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawują Kierownicy komórek organizacyjnych.

§ 10.

1. Z zasadami w Polityce bezpieczeństwa obowiązkowo są zapoznawani wszyscy użytkownicy systemów tradycyjnych i informatycznych, składając odpowiednie oświadczenie, którego wzór stanowi załącznik Nr 1 do Polityki.
2. Oświadczenie przechowywane jest w aktach osobowych pracownika a drugi egzemplarz w dokumentacji ABI.

§ 11.

1. Do informacji przechowywanych w systemach tradycyjnych jak i informatycznych mają dostęp jedynie upoważnieni pracownicy Starostwa Powiatowego w Turku oraz osoby mające imienne, zarejestrowane upoważnienie. Wszyscy pracownicy zobowiązani są do zachowania tych danych w tajemnicy. Dopuszczalny sposób i zakres przetwarzania danych osobowych regulują zapisy ustaw kompetencyjnych, właściwych dla komórek organizacyjnych Starostwa Powiatowego w Turku;
2. Upoważnienie określone w ust. 1 przechowywane jest w aktach osobowych pracownika a drugi egzemplarz w dokumentacji ABI;
3. Ewidencję osób uprawnionych do przetwarzania danych osobowych prowadzi Administrator Bezpieczeństwa Informacji;

§ 12.

1. Dane osobowe są chronione zgodnie z polskim prawem oraz procedurami obowiązującymi w jednostce organizacyjnej dotyczącymi bezpieczeństwa i poufności przetwarzanych danych.
2. Systemy informatyczne oraz tradycyjne, które przechowują dane osobowe, są chronione odpowiednimi środkami technicznymi.

§ 13.

1. Za naruszenie ochrony danych osobowych uważa się w szczególności:
    a. nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują,
    b. naruszenie lub próby naruszenia integralności danych rozumiane jako wszelkie modyfikacje, zniszczenia lub próby ich dokonania przez osoby nieuprawnione lub uprawnione działające w złej wierze lub jako błąd w działaniu osoby uprawnionej (np. zmianę zawartości danych, utratę całości lub części danych),
    c. naruszenie lub próby naruszenia integralności systemu,
    d. zmianę lub utratę danych zapisanych na kopiach zapasowych,
    e. naruszenie lub próby naruszenia poufności danych lub ich części,
    f. nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
    g. udostępnienie osobom nieupoważnionym danych osobowych lub ich części,
    h. zniszczenie, uszkodzenie lub wszelkie próby ingerencji nieuprawnionej w system informatyczny zmierzające do zakłócenia jego działania bądź pozyskania w sposób niedozwolony (lub w celach niezgodnych z przeznaczeniem) danych zawartych w systemie informatycznym lub kartotekach,

i. inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy,

2. Za naruszenie ochrony danych osobowych uważa się również włamanie do budynku lub pomieszczeń, w których przetwarzane są dane osobowe lub próby takich działań.

Rozdział III

Administracja i organizacja bezpieczeństwa.

---

§ 1.

1. Za bezpieczeństwo danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada Administrator Danych Osobowych (ADO).
2. Kierownicy komórek organizacyjnych obowiązani są zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinni zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 2.

Administrator Danych Osobowych może powołać Administratora Bezpieczeństwa Informacji, nadzorującego przestrzeganie zasad ochrony. Prowadzi on dokumentację opisującą sposób przetwarzania danych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

§ 3.

1. Administrator Bezpieczeństwa Informacji wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemami informatycznymi i tradycyjnymi.

2. Administrator Bezpieczeństwa Informacji jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, tak by wyłącznie uprawniony użytkownik miał dostęp do systemów informatycznych i tradycyjnych.
3. Administrator Bezpieczeństwa Informacji posiada bieżącą listę osób upoważnionych do przetwarzania danych osobowych.
4. Szczegółowy zakres odpowiedzialności i obowiązków Administratora Bezpieczeństwa Informacji jest następujący:
    a. zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
        i. sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
        ii. nadzorowanie opracowania i aktualizowania dokumentacji oraz przestrzegania zasad w niej określonych,
        iii. administrator danych jest zobowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednia do zagrożeń oraz kategorii danych objętych ochroną , a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą , utratą, uszkodzeniem lub zniszczeniem.
        iv. zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych (szkolenia);
    b. prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych,
    c. nadzoruje bezpieczeństwo systemów informatycznych i tradycyjnych;
    d. nadzoruje przestrzeganie przez wszystkich użytkowników stosowanie obowiązujących procedur;
    e. weryfikuje listę autoryzowanych użytkowników systemów informatycznych;
    f. doradza użytkownikom w zakresie bezpieczeństwa;
    g. dba, aby użytkownicy mający dostęp do systemu posiadali stosowne upoważnienia
    h. oraz byli przeszkoleni w zakresie obowiązujących regulacji bezpieczeństwa;
    i. prowadzi kontrolę w zakresie bezpieczeństwa;
    j. prowadzi postępowanie wyjaśniające w przypadku naruszenia ochrony danych osobowych,
    k. przygotowuje wnioski pokontrolne dla Administratora Danych Osobowych,
    l. prowadzi rejestr zbiorów danych osobowych przetwarzanych przez administratora danych.

§ 4.

1. Administrator Danych Osobowych wyznacza Administratora Systemu Informatycznego (ASI), który posiada najwyższe uprawnienia w systemie informatycznym. Tylko ASI jest osobą uprawnioną do instalowania i usuwania oprogramowania systemowego i narzędziowego.
2. Administrator Systemu Informatycznego wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemem informatycznym. Jest zobowiązany do zapewnienia,

poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, w taki sposób, że wyłącznie uprawniony użytkownik ma dostęp do systemów informatycznych.

3. Szczegółowy zakres odpowiedzialności i obowiązków Administratora Systemu Informatycznego jest następujący:
    a. zapewnia stałą sprawność urządzeń mających wpływ na bezpieczeństwo danych;
    b. odpowiada za bezpieczeństwo systemu informatycznego;
    c. zobowiązuje i bieżąco kontroluje stosowanie się użytkowników do obowiązujących procedur;
    d. utrzymuje i aktualizuje listę autoryzowanych użytkowników systemu informatycznego;
    e. zapewnia aktualizację dokumentacji technicznej systemu w tym opis struktur zbiorów
    f. i ich zależności;
    g. prowadzi nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisywane są dane osobowe;
    h. wykonuje kopie awaryjne/archiwalne /oraz nadzoruje ich przechowywanie;
    i. wprowadza i nadzoruje mechanizmy autoryzacji.

§ 5.

Kierownik komórki organizacyjnej odpowiada za przestrzeganie ustawy o ochronie danych oraz przepisów wewnętrznych na poszczególnych stanowiskach, a w szczególności:

1. kontroluje sposób zabezpieczenia zbiorów danych osobowych przez pracowników,
2. kontroluje sposób realizacji obowiązku udzielania informacji o jakich mowa w ustawie,
3. zgłasza ABI planowaną rejestrację nowych zbiorów oraz przygotowuje wniosek w tej sprawie,
4. wnioskuje o nadanie upoważnień do przetwarzania danych osobowych pracownikom,
5. zgłasza potrzeby w zakresie zabezpieczenia danych osobowych w Starostwie Powiatowym w Turku.

§ 6.

1. Użytkownik systemu wykonuje wszystkie prace niezbędne do efektywnej oraz bezpiecznej pracy na stanowisku pracy również z wykorzystaniem stacji roboczej. Jest odpowiedzialny przed Administratorem Bezpieczeństwa Informacji za realizację i utrzymanie niezbędnych warunków bezpieczeństwa, w szczególności do przestrzegania procedur dostępu do systemu i ochrony danych osobowych.
2. Użytkownicy powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych. W tym celu należy:
    a. zwracać szczególną uwagę przy wchodzeniu wychodzeniu z obiektu na podejrzane osoby lub samochody parkujące w pobliżu,
    b. przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń , a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych,
    c. informować Administratora Bezpieczeństwa Informacji lub pracowników ochrony o podejrzanych osobach, tj.:

i. osobach zachowujących się nienormalnie np. nieodpowiednio ubranych do pory roku, dnia i pogody;
ii. osobach przebywających w obiekcie bez wyraźnego celu;
iii. osobach posiadających przy sobie podejrzane bagaże, w których mogą być ukryte niebezpieczne przedmioty;

d. przestrzegać zasad i procedur ochrony danych osobowych, w czasie pracy, a także po jej zakończeniu.

3. Kierownicy komórek organizacyjnych, a także osoby na stanowiskach samodzielnych oraz użytkownicy zobowiązani są, na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać Administratorowi Bezpieczeństwa Informacji projekty i propozycje stosownych rozwiązań, których celem jest zabezpieczenie przed naruszeniem ochrony danych osobowych.

Rozdział IV

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

§ 1.

1. Dane osobowe są gromadzone, przechowywane i przetwarzane w kartotekach, skorowidzach, księgach, wykazach oraz w innych zbiorach ewidencyjnych poszczególnych komórek organizacyjnych jednostki organizacyjnej w postaci dokumentów papierowych i w systemie informatycznym, w którym stosowane są pakiety biurowe lub wyspecjalizowane aplikacje (programy).
2. Zestawienie zbiorów danych osobowych oraz programów do przetwarzania tych danych stanowi załącznik Nr 4 do polityki bezpieczeństwa.

§ 2.

1. Ze względu na rodzaj i charakter danych osobowych zawartych w zbiorach, w Starostwie Powiatowym w Turku wyróżnia się dwie kategorie danych:
   a. dane osobowe zwykłe - wszelkie dane (informacje) dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zgromadzone w zbiorach danych osobowych.
   b. dane osobowe szczególnie chronione – zgodnie z art.27 ust.1 ustawy o ochronie danych osobowych (art. 27 ust. 1) wszelkie dane (informacje) ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, przynależność partyjną lub związkową, jak również informacje o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazania osoby,

orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

§ 3.

Zgodnie z postanowieniami art. 40 ustawy o ochronie danych osobowych, z uwagi na gromadzone kategorie zbiorów danych osobowych istnieje obowiązek zgłoszenia do rejestracji tych zbiorów Generalnemu Inspektorowi Ochrony Danych Osobowych z wyjątkiem przypadków, o których mowa w art. 43 ust. 1i 1a tejże ustawy.

Rozdział V

Przetwarzanie danych osobowych.

---

§ 1.

2. Przetwarzanie danych osobowych z użyciem stacjonarnego sprzętu komputerowego i kartotek odbywa się wyłącznie w obszarze przetwarzania danych, w pomieszczeniach Administratora Danych.
3. Przetwarzanie danych osobowych w urządzeniach przenośnych może odbywać się poza obszarem przetwarzania danych wyłącznie za zgodą Starosty lub osób przez niego upoważnionych .
4. Przetwarzanie, w tym udostępnianie danych osobowych jest prawnie dopuszczalne, jeżeli jest niezbędne dla zrealizowania uprawnienia łub spełnienia obowiązku wynikającego z przepisu prawa.
5. Podmiot występujący o udostępnienie danych osobowych powinien wskazać podstawę prawną upoważniającą go do otrzymania tych danych albo uzasadnioną potrzebę żądania ich udostępnienia. Tylko w takiej sytuacji można dokonać oceny, czy w określonym przypadku udostępnienie danych jest prawnie dopuszczalne, i czy nie będzie ono stanowić naruszenia zasad ochrony danych osobowych.
6. Przetwarzanie, w tym udostępnianie danych osobowych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje w celach badań naukowych, dydaktycznych, historycznych lub statystycznych, z zachowaniem przepisów art. 23 i 25 ustawy o ochronie danych osobowych.
7. Udostępnienie danych osobowych może nastąpić jedynie za zgodą Administratora Danych lub osób przez niego upoważnionych.

§ 2.

W celu ograniczenia dostępu osób postronnych do pomieszczeń, w których zlokalizowano przetwarzanie danych osobowych, należy zapewnić, aby:

1. drzwi wejściowe były zabezpieczone tak, aby otwarcie z zewnątrz mogło nastąpić wyłącznie przez uprawnione osoby,
2. wydawanie kluczy pozwalających na wejście do urzędu podlegało rejestracji, z jednoczesnym poświadczeniem przez osobę odbierającą, faktu otrzymania kluczy,
3. budynek był chroniony i monitorowany w systemie 24 godzinnym przez wszystkie dni w roku. Monitorowaniu powinny podlegać wyznaczone pomieszczenia w stopniu adekwatnym do ich przeznaczenia,
4. pomieszczenia, w których znajdują się serwery były wyposażone w miarę możliwości w sprawne systemy klimatyzacji, ochrony przeciwpożarowej i przeciwwłamaniowej,
5. pracownicy Administratora Danych oraz pracownicy ochrony są zobowiązani do przestrzegania zasad określających dopuszczalne sposoby przemieszczania się osób trzecich w obrębie pomieszczeń, w których przetwarzane są dane osobowe,
6. przebywanie osób trzecich w pomieszczeniach tworzących obszar przetwarzania danych może odbywać się wyłącznie w obecności użytkowników lub za zgodą Administratora Danych.

§ 3.

Przebywanie użytkownika po godzinach pracy w pomieszczeniach, w których przetwarzane są dane osobowe jest dopuszczalne jedynie za zgodą Starosty lub osób przez niego upoważnionych.

§ 4.

W trakcie prac technicznych wykonywanych przez osoby trzecie w pomieszczeniach, przetwarzanie danych osobowych jest zabronione.

§ 5.

1. Administrator Bezpieczeństwa Informacji nadzoruje przestrzeganie zasad ochrony przetwarzanych danych osobowych.
2. W celu sprawnego wykonywania swoich zadań Administrator Bezpieczeństwa Informacji jest uprawniony do wnioskowania do Starosty o wyznaczanie kierownikom komórek organizacyjnych oraz użytkownikom określonych zadań.
3. Kierownicy komórek organizacyjnych oraz pracownicy na stanowiskach samodzielnych zobowiązani są do przestrzegania przepisów o ochronie danych osobowych na terenie

podległych komórek organizacyjnych, a także do ścisłej współpracy z Administratorem Bezpieczeństwa Informacji. W tym celu zobowiązani są do:

a. pisemnego wnioskowania do Administratora Bezpieczeństwa Informacji o rejestrację nowych zbiorów danych osobowych,
b. pisemnego wnioskowania do Administratora Bezpieczeństwa Informacji o konieczności aktualizacji zbiorów danych osobowych.
c. okresowego składania pisemnej informacji z przebiegu bieżącej kontroli i oceny funkcjonowania mechanizmów zabezpieczeń i ochrony,
d. występowania z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych.

§ 6.

1. Osoby odpowiedzialne za poszczególne zbiory zobowiązane są do pisemnego zgłaszania do Administratora Bezpieczeństwa Informacji konieczności aktualizacji zarejestrowanych zbiorów danych osobowych oraz opracowywania stosownych zgłoszeń zmian w zbiorach.
2. Administrator Systemu Informatycznego odpowiedzialny jest za pisemne zgłaszanie do Administratora Bezpieczeństwa Informacji nazw programów wykorzystywanych do przetwarzania danych osobowych.

Rozdział VI

Sposób przepływu danych pomiędzy poszczególnymi systemami.

---

§ 1.

1. Obieg dokumentów zawierających dane osobowe, pomiędzy komórkami organizacyjnymi jednostki , winien się odbywać w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji).
2. Przekazywanie informacji (danych) w systemie informatycznym poza sieć lokalną jednostki odbywa się w relacji jednostka organizacyjna - mieszkańcy, przedsiębiorcy, kontrahenci, zakład ubezpieczeń społecznych, urząd skarbowy, banki, Narodowy Fundusz Ochrony Zdrowia, urząd wojewódzki, urząd marszałkowski inne jednostki administracji samorządowej i rządowej.
3. Zabronione jest jednoczesne podłączanie komputerów do sieci wewnętrznej Starostwa Powiatowego w Turku i sieci zewnętrznych (Plus, Era, Orange, Play, pozostałe sieci komórkowe, WiFi, WiMAX itp.).

Rozdział VII

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

§ 1.

1. Dostęp do danych wprowadzonych przez użytkowników systemów informatycznych mają jedynie upoważnione osoby oraz Administrator Systemu Informatycznego zapewniający jego prawidłową eksploatację.
2. Pomieszczenia, w których przetwarza się dane osobowe powinny być fizycznie zabezpieczone przed dostępem osób nieuprawnionych, to znaczy posiadać odpowiednie zamki do drzwi, zabezpieczenia w oknach (w szczególności na parterze) oraz być wyposażone w środki ochrony ppoż.
3. W pomieszczeniach gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób by uniemożliwić tym osobom wgląd w dane osobowe.
4. Dokumenty i nośniki informacji, zawierające dane osobowe powinny być zabezpieczone przed dostępem osób nieupoważnionych do przetwarzania danych. Jeśli nie są aktualnie używane powinny być przechowywane w szafach lub w innych przeznaczonych do tego celu urządzeniach biurowych, posiadających odpowiednie zabezpieczenia.

§ 2.

1. Stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe, mają tylko użytkownicy.
2. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe, osób innych, niż wymienione w ust. 1, jest możliwy wyłącznie w obecności, co najmniej jednego użytkownika lub za zgodą Starosty.
3. Zakaz wyrażony w ust. 2 dotyczy innych, niż określeni w ust. 1, pracowników Administratora Danych oraz pracowników służb technicznych, porządkowych, itp.

§ 3.

1. Klucze do pomieszczeń przechowywane są w wyznaczonym pomieszczeniu.
2. Klucze wydawane są wyłącznie osobom do tego uprawnionym.
3. Klucze zapasowe do pomieszczeń, przechowywane są w specjalnej szafie i mogą być wydawane w sytuacjach awaryjnych.

4. Każdorazowe pobranie kluczy zapasowych podlega wpisowi do rejestru, w rejestrze odnotowuje się datę, godzinę i nazwisko osoby zdającej lub pobierającej klucze oraz jej podpis.
5. W przypadku podejrzenia zagrożenia pracownik ochrony może posłużyć się kluczami, o których mowa w ust. 1, w celu usunięcia zagrożenia; przed opuszczeniem urzędu zobowiązany jest złożyć Administratorowi Bezpieczeństwa Informacji lub upoważnionej przez Starostę osobie pisemny raport na okoliczność użycia kluczy.

§ 4.

1. Kartoteki należy przechowywać w przeznaczonych do tego szafach, do których dostęp mają wyłącznie użytkownicy.
2. Użytkownicy, o których mowa w ust. 1, odpowiedzialni są za rzetelne prowadzenie kartotek, ich kompletność oraz ochronę.

Rozdział VIII

Udostępnianie posiadanych w zbiorze danych osobowych.

---

§ 1.

1. Na wniosek osoby, której dane dotyczą, ADO jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach, a zwłaszcza wskazać w formie zrozumiałej odnośnie danych osobowych jej dotyczących:
    a. jakie dane osobowe zawiera zbiór,
    b. w jaki sposób zebrano dane,
    c. w jakim celu i zakresie dane są przetwarzane,
    d. w jakim zakresie oraz komu dane zostały udostępnione.
2. Na wniosek osoby, której dane dotyczą, informacji, o których mowa w ust. 1, udziela się na piśmie.

§ 2.

1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:

a. uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy,
b. uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze,
c. uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych,
d. uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące,
e. uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,
f. żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane
g. prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, jeżeli nawet przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą,
h. wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych
i. wniesienia do administratora danych żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej z naruszeniem zakazu ostatecznego rozstrzygnięcia indywidualnej sprawy, gdy treść była wyłącznie wynikiem operacji na danych osobowych prowadzonych w systemie informatycznym.

2. Osoba zainteresowana może skorzystać z prawa do informacji, o których mowa w ust. 1 pkt 1 - 5, nie częściej niż raz na 6 miesięcy.

§ 3.

1. W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy.
2. Każda z osób zatrudnionych przy przetwarzaniu danych w razie powzięcia takiej wiadomości ma obowiązek o wystąpieniu osoby, której dane dotyczą, poinformować ABI.

§ 4.

1. Do udostępniania posiadanych w zbiorze danych osobowych upoważniony jest kierownik jednostki lub pracownik posiadający wymagane prawem upoważnienie.
2. W przypadku udostępniania danych osobowych w celach innych niż wyłączenie do zbioru, administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

§ 5.

Powierzenie przetwarzania danych osobowych innemu podmiotowi może nastąpić wyłącznie w drodze umowy zawartej w formie pisemnej przez ADO.Z uwzględnieniem wymagań określonych w art.31ust.1 tejże ustawy.

Rozdział IX

Kontrola przestrzegania zasad zabezpieczenia danych osobowych.

---

§ 1.

1. Administrator Bezpieczeństwa Informacji sprawuje nadzór nad przestrzeganiem zasad ochrony przetwarzanych danych osobowych.
2. W przypadku nieobecności Administratora Bezpieczeństwa Informacji, osobę zastępującą wyznacza Starosta.
3. Administrator Bezpieczeństwa Informacji lub osoba przez mego upoważniona dokonuje okresowych kontroli i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad postępowania w przypadku naruszenia ochrony danych osobowych zgodnie z wcześniej opracowanym planem sprawdzeń.
4. Plan sprawdzeń jest przygotowywany przez administratora bezpieczeństwa informacji na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan sprawdzeń jest przedstawiany administratorowi danych nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem. Plan sprawdzeń obejmuje co najmniej jedno sprawdzenie.
5. Przedmiotem kontroli, o których mowa w ust. 3 powinno być w szczególności:
6. funkcjonowanie zabezpieczeń systemowych,
    a. prawidłowość funkcjonowania mechanizmów kontroli dostępu do zbioru danych,
    b. funkcjonowanie zastosowanych zabezpieczeń fizycznych,
    c. zasady przechowywania kartotek,
    d. zasady i sposoby likwidacji oraz archiwizowania zbiorów archiwalnych,
    e. realizacja procedur wdrożonych przez Administratora Danych w zakresie ochrony danych osobowych.

7. Administrator Bezpieczeństwa Informacji prowadzi rejestr dokonywanych kontroli oraz ustaleń, wniosków i zaleceń z nich wynikających, a także nadzoruje ich wykonywanie.
8. Z kontroli, o których mowa w ust. 3 należy sporządzać sprawozdania, które przechowuje Administrator Bezpieczeństwa Informacji.

Rozdział X

Zachowanie bezpieczeństwa przez użytkowników systemu.

---

§ 1.

1. Użytkownicy systemu zobowiązani są stosować odpowiednie środki bezpieczeństwa w pomieszczeniach, w których zainstalowano sprzęt systemu informatycznego by nie spowodować jego uszkodzenia.
2. Wszyscy użytkownicy systemu muszą stosować się do obowiązujących procedur bezpieczeństwa.
3. Hasło podlega szczególnej ochronie. Użytkownik ma obowiązek tworzenia haseł.
4. W przypadku, gdy użytkownik zapomni swoje hasło, może on odnowić hasło w porozumieniu z Administratorem Systemu Informatycznego.

Rozdział XI

Zachowanie bezpieczeństwa przez użytkowników systemu.

---

§ 1.

Dane osobowe, które są przedmiotem przetwarzania zgodnie z przepisami ustawy o ochronie danych osobowych, gromadzone i przechowywane są w serwerach i w postaci tradycyjnej .

Środki bezpieczeństwa fizycznego są konieczne dla zapobiegania niepowołanemu dostępowi do informacji, nieautoryzowanym operacjom w systemie, kontroli dostępu do zasobów oraz w celu zabezpieczenia sprzętu teleinformatycznego.

§ 2.

Obszar systemów informatycznych w Starostwie Powiatowym w Turku, obejmuje wszystkie pomieszczenia w następujących budynkach:

1. Budynek główny Starostwa przy ul. Kaliskiej 59, 62-700 Turek;
2. Budynki wydziałów Geodezji i Komunikacji przy ul. Łąkowej 4a, 62-700 Turek;

§ 3.

Pomieszczenia, w których znajdują się systemy informacji winny być:

1. wyposażone w szafy, meble biurowe zamykane na klucz umożliwiające przechowywanie dokumentów,
2. zamknięte, jeśli nikt w nich nie przebywa.

§ 4.

Instalacja urządzeń systemu i sieci teleinformatycznej odbywa się za wiedzą i pod kontrolą kierownika komórki organizacyjnej, który jest również odpowiedzialny za warunki wprowadzania do użycia, przechowywania, eksploatacji oraz wycofywania z użycia każdego urządzenia.

Rozdział XII

Bezpieczeństwo sprzętu i oprogramowania.

---

§ 1.

1. Sprzęt i oprogramowanie, indywidualnie lub łącznie mają ścisły związek z bezpieczeństwem systemu i sieci teleinformatycznej. Dlatego, powinny być ściśle przestrzegane procedury bezpieczeństwa odnoszące się do tych elementów.
2. Sieć teleinformatyczna jest organizacyjnym i technicznym połączeniem systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami telekomunikacyjnymi. Niedopuszczalne jest samowolne przemieszczanie lub zmiana konfiguracji stacji roboczej bez wiedzy kierownika komórki organizacyjnej.
3. Zabrania się na korzystanie z jakiegokolwiek nowego oprogramowania bez zgody Administratora Systemu Informatycznego.
4. Dostęp do zbiorów danych osobowych znajdujących się na serwerach następuje po wprowadzeniu hasła, które znane jest tylko osobie przetwarzającej dane.
5. Każdorazowo po dokonaniu przetworzenia aplikacja powinna być zamknięta.
6. W przypadku podejrzenia, iż wiadomości o sposobie dostępu do elektronicznej bazy danych uzyskała osoba do tego niepowołana, osoba przetwarzająca dane w porozumieniu z ASI powinna dokonać zmiany hasła.
7. Elektroniczne bazy danych osobowych są archiwizowane.
8. Używanie oprogramowania prywatnego w sieci jest zabronione. Na stacjach roboczych powinno być zainstalowane jedynie niezbędne oprogramowanie.

Rozdział XIII

Polityka antywirusowa.

---

§ 1.

1. Wszystkie serwery i komputery są sprawdzane przy użyciu oprogramowania do wykrywania i usuwania wirusów komputerowych.

2. W zakresie ochrony antywirusowej wprowadza się następujące zalecenia:
    a. nie należy używać oprogramowania na stacji roboczej innego niż zaleca Administrator Systemu Informatycznego;
    b. przed użyciem nośnika danych sprawdzić czy nie jest zainfekowany wirusem komputerowym.
3. W przypadku jakichkolwiek wątpliwości odnośnie zagrożenia wirusowego należy sprawdzić zawartość całego dysku twardego programem antywirusowym. W przypadku dalszych niejasności należy kontaktować się z administratorem sieci lokalnej.

Rozdział XIV

Konserwacje i naprawy.

---

§ 1.

1. Każde urządzenie użytkowane w systemie informatycznym, powinno podlegać rutynowym czynnościom konserwacyjnym oraz przeglądom wykonywanym przez uprawnione osoby.
2. Za konserwację oprogramowania systemowego oraz aplikacyjnego serwera systemu informatycznego odpowiedzialny jest Administrator Systemu Informatycznego. Konserwacja oprogramowania obejmuje także jego aktualizację.
3. Za konserwację oprogramowania stanowisk roboczych odpowiedzialny jest kierownik komórki organizacyjnej. Wszelkie aktualizacje oprogramowania powinny być uzgadniane z Administratorem Systemu Informatycznego.
4. Administrator Systemu Informatycznego przed rozpoczęciem naprawy urządzenia przez zewnętrzne firmy sprawdza, czy spełnione są następujące wymagania:
    a. w przypadku awarii serwera i konieczności oddania sprzętu do serwisu, nośniki magnetyczne zawierające dane osobowe powinny być wymontowane i do czasu naprawy serwera przechowywane w pomieszczeniu biurowym znajdującym się w strefie o ograniczonym dostępie;
    b. w przypadku uszkodzenia nośnika magnetycznego zawierającego dane osobowe należy komisyjnie dokonać jego zniszczenia.

Rozdział XV

Plany awaryjne i zapobiegawcze.

§ 1.

Serwer systemu oraz poszczególne stacje robocze (opcjonalnie) powinny być zabezpieczone urządzeniami podtrzymującymi zasilanie (UPS), co umożliwi funkcjonowanie systemu w przypadku awarii zasilania.

§ 2.

W celu zabezpieczenia ciągłości pracy, informacja przechowywana i przetwarzana w systemie podlega codziennej, przyrostowej archiwizacji (opcjonalnie) oraz pełnej archiwizacji przeprowadzanej nie rzadziej niż raz na dwa tygodnie. Kopie archiwalne danych przechowywane są przez Administratora Systemu Informatycznego. Użycie kopii zapasowych następuje na polecenie Administratora Systemu Informatycznego w przypadku odtwarzania systemu po awarii.

Rozdział XVI

Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych.

§ 1.

1. Przed przystąpieniem do pracy użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz oględzin swojego stanowiska pracy, ze zwróceniem

szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.

2. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Administratora Bezpieczeństwa Informacji.
3. Obowiązek określony w ust. 2 ciąży również na pozostałych pracownikach Administratora Danych.
4. Postanowienia ust. 2 i 3 mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych gromadzonych w systemie informatycznym, jak i w kartotekach.

§ 2.

1. Do czasu przybycia Administratora Bezpieczeństwa Informacji lub upoważnionej przez Starostę osoby, zgłaszający:
    a. powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,
    b. zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym,
    c. podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
2. Postanowienia ust. 1 mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych.

§ 3.

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, Administrator Bezpieczeństwa Informacji lub osoba upoważniona przez Starostę, po przybyciu na miejsce:

1. ocenia zastałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe oraz stan urządzeń, a także identyfikuje wielkość negatywnych następstw incydentu,
2. wysłuchuje relacji osoby, która dokonała powiadomienia,
3. podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych. W uzasadnionych przypadkach niezwłocznie powiadamia Starostę.

§ 4.

1. Administrator Bezpieczeństwa Informacji lub upoważniona przez Starostę osoba sporządza z przebiegu zdarzenia raport, w którym powinny się znaleźć w szczególności informacje o:
    a. dacie i godzinie powiadomienia,
    b. godzinie pojawienia się w pomieszczeniach, w których przetwarzane są dane,
    c. sytuacji, jaką zastał,
    d. podjętych działaniach i ich uzasadnieniu.
2. Kopia raportu przekazywana jest bezzwłocznie Staroście, a w przypadku, gdy raport sporządzony został przez osobę upoważnioną przez Starostę, także Administratorowi Bezpieczeństwa Informacji.

§ 5.

1. Administrator Bezpieczeństwa Informacji podejmuje kroki zmierzające do likwidacji naruszeń zabezpieczeń danych osobowych i zapobieżenia wystąpieniu ich w przyszłości. W tym celu:
    a. w miarę możliwości przywraca stan zgodny z zasadami zabezpieczenia systemu,
    b. relacjonuje Staroście przedsięwzięte czynności,
    c. jeśli taka potrzeba zachodzi, postuluje wprowadzenie nowych form zabezpieczenia, a w razie ich wprowadzenia nadzoruje zaznajamianie z nimi osób dopuszczonych do przetwarzania danych osobowych.
2. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej u Administratora Danych dyscypliny pracy, Administrator Bezpieczeństwa

Informacji lub upoważniona przez Starostę osoba wnioskuje do Starosty o wyjaśnienie wszystkich okoliczności incydentu i o podjęcie stosownych działań wobec sprawcy/sprawców.

3. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od Administratora Bezpieczeństwa Informacji lub osoby przez niego upoważnionej.

§ 6.

1. W przypadku zaginięcia komputera lub nośników magnetycznych, na których były zgromadzone dane osobowe, użytkownik posługujący się komputerem niezwłocznie powiadamia Administratora Bezpieczeństwa Informacji, a w przypadku kradzieży występuje o powiadomienie jednostki policji .
2. W sytuacji, o której mowa w ust. 1 Administrator Bezpieczeństwa Informacji lub upoważniona przez Starostę osoba podejmuje niezbędne kroki do wyjaśnienia okoliczności zdarzenia, sporządza protokół z zajścia, który powinna podpisać także osoba, której skradziono lub, której zaginął sprzęt oraz powiadamia Starostę.
3. W przypadku kradzieży komputera razem z nośnikiem magnetycznym Administrator Bezpieczeństwa Informacji lub upoważniona przez Starostę osoba podejmuje działania zmierzające do odzyskania utraconych danych oraz nadzoruje proces przebiegu wyjaśnienia sprawy.

§ 7.

Osoba dopuszczona do przetwarzania danych osobowych za naruszenie obowiązków wynikających z niniejszej Polityki ponosi odpowiedzialność przewidzianą w przepisach aktów wewnętrznych Administratora Danych oraz na podstawie innych, odrębnych przepisów prawa.

Rozdział XVII

Postępowanie w wypadku klęski żywiołowej.

§ 1.

Klęską żywiołową jest katastrofa, spowodowana działaniem sił przyrody np. takich jak ogień, huragan, woda lub ich przejawami.

§ 2.

W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń, w których przetwarzane są dane osobowe, mają zastosowanie przepisy niniejszego rozdziału oraz innych przepisów szczególnych.

§ 3.

1. O zagrożeniu, jego skali i podjętych krokach zaradczych pracownik ochrony lub osoba kierująca ewakuacją zobowiązani są niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji w każdy możliwy sposób. W razie niemożności skontaktowania się z nim pracownik ochrony zawiadamia, co najmniej jedną z niżej wymienionych osób:
    a. osobę wyznaczoną przez Starostę,
    b. Starostę.
2. Numery telefonów Administratora Bezpieczeństwa Informacji i osób, z którymi należy się kontaktować na wypadek klęski żywiołowej powinny być znane pracownikom.

§ 4.

Osoby biorące udział w akcji ratunkowej, mają prawo wejść do pomieszczeń, w których przetwarzane są dane osobowe.

§ 5.

W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy, przebywający w pomieszczeniach, w których przetwarzane są dane osobowe, obowiązani są do przerwania pracy i w miarę możliwości przed opuszczeniem tych pomieszczeń do:

1. zamknięcia systemu informatycznego,
2. zabezpieczenia danych osobowych gromadzonych w kartotekach.

§ 6.

1. W czasie trwania akcji ratunkowej i po jej zakończeniu Administrator Bezpieczeństwa Informacji oraz obecni użytkownicy powinni, w miarę możliwości, zabezpieczać dane osobowe przed nieuprawnionym do nich dostępem.
2. Obowiązek ten ciąży w równym stopniu na innych pracownikach Administratora Danych, obecnych przy akcji ratunkowej.

Rozdział XVIII

Przepisy końcowe.

---

§ 1.

Naruszenie obowiązków wynikających z niniejszej Polityki Bezpieczeństwa oraz przepisów ustawy o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym w szczególności wynikającym z przepisów tejże ustawy.

Art.49.

1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których nie jest uprawniony , podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2;
2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

Art. 51.

1. Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 52.

Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 53.

Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 54.

Kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 52.

Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 53.

Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 54.

Kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

§ 2.

Polityka jest dokumentem wewnętrznym i me może być udostępniania osobom postronnym w żadnej formie.

§ 3.

1. Kierownicy komórek organizacyjnych są obowiązani zapoznać z treścią Polityki każdego użytkownika .
2. Użytkownik zobowiązany jest złożyć oświadczenie , o tym, iż został zaznajomiony z przepisami ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych oraz dokumentacją obowiązującą u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania.

§ 4.

W sprawach nie uregulowanych w niniejszej Polityce bezpieczeństwa informacji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182, z późn. zm.) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i

organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).