Załącznik Nr 1
do Zarządzenia Nr 35/2017
Starosty Mławskiego
z dnia 08.08.2017 r.

ABI. 142.1.2017

POLITYKA BEZPIECZEŃSTWA

STAROSTWA POWIATOWEGO

W MŁAWIE

Integralną częścią Polityki Bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Mławie są następujące załączniki:

Załącznik nr 1 do Polityki bezpieczeństwa pn.: „Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe"

Załącznik nr 2 do Polityki bezpieczeństwa pn.: „Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych"

Załącznik nr 3 do Polityki bezpieczeństwa pn.: „Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych"

Załącznik nr 4 do Polityki bezpieczeństwa pn.: „Opis powiązań między polami informacyjnymi zbiorów danych osobowych"

1.Definicje

1.1.Zbiór danych osobowych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
1.2.Administrator danych osobowych (ADO) - zadania Administratora Danych Osobowych wykonuje Starosta Mławski. ADO oraz osoby podpisujące w jego imieniu upoważnienia do przetwarzania danych osobowych tzn. Wicestarosta, Sekretarz Powiatu oraz Administrator Bezpieczeństwa Informacji nie potrzebują upoważnień do przetwarzania danych osobowych. Upoważnienia nie potrzebuje również osoba czasowo zastępująca Sekretarza Powiatu, lecz tylko w okresie tego zastępstwa (nieobecności Sekretarza Powiatu)
1.3.Administrator Bezpieczeństwa Informacji (ABI) - osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za bezpieczeństwo danych osobowych w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
1.4.Administrator Systemu Informatycznego (ASI) – osoba lub osoby odpowiedzialne za bezpieczeństwo danych osobowych w systemie informatycznym w tym: komputery, serwery i oprogramowanie a także odpowiedzialna za ich sprawność, konserwację oraz wdrażanie i realizację Instrukcji Zarządzania Systemem Informatycznym w Starostwie Powiatowym w Mławie.
1.5.System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
1.6.Stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.
1.7.Bezpieczeństwo systemu informatycznego - wdrożenie przez Administratora Danych Osobowych lub osobę przez niego uprawnioną (ABI, ASI) środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.
1.8.Przetwarzanie danych osobowych - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, archiwizowanie, opracowywanie, zmienianie, usuwanie, odczytywanie, udostępnianie, a także dostęp do nich.
1.9.Osoba upoważniona - osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych (lub osobę uprawnioną przez niego) i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu.

1.10.Użytkownik systemu - osoba posiadająca uprawnienia do przetwarzania danych osobowych w systemie informatycznym.
1.11.Osoba uprawniona - osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych do wykonywania w jego imieniu określonych czynności.
1.12.Ustawa – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
1.13.Rozporządzenie w sprawie dokumentacji - 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.
1.14.Rozporzadzenie w sprawie KRI - Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformacyjnych

2.Sposób przepływu danych pomiędzy poszczególnymi systemami

2.1.Istnieje przepływ danych w zbiorach obsługiwanych przez system elektroniczny: „Płace" i „Płatnik" poprzez eksport i import plików xml.
2.2.Istnieje przepływ danych systemie geodezyjnym między programami EWMAPA, EWOPIS, OŚRODEK I BANK OSNÓW poprzez korzystanie ze wspólnej bazy danych.

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

3.1.Środki ochrony fizycznej
3.1.1.Budynki urzędu, w których zlokalizowany jest obszar przetwarzania danych osobowych otwierane są przed rozpoczęciem pracy urzędu oraz zamykane po zakończeniu pracy przez upoważnionych pracowników. Osoby te odpowiedzialne są za klucze oraz za przekazywanie kluczy od poszczególnych pokoi właściwym pracownikom. Przy otwieraniu i zamykaniu budynku wyłączany i włączany jest alarm elektroniczny. Klucze do obszarów bezpiecznych posiadają Administratorzy Systemu Informatycznego, osoby upoważnione do pobierania kluczy lub dyrektorzy wydziałów w których znajdują się te obszary. Tylko pod ich nadzorem odbywają się wejścia do tych obszarów osób nieuprawnionych. Wejścia te odnotowane są w dzienniku wejść i wyjść prowadzonych przez ASI.
3.1.2.Budynki opisane w pkt. 3.1.1 zlokalizowane są w trzech miejscach pod następującymi adresami:

a)Mława, ul. Reymonta 6
Budynek przed rozpoczęciem pracy otwierany jest przez upoważnionego pracownika. Wyłącza on następnie system alarmowy. Pracownicy przychodzący do pracy pobierają klucze od pokoi od upoważnionego pracownika w pomieszczeniu pracownika zatrudnionego przy obsłudze i pracach porządkowych i konserwatorskich w piwnicy budynku. Po zakończeniu pracy pracownicy zamykają pomieszczenia, a klucze od pomieszczeń przekazują osobiście osobie zatrudnionej przy sprzątaniu. Osoba sprzątająca po zakończeniu pracy zamyka wszystkie pomieszczenia, a klucze składa w pomieszczeniu pracownika zatrudnionego przy obsłudze i pracach porządkowych i konserwatorskich. Osoba zatrudniona przy sprzątaniu zabiera klucz od tego pomieszczenia ze sobą, zamyka budynek i włącza system alarmowy. W obszarach bezpiecznych takich jak np. serwerownie, osoba ta sprząta tylko i wyłącznie pod nadzorem Administratora Systemu informatycznego lub upoważnionego do pobierania kluczy pracownika.

b)Mława, ul. Wyspiańskiego 9
Budynek przed rozpoczęciem pracy otwierany jest przez upoważnionego pracownika. Wyłącza on następnie system alarmowy i otwiera pomieszczenie Dyrektora Wydziału. Przychodzący do pracy pracownicy pobierają klucze od pokoi od upoważnionego pracownika lub od Dyrektora Wydziału w pomieszczeniu Dyrektora Wydziału w obecności tego pracownika lub Dyrektora Wydziału. Po zakończeniu pracy pracownicy zamykają pomieszczenia, a klucze od pomieszczeń przekazują osobiście osobie zatrudnionej przy sprzątaniu. Osoba sprzątająca po zakończeniu pracy zamyka wszystkie pomieszczenia, a klucze składa w pomieszczeniu Dyrektora Wydziału. Klucz od tego pomieszczenia zabiera ze sobą, zamyka budynek i włącza system alarmowy. W obszarach bezpiecznych takich jak np. serwerownie, osoba sprzątająca dokonuje prac porządkowych tylko i wyłącznie pod nadzorem Administratora Systemu informatycznego, dyrektora wydziału lub upoważnionego do pobierania kluczy pracownika.

c)Mława, ul. Stary Rynek 10
Budynek przed rozpoczęciem pracy otwierany jest przez upoważnionego pracownika. Wyłącza on następnie system alarmowy i otwiera pomieszczenie Dyrektora Wydziału. Przychodzący do pracy pracownicy pobierają klucze od pokoi od upoważnionego pracownika lub od Dyrektora Wydziału w pomieszczeniu Dyrektora Wydziału w obecności tego pracownika lub Dyrektora Wydziału. Po zakończeniu pracy pracownicy zamykają pomieszczenia, a klucze od pomieszczeń przekazują osobiście osobie zatrudnionej przy sprzątaniu. Osoba sprzątająca po zakończeniu pracy zamyka wszystkie pomieszczenia, a klucze składa w pomieszczeniu Dyrektora Wydziału. Klucz od tego pomieszczenia zabiera ze sobą, zamyka budynek i włącza system alarmowy. W obszarach bezpiecznych takich jak np. serwerownie, osoba sprzątająca dokonuje prac porządkowych tylko i wyłącznie pod nadzorem Administratora Systemu informatycznego, dyrektora wydziału lub upoważnionego do pobierania kluczy pracownika.

3.1.3.Urządzenia służące do przetwarzania danych osobowych oraz zbiory danych osobowych znajdują się w pomieszczeniach, które zabezpieczone są zamkami.
3.1.4.Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu lub w obecności zwierzchnika służbowego takiej osoby.
3.1.5.Po godzinach pracy dopuszcza się przebywanie w pomieszczeniach, w których przetwarzane i przechowywane są zbiory danych osobowych jedynie osobom zatrudnionych przy sprzątaniu i konserwacji, upoważnionych do przebywania w tych pomieszczeniach lub dyrektora wydziału albo upoważnionego do pobierania kluczy pracownika. Po wypełnieniu w/w czynności pomieszczenia zamykane są na klucz.
3.1.6.Pomieszczenia w których zbiory danych osobowych, z jakiś powodów nie są zabezpieczone w zamykanych szafach, biurkach i innych sprzętach biurowych, mogą być sprzątane tylko w obecności upoważnionego pracownika w godzinach obowiązującego czasu pracy. Po zakończeniu pracy i zamknięciu pomieszczenia, klucz od tego pokoju zabierany jest przez pracownika zatrudnionego przy przetwarzaniu danych osobowych.
3.1.7.W Starostwie wydzielono obszary bezpieczne, w których dozwolone jest przebywanie, tylko i wyłącznie dyrektorom wydziałów i Administratorom Systemu Informacyjnego (ASI). Tymi obszarami są:
a)pomieszczenie serwerowni znajdujące sie pod adresem: Mława, ul.Reymonta 6
b)pomieszczenie serwerowni znajdujące sie pod adresem: Mława, ul.Wyspiańskiego 9
c)pomieszczenie serwerowni znajdujące sie pod adresem: Mława, ul.Stary Rynek 10
3.1.8.W czasie sprzątania pomieszczeń po obowiązujących godzinach pracy wejście do budynku jest zamknięte. Zabronione jest wpuszczanie i przebywanie w budynku jakiejkolwiek nieupoważnionej osoby. Przebywanie osób nieupoważnionych zarówno przed jak i po godzinach

obowiązującego czasu pracy dozwolone jest wyłącznie za zgodą Administratora Danych Osobowych (ADO) pod nadzorem osób wymienionych w pkt. 3.1.5.
3.1.9.Po zakończeniu pracy zbiory danych osobowych będące w formie papierowej powinny być zamknięte na klucz (szafy, biurka), a następnie całe pomieszczenie powinno być w ten sam sposób zamknięte, a klucz od pomieszczenia oddany osobie wymienionej w pkt. 3.1.5.
3.1.10.Po skończeniu pracy klucze od szaf i biurek w których znajdują się zbiory danych osobowych, po ich zamknięciu powinny być zbierane w jedno miejsce np. jedna z szaf lub biurko. Klucz od tej szafy powinien być zabrany przez pracownika zajmującego się przetwarzaniem tych zbiorów. W przypadku braku takich zabezpieczeń pracownik wychodzący ostatni zamyka całe pomieszczenie na klucz i zabiera go ze sobą (patrz pkt. 3.1.1). Kopie kluczy od pomieszczeń, szaf i biurek powinny być przechowywane u Dyrektora Wydziału.
3.1.11.Przy rozpoczynaniu pracy klucze od pomieszczeń pobierane są od osoby odpowiedzialnej za otwarcie budynków, która wymieniona jest w punkcie 3.1.1.
3.1.12.Pomieszczenia, o których mowa w punkcie 3.1.4, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.
3.1.13.W przypadku przebywania osób postronnych w pomieszczeniach, o których mowa wyżej, monitory stanowisk dostępu do danych osobowych oraz wszelkie dokumenty papierowe powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
3.1.14.Do przebywania w obszarach bezpiecznych wymienionych w pkt 3.1.7 uprawnieni są: Administratorzy Systemu Informatycznego, Administrator Bezpieczeństwa Informacji oraz Administrator Danych Osobowych, osoby uprawnione wymienione w pkt 1.2 lub osoby specjalnie upoważnione do tego celu przez ADO.
3.1.15.Przebywanie w obszarze bezpiecznym osób nieuprawnionych (konserwator, elektryk, sprzątaczka i inni) dopuszczalne jest tylko w obecności Administratora Systemu Informatycznego, a w przypadku ich nieobecności – w obecności upoważnionej przez ADO. Każde wejście osób nieuprawnionych, powinno być udokumentowane w dzienniku wejść do obszaru bezpiecznego.
3.1.16.Każdy dokument papierowy na którym znajdują się dane osobowe przeznaczony do wyrzucenia powinien być uprzednio zniszczony w sposób uniemożliwiający jego odczytanie.
3.1.17.Każdy dokument papierowy lub elektroniczny przeznaczony do publikacji w Biuletynie Informacji Publicznej powinien być poddany anonimizacji.
3.1.18.Za nieprzestrzeganie realizacji środków ochrony fizycznej w Wydziałach Starostwa odpowiada Dyrektor podległego mu Wydziału
3.1.19.Za naruszenie obowiązku zabezpieczenia danych przed zabraniem przez osobę nieprawioną, uszkodzeniem lub zniszczeniem na stanowisku pracy oraz za udostępnianie lub umożliwienie dostępu osobom nieupoważnionym odpowiada pracownik przetwarzający te dane.

3.2.Środki sprzętowe, informatyczne i telekomunikacyjne.

3.2.1.Urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej centralnym UPS-em.
3.2.2.Zastosowano odrębne urządzenie pamięci masowej zabezpieczonej hasłem w zamykanym pomieszczeniu, w celu archiwizacji danych z serwerów.
3.2.3.Na wszystkich serwerach oraz stacjach roboczych zainstalowano oprogramowanie antywirusowe. Poczta elektroniczna wpływająca do Urzędu skanowana jest programem antywirusowym przed przesłaniem jej do Użytkownika.
3.2.4.Komputery zabezpieczone są hasłami, które znane są tylko użytkownikowi danego komputera.

3.2.5.Zawartość przenośnych nośników informacji zabezpieczona jest przez programy szyfrujące

3.3.Środki ochrony w ramach oprogramowania systemu.

3.3.1.Dostęp fizyczny do baz danych osobowych zastrzeżony jest wyłącznie dla osób zajmujących się obsługą informatyczną Urzędu.
3.3.2.Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych w tym w zbiorach doraźnych, jedynie za pośrednictwem aplikacji.
3.3.3.System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu.
3.3.4.W sieciowym systemie operacyjnym zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do systemu.

3.4.Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych.

3.4.1.Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji.
3.4.2.Dla każdego Użytkownika systemu jest ustalony odrębny identyfikator.
3.4.3.Zdefiniowano Użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (unikalny identyfikator i hasło).

3.5.Środki ochrony w ramach systemu Użytkowego.

3.5.1.Zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności Użytkownika.
3.5.2.Komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem.

3.6.Środki organizacyjne.

3.6.1.Powołano Administratora Bezpieczeństwa Informacji (ABI), jako osobę odpowiedzialną za bezpieczeństwo informacji, a w szczególności za bezpieczeństwo danych osobowych w Starostwie Powiatowym w Mławie.
3.6.2.Wyznaczono Administratorów/Administratora Systemu Informatycznego (ASI), którzy odpowiedzialni są za bezpieczeństwo przetwarzanych i przechowywanych danych osobowych w systemie i w procedurach informatycznych oraz na urządzeniach informatycznych i nośnikach elektronicznych.
3.6.3.Użytkownicy odpowiedzialni są za bezpieczeństwo przetwarzanych i przechowywanych danych osobowych na używanych przez nich nośnikach informacji zarówno elektronicznych jak i papierowych.
3.6.4.ASI odpowiadają w szczególności za wdrożenie i realizację „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Mławie" oraz za zabezpieczenie komputerów, serwerów i oprogramowania, a także sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych. Prowadzą ewidencję urządzeń i nośników elektronicznych. Administrator Systemu Informatycznego przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie informacji inspektora ds. kadr określającej czas trwania i zakres uprawnień pracownika do przetwarzania określonych zbiorów danych osobowych.
3.6.5.Prowadzona jest ocena ryzyka utraty bezpieczeństwa danych osobowych w ramach Kontroli Zarządczej w dokumencie pn. „Rejestr ryzyk"

3.6.6.Osoby przyjmowane do pracy lub wobec których zmieniono zakres wykonywanej pracy w ten sposób, że powinny być upoważnione do przetwarzania danych osobowych są kierowane przez inspektora ds. kadr do przeszkolenia przez ABI zanim dopuszczone będą do pracy z tymi zbiorami danych.
3.6.7.Szkolenie wymienionych w pkt. 3.6.6 osób obejmuje zakres podstawowych przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym. Bez względu na szkolenie wszyscy pracownicy Starostwa zobowiązani są znać oraz zobowiązani są przestrzegać przepisy w zakresie ochrony danych osobowych a w szczególności ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych z późniejszymi zmianami, a także procedury przetwarzania danych obowiązujące w Starostwie Powiatowym w Mławie. Ponadto. zobowiązani są zachować tajemnicę służbową oraz poufność informacji zarówno w trakcie wykonywania obowiązków służbowych jak również po zakończeniu pracy na tym stanowisku lub w Starostwie Powiatowym w Mławie.
3.6.8.Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
3.6.9.Wprowadzono instrukcję zarządzania systemem informatycznym.
3.6.10.Wprowadzono instrukcję postępowania w sytuacji naruszenia systemu ochrony danych osobowych
3.6.11.Określono sposób postępowania z nośnikami informacji.
3.6.12.Wydawane lub akceptowane są upoważnienia dostępu do danych osobowych dla osób z zewnątrz przeprowadzających kontrolę lub audyt.
3.6.13.Administrator Bezpieczeństwa Informacji przeprowadza co najmniej raz na rok sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych i sporządza dla Administratora Danych sprawozdanie zgodnie z art. 36a i 36b ustawy o ochronie danych osobowych.
3.6.14.W przypadku powierzenia przetwarzania danych innym podmiotom stosuje się odpowiednie umowy powierzenia.
3.6.15. Kontrola nad tym jakie dane osobowe, kiedy i przez kogo zostały do zbiorów wprowadzone i komu są przekazywane realizowana jest przez odnotowanie tego faktu w książce korespondencji przychodzącej i wychodzącej. Wnioski/żądania udostępnienia kopii dokumentów lub wglądu w akta sprawy mają formę pisemną.

4. Instrukcja w sprawie zarządzania oprogramowaniem

4.1.Oprogramowanie używane w systemie informatycznym musi posiadać aktualną licencję
4.2.Oprogramowanie nie posiadające licencji powinno być zgłoszone przez użytkownika i natychmiast usunięte przez Administratorów Systemu Informatycznego
4.3.Komputery powinny być zabezpieczone przed możliwością wgrywania nie licencjonowanego oprogramowania na ile pozwala na to środowisko informatyczne komputera, w którym pracuje użytkownik.
4.4.Odpowiedzialność za posiadanie zainstalowanych nie licencjonowanych programów ponosi użytkownik.
4.5.Administratorzy Systemu Informatycznego sporządzają i aktualizują listę oprogramowania wraz z lokalizacją użytkowania tego oprogramowania oraz sporządzają opis powiązań między polami informacyjnymi o ile dotyczą danych osobowych. Opis tych powiązań stanowi załącznik do Polityki bezpieczeństwa Nr 4.
4.6.Administratorzy Systemu Informatycznego przechowują elektroniczne nośniki oprogramowania, które używane jest w systemie informatycznym.
4.7.Każdy licencja oprogramowania ewidencjonowana jest w programie OCS Inventory

4.8.Elektroniczne nośniki, na których zapisane jest oprogramowanie powinno być przechowywane w zamykanych szafkach w pomieszczeniu ASI.
4.9.Kopie oprogramowania o ile pozwalają na to przepisy licencyjne mogą być wykonane tylko przez Administratorów Systemu Informatycznego.
4.10.Administratorzy Systemu Informatycznego co najmniej raz w roku przeprowadzają kontrolę oprogramowania u użytkowników. Lista oprogramowania wymieniona w pkt 4.5 aktualizowana jest na bieżąco.
4.11.Za wdrożenie i aktualizację niniejszej instrukcji odpowiadają Administratorzy Systemu Informatycznego

5.Opis zdarzeń naruszających ochronę danych osobowych

5.1.Podział zagrożeń:
5.1.1.Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) – ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu – ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
5.1.2.Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania) – może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
5.1.3.Zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia naruszenia poufności danych. Zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy.

Zagrożenia te możemy podzielić na:
a) nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
b) nieuprawniony dostęp do systemu z jego wnętrza,
c) nieuprawniony przekaz danych,
d) pogorszenie jakości sprzętu i oprogramowania,
e) bezpośrednie zagrożenie materialnych składników systemu.

5.2.Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe, to głównie:
5.2.1.Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, kradzież, niepożądana ingerencja ekipy remontowej i inne.;
5.2.2.Niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;
5.2.3.Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż;
5.2.4.Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
5.2.5.Pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
5.2.6.Naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;

5.2.7.Stwierdzona próba modyfikacji lub modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
5.2.8.Niedopuszczalna manipulacja danymi osobowymi w systemie;
5.2.9.Ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedury ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń;
5.2.10.Nieprzypadkowe odstępstwa od zasad bezpieczeństwa pracy w systemie lub sieci komputerowej wskazujące na przełamanie lub zaniechanie ochrony danych osobowych np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu itp.;
5.2.11.Istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki" itp.;
5.2.12.Podmiana lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia, jak również skasowanie lub skopiowanie w sposób niedozwolony danych osobowych;
5.2.13.Świadome, nie wynikające z zapomnienia, naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, itp.).

5.3.Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych na nośnikach tradycyjnych oraz elektronicznych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach, płyty CD, pamięci przenośnych w formie niezabezpieczonej itp.

5.4. Prowadzony jest rejestr incydentów.

6.Instrukcja postępowania w sytuacji naruszenia systemu ochrony danych osobowych

6.1.Użytkownik systemów komputerowych zobowiązany jest zawiadomić Administratora Systemu Informatycznego, o każdym naruszeniu zabezpieczenia systemu polegającym na:
6.1.1.Naruszeniu hasła dostępu,
6.1.2.Częściowym lub całkowitym braku bazy danych
6.1.3.Brak możliwości uruchomienia właściwej aplikacji (programu komputerowego),
6.1.4.Istotnej zmianie położenia komputerów
6.1.5.Kradzieży z pomieszczenia, w którym znajduje się sprzęt komputerowy.
6.1.6.Naruszenia zawartości zbioru danych osobowych,
6.1.7.Innych incydentów wskazujących na naruszenie zabezpieczenia systemu

6.2.Pracownik zatrudniony przy przetwarzaniu danych osobowych przechowywanych w formie papierowej zobowiązany jest zawiadomić Administratora Bezpieczeństwa Informacji o naruszeniu zbioru danych osobowych a w szczególności przy stwierdzeniu:
6.2.1.Częściowym lub całkowitym braku bazy danych
6.2.2.Kradzieży w pomieszczeniu w którym przechowywane były zbiory danych osobowych
6.2.3.Śladów prób włamania się do tego pomieszczenia
6.2.4.Częściowym lub całkowitym zniszczeniu zbioru na skutek przypadku losowego
6.2.5.Naruszenia zawartości zbioru danych osobowych,
6.2.6.Innych incydentów wskazujących na naruszenie zabezpieczenia bezpieczeństwa danych

6.3.Administrator Systemu Informatycznego, po otrzymaniu zawiadomienia o naruszeniu zabezpieczenia systemu informatycznego powinien niezwłocznie:

6.3.1.Powiadomić Administratora Danych i Administratora Bezpieczeństwa Informacji
6.3.2.Przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia i osoby odpowiedzialnej za naruszenie,
6.3.3.Podjąć działania zabezpieczające system przed ponownym naruszeniem,
6.3.4.Sporządzić protokół dokonanych czynności.

6.4.W przypadku kradzieży z pomieszczenia, w którym znajdują się komputery należy niezwłocznie poinformować o tym fakcie policję i przełożonych.

6.5.W razie niemożliwości zawiadomienia ABI lub osoby przez niego upoważnionej, należy powiadomić dyrektora wydziału.

6.6.Do czasu przybycia na miejsce naruszenia danych osobowych ABI, ASI lub upoważnionej osoby, należy:
6.6.1.Niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców naruszenia danych osobowych;
6.6.2.Udokumentować wstępnie zaistniałe naruszenie.
6.6.3.Nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI lub osoby przez niego upoważnionej.

6.7.Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, ABI, ASI lub osoba upoważniona:
6.7.1.Zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy organizacji;
6.7.2.Może żądać dokładnej relacji z zaistniałego naruszenia lub ujawnienia ochrony danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
6.7.3.Rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu lub ujawnieniu ochrony danych osobowych ADO.
6.7.4.Nawiązuje bezpośredni kontakt – jeżeli zachodzi taka potrzeba – ze specjalistami spoza organizacji.

6.8.Po wyczerpaniu niezbędnych środków doraźnych związanych z zaistniałym naruszeniem/ujawnieniem ochrony danych osobowych, ABI zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

6.9.ABI dokumentuje zaistniały przypadek naruszenia lub ujawnienia ochrony danych osobowych oraz sporządza raport, który powinien zawierać w szczególności:
6.9.1.Wskazanie osoby powiadamiającej oraz innych osób zaangażowanych lub odpytywanych w związku z naruszeniem lub ujawnieniem ochrony danych osobowych;
6.9.2.Określenie czasu i miejsca: naruszenia/ujawnienia i powiadomienia o tym fakcie;
6.9.3.Określenie okoliczności towarzyszących i rodzaju naruszenia/ujawnienia;
6.9.4.Wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania;
6.9.5.Wstępną ocenę przyczyn wystąpienia naruszenia/ujawnienia;
6.9.6.Ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

6.10.Raport, o którym mowa w pkt. 6.9, ABI niezwłocznie przekazuje ADO.

6.11.Zaistniałe naruszenie ochrony danych osobowych może stać się przedmiotem szczegółowej analizy prowadzonej przez ADO i ABI.

7.Zasady postępowania z informacjami, zapewniającymi minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.

7.1. Wprowadzono coroczna analizę ryzyka oceniającą stopień zagrożenia utraty bezpieczeństwa danych osobowych zgodnie z punktem 3.6.5

7.2. Pomieszczenia powinny zapewniać takie rozmieszczenie sprzętu oraz dokumentów aby uniemożliwić dostęp do informacji osobom nie upoważnionym do dostępu do tej informacji

7.3 Pomieszczenia powinny być zlokalizowane w miejscach gdzie ryzyko ich zatopienia lub zalania jest zminimalizowane.

7.4. Zaleca się aby pomieszczenia były wyposażone w system alarmowy, czujki wilgoci oraz dymu funkcją powiadomienia do służby ochrony lub jednostek straży pożarnej, policji

7.5. Kontrola dostępu do obszarów bezpiecznych realizowana jest metodami organizacyjno-proceduralnymi.

7.6. Dostęp do Pomieszczeń mogą mieć tylko osoby upoważnione do przetwarzania danych przez podmiot uprawniony. Inne osoby mogą przebywać w Pomieszczeniach jedynie w obecności osób upoważnionych, za ich wiedzą i zgodą.

7.7. Dokumenty i nośniki informacji zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym dostęp do nich osobom nieupoważnionym.

7.8 Karty kryptograficzne służące do logowania, należy składować w szafach wyposażonych w co najmniej 1 zamek. Zakazane jest przechowywanie wraz z kartą kodu PIN.

7.9. Do likwidacji wydruków dokumentów i nośników informacji powinny być stosowane niszczarki.

7.10. Oprogramowanie antywirusowe powinno posiadać aktualne definicje i bazy antywirusowe.

7.11. Wbudowane konto administratora należy używać tylko w przypadku wykonywania czynności administratora;

7.12. Konta użytkownika nie mogą mieć uprawnień administratora o ile nie jest to wymagane przy bieżącej pracy;

7.13. Długość hasła konta administratora lub użytkownika z uprawnieniami administratora nie mniej niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie dłuższy niż 30 dni;

7.14. Długość hasła konta użytkownika nie mniej niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra), okres ważności hasła nie dłuższy niż 30 dni

7.15. Oprogramowanie antywirusowe instalowane na stacjach przetwarzających dane działające w czasie rzeczywistym, ustawienie oprogramowania zapewniające bieżącą aktualizację sygnatur antywirusowych

7.16. Stacja powinna być ustawiona w miejscu uniemożliwiającym do niej dostęp osobom nieupoważnionym

7.17. Wymagane jest takie ustawienie drukarki aby nie było możliwości podejrzenia bądź pobrania wydruków przez osoby nieuprawnione

7.18. Wymagane jest takie ustawienie monitora i dokumentów papierowych aby nie było możliwości podejrzenia danych przetwarzanych na ekranie lub biurku przez osoby nieuprawnione.

7.19. Każdemu użytkownikowi komputera należy założyć oddzielne konto;

8.Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

8.1.Opis sposobu zarządzania systemem informatycznym służącym do przetwarzania danych osobowych znajduje się w załączniku 2 do Zarządzenia Starosty Mławskiego w sprawie wprowadzenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

8.2.Załącznik jest aktualizowany w przypadku wystąpienia potrzeby wprowadzeniu istotnych zmian w zakresie zarządzania systemem informatycznym. Podpisywany jest przez Administratora Danych Osobowych.

9.Ewidencja osób upoważnionych do przetwarzania danych osobowych, procedura nadawania upoważnień i odpowiedzialność osób zaangażowanych w ten proces

9.1.Ewidencja osób upoważnionych do przetwarzania danych osobowych prowadzona jest przez Administratora Bezpieczeństwa Informacji.

9.2.Ewidencja prowadzona jest w wersji elektronicznej. W razie potrzeby drukowana jest wersja papierowa. Ewidencja nie podlega ogłoszeniu w Biuletynie Informacji Publicznej.

9.3.W celu nadania upoważnień lub dokonania jakiekolwiek zmiany czasu i zakresu upoważnienia danego pracownika przetwarzającego dane lub w przypadku ustania stosunku pracy i wszelkich innych zmian wynikających ze stosunku pracy, pracownik lub jego zastępca do spraw kadrowych informuje o tym Administratora Bezpieczeństwa Informacji na odpowiednim formularzu.

9.4.Dyrektorzy Wydziałów zgłaszają do pracownika do spraw kadrowych przypadki wszelkich zmian w organizacji pracy wiążących się z koniecznością zmiany uprawnień podległych pracowników do przetwarzania innych zbiorów danych osobowych. Pracownik do spraw kadrowych, przekazuje w/w informację Administratorowi Bezpieczeństwa Informacji na formularzu w celu nadania upoważnienia

9.5.Za dopuszczenie pracownika do pracy, wykonywanie lub kontynuację tej pracy przy przetwarzaniu danych osobowych nie zgodnej z upoważnieniem lub pracy bez upoważnienia odpowiada Dyrektor Wydziału.

9.6.Za niedopełnienie obowiązku informacyjnego wynikającego z art 24 i 25 Ustawy odpowiada Dyrektor Wydziału w zakresie zbiorów danych osobowych przetwarzanych przez podległych pracowników.

10.Zgłaszanie i modyfikacje zbiorów danych do ich ewidencji

10.1. Administrator Bezpieczeństwa Informacji prowadzi rejestr zbiorów danych osobowych, o którym mowa w art. 36a ust.2 pkt 2 ustawy o ochronie danych osobowych

10.2.Dyrektor Wydziału identyfikuje, aktualizuje i zgłasza zbiory danych osobowych do Administratora Bezpieczeństwa Informacji.

10.3.Dyrektor Wydziału identyfikuje, aktualizuje oraz zgłasza zbiory danych osobowych zawierające dane wyszczególnione w art. 27 ust 1 ustawy o ochronie danych osobowych a wyznaczony przez niego pracownik przesyła projekt wniosku o rejestrację zbioru danych osobowych w wersji elektronicznej do Generalnego Inspektora Ochrony Danych Osobowych pod nadzorem ABI.

10.4.Wydruk projektu wniosku przesłanego elektronicznie z zamiarem rejestracji zbioru według art. 27 ust 1 ustawy o ochronie danych osobowych oznaczony jest statusem „Projekt”. Po

podpisaniu przez Dyrektora Wydziału jako projekt zgłoszenia, przekazywany jest następnie do Administratora Bezpieczeństwa Informacji

10.5.Administrator Bezpieczeństwa Informacji wysyła zgłoszenie zbioru według art. 27 ust 1 ustawy o ochronie danych osobowych do rejestracji w formie papierowej do Biura Generalnego Inspektora Ochrony Danych Osobowych (GIODO), a w przypadku zbioru nie podlegającego obowiązkowi zgłaszania do GIODO rejestruje zbiór w rejestrze zbiorów danych oraz w załączniku 1,2 i 3 do Polityki bezpieczeństwa.

10.6.Za nie zgłoszenie do rejestracji zbioru danych lub nie zaktualizowanie tego zbioru według procedury opisanej w pkt. 10.2, 10.3 i 10.4 odpowiada Dyrektor Wydziału

11. Obowiązek informacyjny

11.1. Osoby od których zbierane są dane osobowe zostają poinformowane przez administratora danych o których mowa w art. 24 ust. 1 Ustawy o ochronie danych osobowych,
11.2. Obowiązek informacyjny uznaje się za spełniony w przypadku spraw o których mowa w art. 24 ust 2 pkt 1 i 2 wyżej wymienionej ustawy.