Załącznik nr 2
do Zarządzenia nr 22/2018
Starosty Mławskiego
z dnia 23.05.2018 r.

Or. 142.2.2018

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

1.Procedura nadawania i zmiany uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemach informatycznych oraz wskazanie osoby odpowiedzialnej za te czynności

1.1.Administrator Danych Osobowych (ADO) nadaje upoważnienie do przetwarzania danych osobowych również w zakresie dostępu do systemu informatycznego osobie, która w związku z wykonywanymi przez siebie obowiązkami będzie miała dostęp do danych osobowych w systemie. Upoważnienie to przekazywane jest w postaci papierowej do:

1 egz. do kadr - celem umieszczenia teczce akt osobowych,
1 egz. do osoby, której upoważnienie dotyczy,
1 egz. do teczki spraw o sygnaturze 142.3 (według JRWA)

1.2.IOD lub pracownik współpracujący z IOD, aktualizuje ewidencję osób upoważnionych do przetwarzania danych osobowych na podstawie informacji pochodzących od pracownika ds. kadr, a od Administratorów/Administratora Systemu Informatycznego otrzymuje informacje o nadanych identyfikatorach za pomocą systemu zarządzania użytkownikami

1.3. Administrator/Administratorzy Systemu Informatycznego (ASI) - upoważnieni pracownicy zatrudnieni w Starostwie Powiatowym w Mławie na etacie informatyka lub starszego informatyka zobowiązani są do następujących czynności:

1.3.1.Rejestrują użytkownika w systemie i nadają mu określone uprawnienia oraz hasło
1.3.2.Nadają identyfikator, tymczasowe hasło i prowadza ewidencję identyfikatorów użytkowników w systemie zarządzania użytkownikami
1.3.3.Umożliwiają użytkownikowi zastosowanie i zmianę hasła podczas pierwszego logowania
1.3.4.Prowadzą rejestr komputerów, serwerów oraz wszelkich nośników informacji zarówno stacjonarnych jak i przenośnych oraz odpowiedzialnych za nie użytkowników.
1.3.5.Dbają o właściwe oznaczenie i zabezpieczenie nośników wymienionych w pkt 1.3.4.

1.4.Użytkownik po otrzymaniu informacji o założonym koncie z wymaganymi uprawnieniami:
1.4.1.Loguje się do systemu/aplikacji w celu sprawdzenia poprawności konta i uprawnień,
1.4.2.Przy pierwszym logowaniu się do systemu/aplikacji użytkownik musi zmienić nadane mu hasło. Hasło jest tajne i znane jedynie użytkownikowi.
1.4.3.Użytkownik zobowiązany jest zmiany hasła nie rzadziej niż 30 dni lub w przypadku gdy hasło mogło być ujawnione.
1.4.4.W przypadku zablokowania konta lub zapomnienia hasła użytkownik kontaktuje się z ASI w celu wygenerowania nowego tymczasowego hasła (które należy zmienić przed logowaniem się do systemu) i/lub odblokowania konta.

1.5.Użytkownik odpowiada za właściwe użytkowanie sprzętu informatycznego (komputery, monitory i drukarki i inne urządzenia) oraz mobilne nośniki informacji (nośniki przenośne, dyskietki, karty elektroniczne, itp.).

1.6.Użytkownik jest wyrejestrowany z systemu informatycznego w każdym przypadku utraty przez niego uprawnień do dostępu do danych osobowych, co ma miejsce w przypadku:
1.6.1.Ustania zatrudnienia,
1.6.2.Zmiany zakresu obowiązków,
1.6.3.Utraty upoważnienia.

1.7. Pracownik ds. kadr przekazuje do IOD lub innego wyznaczonego pracownika i ASI informację pisemną o zatrudnieniu lub ustaniu zatrudnienia, zmianie zakresu obowiązków i utracie upoważnienia niezwłocznie z chwilą ich zaistnienia

1.8. Hasła uprzywilejowane, hasła ASI, hasła do urządzeń zarządzających siecią oraz innych urządzeń używanych w urzędzie przechowywane są w metalowej kasecie w serwerowni.

1.9. IOD posiada konto uprzywilejowane pozwalające mu na pełen dostęp do systemów teleinformatycznych pozwalających mu na wykonywanie swojego zakresu obowiązków.

2. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

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

2.2.W systemie informatycznym stosuje się uwierzytelniania dwustopniowe; na poziomie:
a)dostępu do systemu,
b)dostępu do systemu/aplikacji.

2.3.Do uwierzytelnienia użytkownika w systemie na obu poziomach stosuje się identyfikatory i hasła lub karty inteligentne
2.3.1.Stosowanie unikalnych identyfikatorów użytkownika zapewnia bezpieczeństwo i realizuje zasady rozliczalności w systemach i sieciach teleinformatycznych Starostwa Powiatowego w Mławie,
2.3.2.Zasada ta ma na celu przypisanie w sposób jednoznaczny wszelkich działań w systemie konkretnemu użytkownikowi (nie dopuszcza się, aby użytkownik korzystał z kont: administrator, gość, a także z konta innego użytkownika),

2.4.W Starostwie Powiatowym w Mławie, stosuje się poziom bezpieczeństwa przetwarzania danych adekwatnie do klasyfikacji tych danych w systemach/aplikacjach zgodny z przeprowadzoną analizą ryzyka

2.5.Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: identyfikatora, dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów bądź innych bezpośrednio kojarzących się z użytkownikiem.

2.6.Hasło nie może być ujawnione innej osobie nawet po utracie ważności hasła.

2.7.System automatycznie powinien wymuszać zmianę hasła nie rzadziej, niż jeden raz w miesiącu. Hasło musi być zmienione przez użytkownika niezwłocznie w przypadku podejrzenia lub stwierdzenia jego ujawnienia.

2.8.W przypadku komputerów podłączonych do domeny konto jest blokowane po 5-cio krotnym wpisaniu błędnego hasła. Blokada zostaje zdjęta po 30 minutach od ostatniej próby wprowadzenia błędnego hasła.

2.9.Procedura zarządzania środkami uwierzytelniania:
2.9.1.ASI nadają hasło dostępu do systemu/aplikacji dla nowego użytkownika albo dla

użytkownika, który zapomniał swoje ostatnie hasło,
2.9.2.Użytkownik systemu/aplikacji niezwłocznie ustala swoje, znane tylko jemu hasło, po nadaniu hasła przez ASI. System powinien automatycznie wymuszać na użytkowniku zmianę nadanego przez administratora hasła przy pierwszym logowaniu,
2.9.3.Użytkownik systemu w dowolnym momencie może zmienić swoje hasło dostępu do systemu/aplikacji,
2.9.4.Obowiązuje bezwzględny zakaz notowania w jakiejkolwiek formie obecnych oraz wygasłych haseł dostępu,
2.9.5.ASI zapisują swój identyfikator oraz hasła dostępu po każdej ich zmianie i umieszczają je w kopercie, a następnie zamykają kopertę w metalowej kasetce wyznaczonej do tego celu ulokowanej w serwerowni głównego budynku Starostwa Powiatowego w Mławie. Koperta taka może być awaryjnie udostępniona innemu administratorowi za zgodą administratora danych. Po awaryjnym użyciu hasła, musi ono zostać niezwłocznie zmienione przez właściwego ASI.

3.Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

3.1.Procedura rozpoczęcia pracy
3.1.1.uruchomić komputer wchodzący w skład systemu informatycznego, podłączony fizycznie do sieci lokalnej i zalogować się podając własny identyfikator i hasło dostępu,
3.1.2.W przypadku systemów podłączonych do domeny jeśli użytkownik wprowadzi 5-krotnie błędnie hasło, wówczas jego identyfikator i hasło zostaną zablokowane. W celu odblokowania swojego identyfikatora, użytkownik kontaktuje się z ASI w celu uzyskania nowego hasła lub odblokowania konta.
3.1.3.Uruchomić wybrany system/aplikację (w szczególności aplikację bazodanową m.in. przetwarzającą dane),
3.1.4.Zalogować się do systemu/aplikacji w sposób analogiczny do przedstawionego powyżej.
3.2.Procedura zawieszenia pracy w systemie/aplikacji. Przy każdorazowym opuszczeniu stanowiska komputerowego, należy dopilnować, aby na ekranie nie były wyświetlane informacje lub dane, poprzez zablokowanie lub wylogowanie komputera. Każdy użytkownik ma obowiązek stosowania blokady ekranu zabezpieczonego hasłem, zablokowania komputera lub wylogowania się z systemu.

3.3.Procedura zakończenia pracy w systemie
3.3.1.Zamknąć system/aplikację,
3.3.2.Zamknąć system operacyjny komputera i zaczekać na jego wyłączenie,
3.3.3.Wyłączyć monitor
3.3.4.Sprawdzić, czy stacjonarne elektroniczne nośniki informacji zawierające dane osobowe nie zostały pozostawione bez nadzoru.
3.3.5. Sprawdzić, czy przenośne elektroniczne nośniki informacji zawierające dane osobowe będące w posiadaniu użytkownika nie zostały pozostawione bez nadzoru i czy zostały odpowiednio zabezpieczone przy pomocy środków kryptograficznych.

4.Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

4.1.W cyklu dziennym kopie wykonywane są przez ASI lub automatycznie przez odpowiedni program. Kopie składowane są na odrębnym sprzęcie, który pełni funkcję archiwum.

4.2.W wyjątkowych przypadkach takich jak np. niebezpieczeństwo utraty danych kopie zapasowe mogą być wykonywane po zaszyfrowaniu przez użytkowników aplikacji na zewnętrznych elektronicznych nośnikach informacji.

4.3.Administratorzy Systemu Informatycznego w sytuacji opisanej w pkt.4.2, sprawują nadzór nad wykonywaniem kopii zapasowych, weryfikuje ich poprawność. Kopie te przechowywane są w serwerowni.

4.4.Elektroniczne nośniki informacji zawierające dane osobowe można przekazywać tylko podmiotom lub osobom uprawnionym na podstawie przepisów prawa, za zgodą osoby do tego upoważnionej przez Administratora Danych Osobowych,

4.4.a Elektroniczne nośniki informacji o których mowa w punkcie 4.4 powinny być zabezpieczone za pomocą środków kryptograficznej ochrony zapewniając poufność i integralność danych przekazywanych poza obszar przetwarzania danych. Szyfrowanie danych może odbyć się z użyciem aplikacji 7-zip.

4.5. Za właściwą realizację wdrożonych mechanizmów zapewniających poufność i integralność danych przekazywanych poza obszar przetwarzania danych odpowiada pracownik przygotowujący dane do przekazania. Pracownik ten przekazuje również odbiorcy hasło umożliwiające otwarcie zaszyfrowanych plików.

4.6.Dane osobowe przenoszone za pomocą zewnętrznych nośników informacji powinny być z nich trwale usunięte po poprawnym ich przeniesieniu na docelowy sprzęt komputerowy i do docelowej bazy danych,

4.7.Wewnętrzne elektroniczne nośniki informacji zamontowane na komputerach i serwerach jako dyski twarde są przechowywane w pomieszczeniu stanowiących obszar przetwarzania danych osobowych, określony w polityce bezpieczeństwa.

4.8.Po zakończeniu pracy przez użytkowników systemu przenośne elektroniczne nośniki informacji są przechowywane w zamykanych na klucz szafach biurowych lub szafach pancernych.

4.9.W przypadku uszkodzenia lub zużycia nośnika elektronicznego zawierającego dane osobowe należy go fizycznie zniszczyć przez spalenie lub rozdrobnienie.

4.10.Dostęp do szaf pancernych mają tylko upoważnieni pracownicy.

4.11.Wydruki, zawierające dane osobowe, należy przechowywać w pokojach stanowiących obszar przetwarzania danych osobowych, określonych w niniejszym zarządzeniu.

4.12.Wydruki, zawierające dane osobowe, należy zniszczyć przez pocięcie w niszczarce po ich wykorzystaniu chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania.

4.13.Dane osobowe zapisane w formie papierowej inne niż wydruki z systemu (pisma, ankiety itp.) są przechowywane na podobnych zasadach, co wydruki.

4.14.ASI prowadzą rejestr nośników elektronicznych oraz ich użytkowników.

4.15.Kopie baz danych w zakresie państwowego zasobu geodezyjnego i kartograficznego oraz ewidencji gruntów i budynków wykonuje Kierownik Powiatowego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej nie rzadziej niż raz na kwartał na nośnik zewnętrzny (np. płyta DVD). Co najmniej 2 ostatnie kopie przechowuje się w budynku przy ul. Reymonta 6 w Wydziale Organizacyjnym w pokoju nr 15 w metalowej szafie. Kopie te

przed skopiowaniem na nośnik zewnętrzny powinny być zabezpieczone hasłem. Hasła zapisywane są w rejestrze i przechowywane w pomieszczeniu serwerowni w budynku przy ul. Stary Rynek 10.

5.Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych o których mowa w pkt 4 i wydruków zawierających dane osobowe

5.1.Dane osobowe w postaci elektronicznej przetwarzane w systemie informatycznym, zapisane na dyskietkach, płytach CD i innych zewnętrznych (wymontowane dyski twarde, nośniki typu pamięć masowa, karty elektroniczne i in.) lub wewnętrznych nośnikach (dyski zamontowane w komputerach, serwerach) nie mogą być wynoszone poza siedzibę urzędu bez zgody Administratora Danych.

5.2.Zewnętrzne nośniki informacji (dyskietki, płyty CD, taśmy magnetyczne, nośniki typu pamięć masowa i inne nośniki) powinny być zabezpieczone przez użytkowników przed nieuprawnionym odczytem, przejęciem lub skopiowaniem za pomocą programów szyfrujących. ASI dostarcza użytkownikom odpowiedni program szyfrujący, a użytkownicy zobowiązani są do wykonywania działań kryptograficznych.

5.3.Do przesyłania danych osobowych metodą teletransmisji są stosowane środki kryptograficzne

5.4.Wewnętrzne elektroniczne nośniki informacji zamontowane na komputerach i serwerach jako dyski twarde są przechowywane w pomieszczeniu stanowiących obszar przetwarzania danych osobowych, określony w polityce bezpieczeństwa.

5.5.Po zakończeniu pracy przez użytkowników systemu przenośne elektroniczne nośniki informacji są przechowywane w zamykanych na klucz szafach biurowych, biurkach lub szafach pancernych.

5.6.Dane osobowe w postaci elektronicznej, po ustaniu ich użyteczności należy usunąć z nośnika informacji w sposób uniemożliwiający ich ponowne odtworzenie.

5.7.W przypadku uszkodzenia lub zużycia nośnika elektronicznego zawierającego dane osobowe należy go fizycznie zniszczyć przez spalenie lub rozdrobnienie.

5.8.Za przechowywanie i właściwe użytkowanie wymienionych w pkt 5.13 nośników odpowiada użytkownik.

6.Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego i sposób zabezpieczenia systemu przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej

6.1.Nadzór nad instalowaniem nowego oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawują Administratorzy Systemu Informatycznego (ASI) .

6.2.Oprogramowanie zastosowane w systemach informatycznych automatycznie monitoruje występowanie wirusów w trakcie załączania lub wczytywania danych z zewnętrznych nośników informacji

6.3.Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.

6.4.Czynności związane z ochroną antywirusową systemu informatycznego wykonują ASI, wykorzystując w trakcie pracy moduł programu antywirusowego z aktualną bazą antywirusową.

6.5.Użytkownik systemu importujący dane osobowe do systemu informatycznego z elektronicznego nośnika jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów.

6.6.O każdorazowym wykryciu wirusa przez oprogramowanie antywirusowe użytkownik obowiązany jest niezwłocznie poinformować ASI.

6.7.Po usunięciu wirusa ASI sprawdzają system informatyczny oraz przywraca go do pełnej funkcjonalności i sprawności.

6.8.Administratorzy Systemu Informatycznego prowadzą w formie elektronicznej rejestr przypadków zainfekowania komputerów i nośników wykorzystywanych do przetwarzania danych osobowych w systemie.

6.9.Administratorzy Systemu Informatycznego są odpowiedzialni za aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku: sieci lokalnej, stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.

6.10.Użytkownikowi systemu zabrania się dokonywania jakichkolwiek zmian konfiguracji w zainstalowanym oprogramowaniu monitorującym wymianę danych na styku tego stanowiska i sieci lokalnej.

6.11.Ochrona systemu informatycznego używanego w Starostwie polega w szczególności na:
a)ochronie przez identyfikator i hasło
b)przydzielaniu uprawnień,

6.12.W systemie informatycznym zastosowano zasilacze awaryjne UPS zabezpieczające przed utratą danych spowodowanych awarią zasilania lub zakłóceniami w sieci zasilającej.

7.Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych.

7.1.W systemie informatycznym odnotowywane są informacje o odbiorcach danych z tego systemu. Ponadto informacja ta odnotowywana jest w elektronicznym systemie obiegu dokumentów.

7.2.Elektroniczny obieg dokumentów rejestruje odbiorcę danych, datę i zakres udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych

7.3.Odbiorca oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego

postępowania zgodnie z prawem nie są jednak uznawane za odbiorców.

7.4.Odnotowanie obejmuje informacje o:

7.4.1.Nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane,
7.4.2.Zakresie udostępnianych danych,
7.4.3.Dacie udostępnienia.

7.5.Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.

7.6.Nadzór nad prawidłowością odnotowywania w systemie w/w informacji sprawuje ASI.

7.7.Udostępnienie danych osobowych może nastąpić na prośbę odbiorcy danych. Przed udostępnieniem danych pracownik identyfikuje tożsamość odbiorcy danych. Procedurę ustalenia tożsamości odbiorcy określa dyrektor danego wydziału.

8.Zasady i sposoby odnotowywania przetwarzania danych osobowych w systemie informacji

8.1.Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, poza programami służącymi tylko do edycji tekstu w celu udostępnienia go na piśmie, system ten zapewnia odnotowanie:
8.1.1.Daty pierwszego wprowadzenia danych,
8.1.2.Identyfikatora użytkownika wprowadzającego dane osobowe,
8.1.3.Źródło danych,
8.1.4.Informacji o odbiorcach danych
8.1.5.Sprzeciwu, odnośnie przetwarzania danych

8.2.Odnotowanie informacji o których mowa w pkt. 8.1.1. i 8.1.2 następuje automatycznie

8.3.System zapewnia sporządzenie i wydrukowanie raportu zawierającego informacje wymienione w pkt. 8.1

8.4.Nadzór nad prawidłowością odnotowywania w systemie w/w informacji sprawuje ASI.

9.Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

9.1.ASI odpowiedzialni są za przeglądy i konserwacje. W przypadku wystąpienia nieprawidłowości, które mogły spowodować utratę integralności danych osobowych, ASI informują o tym IOD.

9.2.Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego wykonywane w przypadku wystąpienia nieprawidłowości.

9.3.Nieprawidłowości ujawnione w trakcie tych działań zostaną niezwłocznie usunięte.

9.4.Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiadają Administratorzy Systemu Informatycznego.

9.5.Sprawdzanie poprawności działania programów i narzędzi programowych

przeprowadza się w następujących przypadkach:
9.5.1.Zmiany wersji oprogramowania serwera plików;
9.5.2.Zmiany wersji oprogramowania stanowiska komputerowego użytkownika systemu;
9.5.3.Zmiany systemu operacyjnego serwera plików;
9.5.4.Zmiany systemu operacyjnego stanowisk komputerowego użytkownika systemu;
9.5.5.Wykonania/zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modyfikacji systemu

9.6.Zarówno przed jak i po dokonaniu zmian w systemie informatycznym należy dokonać przeglądu działania systemu.

9.7.Sprawdzenie wymienione w pkt. 9.6 powinno obejmować:
9.7.1.Poprawność logowania się do systemu w zależności od posiadanych uprawnień przez symulację pracy wszystkich typów uprawnień użytkownika.
9.7.2.Poprawność działania podstawowych elementów aplikacji w obecności ASI.

9.8.Przegląd przeprowadza projektant nowego systemu pod nadzorem Administratora/Administratorów Systemu Informatycznego.

9.9.Za prawidłowość przeprowadzenia przeglądów i konserwacji systemu odpowiada Administrator/Administratorzy Systemu Informatycznego.

9.10.Konserwację oprogramowania przeprowadza się po zgłoszeniu przez użytkownika systemu potrzeby wprowadzenia zmian pozwalających utrzymać funkcjonalność systemu w dynamicznie zmieniającym się środowisku

9.11.Przegląd danych osobowych przechowywanych na nośnikach przenośnych pod kątem celowości i czasu ich przechowywania, dokonywany jest przez użytkownika.

9.12.ASI dokonują przeglądu celowości i czasu użytkowania nośników.

10.Przetwarzanie danych osobowych w zbiorach doraźnych

10.1.Dostęp do danych osobowych powinien odbywać się poprzez aplikację edytora tekstu lub, gdy zachodzi potrzeba zapisania danych w innym formacie np. w postaci pliku arkusza kalkulacyjnego, można tego dokonać w doraźnym zbiorze danych osobowych pod warunkiem, że zapisane dane będą należycie chronione oraz usunięcie danych po okresie użytkowania, tj.

10.1.1.Uniemożliwi się dostęp do danych osobom nieuprawnionym,
10.1.2.Uniemożliwi się zmiany danych a tym samym zafałszowanie informacji pochodzących z systemu,
10.1.3.Dostęp do komputera zawierającego zbiory doraźne zabezpieczony jest hasłem.

10.2.Po wykorzystaniu doraźny zbiór danych osobowych należy niezwłocznie usunąć z nośnika danych, na którym został utworzony lub zniszczyć nośnik.

10.3.Zawiadamiać administratora danych, ASI lub IOD w przypadku podejrzenia lub stwierdzenia dostępu do zbioru osób nieuprawnionych.

11.Obowiązki Administratorów Systemu Informatycznego

11.1.Administrator lub Administratorzy Systemu Informatycznego (ASI) zobowiązani są do przestrzegania zapisów Polityki Bezpieczeństwa obowiązującej w Starostwie Powiatowym w Mławie. Ponadto zobowiązani są do przestrzegania, wdrożenia i realizacji niniejszej Instrukcji, a także do przestrzegania i realizacji aktów prawnych odnoszących się do bezpieczeństwa informacji oraz wynikających z nich obowiązków odnoszących się w szczególności do przetwarzania informacji przy pomocy systemu informatycznego.

11.2.Administrator/Administratorzy Systemu informatycznego zobowiązani są w szczególności do:
11.2.1.Wykonywania poleceń Administratora Danych odnośnie całości spraw związanych z bezpieczeństwem informacji oraz zaleceń IOD w zakresie zarządzania podległymi systemami informatycznymi i polityki bezpieczeństwa
11.2.2.Wdrażanie i realizacja Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz realizacja wytycznych Polityki bezpieczeństwa
11.2.3.Czuwania nad właściwym eksploatowaniem podległych im systemów informatycznych i bieżącą ich konserwacją oraz przeglądami
11.2.4.Prowadzenia i uaktualniania:
a)ewidencji, etykietowania oraz oznaczania wszystkich elektronicznych nośników stacjonarnych, wymiennych i przenośnych Starostwa Powiatowego w tym komputerów i serwerów wraz z ich użytkownikami, identyfikatorami, parametrami technicznymi, miejscami, okresem przechowywania.
b)dopuszcza się prowadzenie wymienionej w pkt 11.2.4. ewidencji w formie elektronicznej
c)rodzaju systemów informatycznych funkcjonujących w zakresie ich działania
d)listy identyfikatorów osób biorących udział przy przetwarzaniu danych osobowych w podległych im systemach informatycznych
e)rejestru naruszeń ochrony danych osobowych
11.2.5.ASI w przypadku wykrycia zdarzeń wpływających w sposób istotny na bezpieczeństwo systemów informatycznych, informują o nich IOD
11.2.6.Kontrolowania i zabezpieczenia prawidłowości przebiegu czynności serwisowych w podległych systemach informatycznych, przy czym urządzenia, dyski lub inne nośniki zawierające dane osobowe, pozbawiają przed naprawą zapisu tych danych lub nadzorują ich naprawę
11.2.7.Pozbawiania zapisu danych osobowych lub uszkadzania w sposób uniemożliwiający odczytanie tych nośników, które przeznaczone są do likwidacji lub zbycia.
11.2.8.Instalowania zabezpieczeń i środków kryptograficznych w podległych systemach informatycznych wynikających z przepisów o ochronie danych osobowych i zaleceń IOD
11.2.9.Zgłaszania Administratorowi Danych oraz Sekretarzowi Powiatu potrzeb w zakresie zabezpieczenia podległych im systemów informatycznych
11.2.10.Postępowania zgodnie z instrukcją w sytuacji naruszenia ochrony danych osobowych
11.2.11.Kontrolowania procesu wykonywania z poszczególnych systemów informatycznych kopii awaryjnych, pod kątem prawidłowości ich wykonania oraz ich dalszej przydatności do odtworzenia w przypadku awarii
11.2.12.Znajomości funkcji poszczególnych systemów informatycznych ze szczególnym uwzględnieniem procedur
a)dostępu i modyfikowania do danych osobowych
b)zarządzania identyfikatorami i hasłami użytkowników
c)wykonywania kopii awaryjnych oraz odtwarzania danych z tych kopii
d)generowania wydruków danych osobowych
e)dostępu do systemów rejestrujących identyfikatory oraz czas logowania użytkowników
11.2.13.Zgłaszania do IOD wdrażania nowych systemów, aktualizacji powiązań między

systemami lub programami. Informację można przekazać w formie elektronicznej.
11.2.14.Realizacji niniejszej Instrukcji oraz polityki bezpieczeństwa informacji.

11.3.Ponadto Administrator/Administratorzy Systemu Informatycznego służącego do przetwarzania danych osobowych odpowiadają za bieżącą eksploatację tego systemu, a w szczególności za:
11.3.1.Wszystkie czynności związane z ich funkcjonowaniem i modernizacją systemu, programów i urządzeń informatycznych
11.3.2.Rejestrowanie i wyrejestrowywanie z systemu użytkowników oraz projektantów i programistów w czasie instalowania systemu oraz jego modyfikacji
11.3.3.Przydzielanie uprawnień dostępu do poszczególnych funkcji systemu
11.3.4.Realizację wymogu 30-dniowego okresu zmian haseł na komputerach użytkowników
11.3.5.Realizację procedur wykonywania kopii awaryjnych, określenie ich częstotliwości, zmianę nośników oraz ich właściwe przechowywanie, sprawdzanie poprawności zapisu oraz likwidację nośników wewnętrznych i zewnętrznych.
11.3.6.Postępowania zgodnie z Instrukcją oraz Polityką Bezpieczeństwa Informacji

12. Procedura likwidacji i zbywania sprzętu.

12.1.Procedura jest opisana w „Regulaminie w sprawie sposobu i trybu gospodarowania składnikami rzeczowymi majątku ruchomego, stanowiącego własność powiatu, przez jednostki organizacyjne Powiatu Mławskiego", który jest wprowadzany i modyfikowany uchwałami Zarządu Powiatu Mławskiego.
12.2.Sprzęt przeznaczany do likwidacji lub zbycia pozbawiany jest przez ASI z elementów przechowujących dane osobowe.
12.3.Dane osobowe przechowywane na nośnikach informacji są usuwane przez ASI poprzez uszkodzenie nośnika uniemożliwiające ich późniejsze odczytanie.
12.4. Sprzęt przeznaczany do likwidacji lub zbycia przekazywany jest do ASI/informatyków w celu właściwego uszkodzenia nośnika zawierającego dane osobowe.
12.5.Likwidacja sprzętu odnotowana jest w ewidencji elektronicznych nośników informacji.