ZARZĄDZENIE NR 116 / 2017
STAROSTY PUCKIEGO
z dnia 9 listopada 2017 r.

w sprawie: wprowadzenia „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Pucku"

Na podstawie: art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922 z późn. zm.) oraz § 38 ust. 1 Regulaminu Organizacyjnego Starostwa Powiatowego w Pucku zarządza się, co następuje:

§ 1

Wprowadzam do stosowania w Starostwie Powiatowym w Pucku „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Pucku", stanowiącą załącznik do niniejszego zarządzenia.

§ 2

Załącznik nr 4 do „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Pucku" nie podlega publikacji w serwisie wewnętrznym Starostwa ani na stronie internetowej Biuletynu Informacji Publicznej.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

Z up. STAROSTY
WICESTAROSTA
Tomasz Herrmann

Barbara Wiśniewska
adwokat

Załącznik do zarządzenia nr 116/2017
Starosty Puckiego z dnia 08.11. 2017 r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Pucku

WERSJA 1.

Opracował:	Data:	Zatwierdził:	Data:
ADMINISTRATOR Systemów Informatycznych Marek Gafka NACZELNIK WYDZIAŁU ORGANIZACJI I KONTROLI Grzegorz Dziewięcin	09.11.2017 r.	Z up. STAROSTY WICESTAROSTA Tomasz Herrmann	08.11.2017 r.

I. Postanowienia wstępne

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Pucku, zwana dalej „Instrukcją" stanowi zestaw procedur opisujących zasady zabezpieczania danych osobowych przetwarzanych w zbiorach papierowych i w systemach informatycznych.
2. Ilekroć w postanowieniach Instrukcji mowa jest o ASI, należy przez to rozumieć Administratora Systemów Informatycznych - osobę lub podmiot sprawującą zadania związane z administracją systemami, bazami lub aplikacjami ADO. Formami zatrudnienia ASI mogą być: umowa o pracę, umowa cywilno-prawna, kontrakt (umowa) z firmą informatyczną w zakresie administracji systemami informatycznymi.

II. Klucze do pomieszczeń służbowych

1. Polityka kluczy obejmuje budynki Starostwa przy ul. Elizy Orzeszkowej 5, ul. Kolejowej 7 B i ul. 1 Maja 13.
2. Klucze do pomieszczeń pozostają pod osobistym nadzorem pracowników, dla których pomieszczenia te są stałym miejscem pracy.
3. Klucze do pomieszczeń szczególnie chronionych np. serwerowni pozostają pod osobistym nadzorem osób upoważnionych. Dostęp osób trzecich do tych pomieszczeń odbywa się pod ścisłym nadzorem osób upoważnionych.
4. Klucze zapasowe przechowywane są w wyznaczonym miejscu. Wydawanie kluczy zapasowych upoważnionym pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą osób uprawnionych. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu.
5. Klucze do pomieszczeń służbowych nie mogą być pozostawiane w drzwiach.
6. Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane
7. Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu.
8. Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.
9. Po zakończeniu pracy pracownicy zobowiązani są
   1) wyłączyć urządzenia znajdujące się w pomieszczeniu,
   2) zabezpieczyć dokumenty w sposób uniemożliwiający dostęp do nich osobom trzecim,
   3) zamknąć biurka, szafy, a klucze pozostawić w zabezpieczonym miejscu,

4) zamknąć okna znajdujące się w pomieszczeniu służbowym,
5) zamknąć pomieszczenia służbowe.

III. Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej

1. Zastosowano UPS centralny do podtrzymania urządzeń w serwerowni. Kluczowe komputery na których przetwarzane są dane osobowe podłączone są również pod UPS.
2. Użytkownicy komputerów przenośnych na których są przetwarzane dane osobowe są zobowiązani do przestrzegania „Regulaminu użytkowania komputerów przenośnych", stanowiącego załącznik nr 1 do Instrukcji. Fakt zapoznania się z regulaminem użytkownik potwierdza własnoręcznym podpisem.
3. Dane osobowe na komputerach przenośnych wynoszonych poza teren Starostwa muszą być przechowywane na zaszyfrowanych partycjach.
4. W przypadku dostępu do danych osobowych przez internet stosuje się szyfrowanie tego połączenia SSL.
5. W przypadku dostępu do danych osobowych przez internet do środków teletransmisji, wymagane jest uwierzytelnienie podanie loginu i hasła.
6. Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
7. Dostęp do stacji roboczych lub systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.

IV. Zabezpieczenia programów i baz przetwarzających dane osobowe

1. Dostęp do danych osobowych w programie lub w bazie wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. Zastosowano mechanizm blokady dostępu po kilku nieudanych próbach logowania się.
2. Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
3. Zastosowano mechanizm umożliwiający automatyczną rejestrację identyfikatora użytkownika i datę pierwszego wprowadzenia danych osobowych.

4. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
5. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
6. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
7. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika (automatyczny wygaszacz ekranu po 10 minutach).

V. Procedura dostępu podmiotów zewnętrznych

1. W umowach podpisywanych z podmiotami, które mają dostęp do danych osobowych na terenie Starostwa (np. w umowach zewnętrznej obsługi bhp, umowach serwisowych sprzętu komputerowego itd.) stosuje się klauzule poufności uzgodnione z kancelarią świadczącą obsługę prawną Starostwa.
2. Z podmiotami, które przetwarzają dane osobowe „na zewnątrz" w formie outsourcingu należy zawrzeć umowę powierzenia przetwarzania danych osobowych.

VI. Procedura korzystania z internetu

1. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą ASI.
3. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo.
4. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
5. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:"

VII. Procedura korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych za pomocą poczty elektronicznej poza Starostwo może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania informacji wrażliwych wewnątrz organizacji bądź wszelkich danych osobowych poza organizację należy wykorzystywać mechanizmy kryptograficzne.
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych pocztą elektroniczną zawarł w treści e-maila prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. Nie należy otwierać załączników (plików) w mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.
7. Należy wykazać ostrożność podczas wchodzenia na podane w e-mailach adresy stron internetowych, gdyż często są to odnośniki do stron zainfekowanych lub niebezpiecznych.
8. Użytkownicy nie powinni rozsyłać za pośrednictwem maila informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia", itp.
9. Użytkownicy nie powinni rozsyłać e-maili zawierających załączniki o dużym rozmiarze.
10. Użytkownicy powinni okresowo usuwać niepotrzebne maile.
11. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW".

VIII. Procedura nadawania uprawnień do przetwarzania danych osobowych.

1. Zarządzanie uprawnieniami użytkowników

1. Przyznanie, anulowanie upoważnienia do przetwarzania danych osobowych w systemie informatycznym lub w zbiorze papierowym wraz z uprawnieniami do przetwarzania tych danych wymaga pisemnego upoważnienia udzielonego przez ABI według wzoru stanowiącego załącznik nr 2 do Instrukcji. O udzieleniu upoważnienia informowany jest

ASI celem nadania identyfikatora oraz uprawnień użytkownika w systemach informatycznych i aplikacjach.

2. Przed nadaniem upoważnienia, ABI zobowiązany jest do sprawdzenia, czy osoba upoważniona:
   1) odbyła szkolenie z zakresu przestrzegania zasad bezpieczeństwa danych osobowych lub została zapoznana z polityką bezpieczeństwa danych osobowych i Instrukcją,
   2) podpisała oświadczenie o zachowaniu poufności
   3) będzie przetwarzać dane osobowe w zakresie i celu określonym upoważnieniu
3. Jeśli jest to wymagane, przełożony określa dla osoby upoważnionej jej zakres uprawnień w systemach informatycznych.
4. Każdy użytkownik musi posiadać swój własny indywidualny identyfikator (login).
5. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
6. ABI odpowiada za przechowywanie i aktualizację wszystkich upoważnień
7. ABI opowiada za prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych (wzór ewidencji określa załącznik nr 3 do Instrukcji).

2. Zarządzanie uprawnieniami administratorów

1. Administrator wyznaczony jest poprzez zakres obowiązków lub poprzez zakres umowy z podmiotem pełniącym jego funkcję.
2. Jeżeli jest to możliwe, każdy administrator systemu zobowiązany jest do bieżącej pracy na koncie roboczym. Użycie tzw. konta administracyjnego (np. „root" lub „admin") dopuszczalne jest jedynie w sytuacjach awaryjnych lub podczas poważnych zmian wprowadzanych w administrowanym systemie.
3. Każdy administrator systemu powinien pracować na koncie administratora przypisanym mu osobiście.

IX. Metody i środki uwierzytelnienia

1. Ogólne zasady postępowania z hasłami

1. ASI informuje pisemnie użytkownika o nadaniu pierwszego hasła do systemu.
2. Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła.

3. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
4. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
5. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
6. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.

2. Hasła do programów przetwarzających dane osobowe

1. Hasło dostępu do programu składa się co najmniej z 8 znaków.
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3. Zmiana hasła odbywa się raz na 30 dni.
4. Zmiana hasła jest wymuszana przez system.

3. Hasła administratora

1. Każdy administrator posiada odrębny login i hasło, umożliwiający dostęp do systemów niezależnie od innego administratora.
2. Hasło administratora składa się co najmniej z 10 znaków.
3. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.

X. Procedura rozpoczęcia, zawieszenia i zakończenia pracy

1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła. Każdy użytkownik musi posiadać indywidualny identyfikator. Zabrania się pracy wielu użytkowników na wspólnym koncie.
2. Użytkownik jest zobowiązany do powiadomienia ASI o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
3. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym ASI, który odpowiada za odblokowanie systemu użytkownikowi.

4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych komórek organizacyjnych) wglądu do danych wyświetlanych na monitorach komputerowych.
5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest włączyć ekran blokady komputera lub wylogować się z systemu. Jeżeli tego nie uczyni – po upływie 10 minut system automatycznie aktywuje wygaszacz.
6. Po zakończeniu pracy użytkownik zobowiązany jest:
   1) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
   2) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki (magnetyczne, optyczne, pamięci flash), na których znajdują się dane osobowe.

XI. Procedura tworzenia kopii zapasowych

1. Kopie zapasowe danych tworzone są przez ASI.
2. Procedury wykonywania kopii zapasowych opisane są w załączniku nr 4 do Instrukcji.
3. Kopie przechowywane są w innym pomieszczeniu.
4. ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.

XII. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji i wydruków

1. Zabezpieczenie elektronicznych nośników informacji

1. Nośniki danych (dyski twarde, płyty CD/DVD, pendrive'y), na których zapisane są dane osobowe są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).
2. Zabrania się wynoszenia poza budynki Starostwa wymiennych nośników informacji, a w szczególności twardych dysków z zapisanymi danymi osobowymi i pendrive bez zgody ASI.

3. Dane osobowe wynoszone poza budynki Starostwa na nośnikach elektronicznych muszą być zaszyfrowane.
4. W sytuacji przekazywania nośników z danymi osobowymi na zewnątrz można stosować należy zasady bezpieczeństwa:
   1) adresat powinien zostać uprzednio powiadomiony o przesyłce,
   2) dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą,
   3) nośniki powinny być umieszczone w bezpiecznych kopertach depozytowych,
   4) przesyłkę należy przesyłać przez kuriera.
5. Osoby wykorzystujące nośniki zobowiązane są do niezwłocznego i trwałego usuwania (kasowania) danych osobowych po ustaniu celu ich przechowywania chyba, że na podstawie odrębnych przepisów należy te dane zachowywać.
6. Podlegające likwidacji uszkodzone lub przestarzałe nośniki a szczególności twarde dyski z danymi osobowymi są komisyjnie niszczone w sposób fizyczny. Wzór protokołu zniszczenia stanowi załącznik nr 5 do Instrukcji.
7. Nośniki informacji zamontowane w sprzęcie IT a w szczególności twarde dyski z danymi osobowymi powinny być wymontowane lub wyczyszczone specjalistycznym oprogramowaniem, zanim zostaną przekazane poza Starostwo (np. sprzedaż lub darowizna komputerów stacjonarnych / laptopów).
8. Osoby wykorzystujące elektroniczne nośniki z danymi osobowymi są zobowiązane do zabezpieczeniach ich (w szafach, biurkach) przed dostępem osób nieupoważnionych, szczególnie poza godzinami pracy.

2. Zabezpieczenie kopii zapasowych

Zabezpieczenie kopii zapasowych opisane jest w procedurach tworzenia kopii zapasowych.

3. Zabezpieczenie dokumentów i wydruków

1. Dokumenty i wydruki trwałe z danymi osobowymi przechowuje się w archiwum lub w zabezpieczonych fizycznie pomieszczeniach, biurkach i szafach.
2. Pracownicy są zobowiązani do zabezpieczania dokumentów przed dostępem osób nieupoważnionych podczas swojej nieobecności w pomieszczeniach lub po zakończeniu pracy.

3. Zabrania się pozostawiania wydruków oraz ksero na drukarkach, skanerach i kserokopiarkach bez nadzoru.
4. Niszczenie dokumentów zawierających dane osobowe, w tym wydruków tymczasowych musi odbywać się z użyciem niszczarek.
5. Za zapewnienie bezpieczeństwa dokumentów i wydruków odpowiedzialni są kierownicy właściwych komórek organizacyjnych oraz podległe im osoby przetwarzające dane osobowe.

XIII. Procedura zabezpieczenia systemu informatycznego, w tym przed wirusami komputerowymi

1. Ochrona antywirusowa

1. Za zaplanowanie i zapewnienie ochrony antywirusowej odpowiada ASI, w tym za zapewnienie odpowiedniej ilości licencji programu antywirusowego dla użytkowników.
2. System antywirusowy zainstalowano na stacjach roboczych.
3. System antywirusowy zapewnia ochronę: systemu operacyjnego, przechowywanych plików, poczty wychodzącej i przychodzącej.
4. ASI zapewnia stałą aktywność programu antywirusowego. Tzn. program antywirusowy musi być aktywny podczas pracy systemu informatycznego przetwarzającego dane osobowe.
5. Aktualizacja definicji wirusów odbywa się automatycznie przez system. W przypadku stwierdzenia pojawienia się wirusa lub problemów z aktualizacją sygnatur antywirusowych, każdy użytkownik winien powiadomić ASI.

2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

1. Za zaplanowanie, konfigurowanie, aktywowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku sieci lokalnej i sieci rozległej odpowiada ASI.
2. Stosowany jest firewall sprzętowy, programowy na serwerze i na stacjach roboczych.
3. Zastosowano mechanizmy kontroli dostępu do sieci bezprzewodowej.
4. Zastosowano mechanizmy monitorujące przeglądanie internetu przez użytkowników. Uwzględniają one:
   1) blokowanie stron internetowych określonego typu

2) blokowanie określonych stron internetowych

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

1. System przetwarzający dane osobowe udostępniane odbiorcom musi umożliwiać rejestrację:
   1) nazwy jednostki organizacyjnej lub imienia i nazwiska osoby, której udostępniono dane,
   2) zakresu udostępnianych danych,
   3) daty udostępnienia.
2. Dane osobowe udostępnia się odbiorcy danych na pisemny wniosek ze wskazaniem przez odbiorcę podstawy prawnej legalizującej przetwarzanie danych osobowych.
3. Zgody na udostępnienie danych udziela ABI.
4. ABI odpowiada za udostępnienie danych osobowych w sposób zgodny z ich przeznaczeniem.

XV. Procedura wykonywania przeglądów i konserwacji

1. Przeglądy i konserwacje systemu informatycznego i aplikacji

1. ASI odpowiada za bezawaryjną pracę systemu IT, w tym: stacji roboczych, aplikacji serwerowych, baz danych, poczty elektronicznej.
2. Przegląd i konserwacja systemu informatycznego powinny być wykonywane w terminach określonych przez producentów systemu lub zgodnie z harmonogramem ASI, jednak nie rzadziej, niż raz w roku.
3. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.
4. ASI odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków.
5. ASI odpowiada za sprawdzanie poprawności działania systemu IT, w tym: stacji roboczych, serwerów, baz danych, poczty elektronicznej.
6. ASI odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich usunięcia.

7. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.
8. Czynności konserwacyjne i naprawcze wykonywane doraźnie przez osoby nie posiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych), muszą być wykonywane pod nadzorem osób upoważnionych.
9. Przed przekazaniem uszkodzonego sprzętu komputerowego z danymi osobowymi do naprawy poza teren organizacji, należy:
   1) wymontować nośniki z danymi osobowymi,
   2) trwale usunąć dane osobowe z użyciem specjalistycznego oprogramowania,
   3) nadzorować proces naprawy przez osobę upoważnioną przez administratora systemu, gdy nie ma możliwości usunięcia danych z nośnika.

2. Aktualizacje oprogramowania

ASI odpowiada za aktualizację oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki).

3. Dziennik administratora

ASI dokumentuje pracę w dzienniku administratora, którego wzór stanowi załącznik nr 6 do Instrukcji.

Wykaz załączników do Instrukcji:

1. „Regulamin użytkowania komputerów przenośnych"
2. Wzór upoważnienia do przetwarzania danych osobowych
3. Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych
4. Procedury wykonywania kopii zapasowych
5. Wzór protokołu zniszczenia nośników
6. Wzór dziennika administratora

Załącznik nr 1 do Instrukcji

Regulamin użytkowania komputerów przenośnych

1. Każdy użytkownik komputera przenośnego winien zapoznać się z Regulaminem użytkowania komputerów przenośnych oraz pisemnie zobowiązać się do jego przestrzegania.
2. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę pracodawcy, użytkownik zobowiązany jest do ich przechowywania na dysku szyfrowanym, zabezpieczonym co najmniej 8 znakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).
3. Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę pracodawcy.
4. W przypadku kradzieży lub zgubienia komputera przenośnego, użytkownik powinien natychmiast powiadomić o tym ASI, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.
5. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:
   1) zaleca się przenoszenie go w specjalnym futerale,
   2) zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru,
   3) podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego pod tylnym siedzeniem kierowcy.
6. W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, użytkownik jest zobowiązany do stosowania kabla zabezpieczającego. W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, targów itp.
7. W przypadku pozostawiania komputerów przenośnych w biurze zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach.
8. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, CD, DVD).

Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.

9. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

Załącznik nr 2 do Instrukcji

Egz. nr ...

Puck, dnia .....

U P O W A Ż N I E N I E N R .....

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2016 r. poz. 922)

upoważniam:

Panią/Pana .....

do przetwarzania danych osobowych znajdujących się w zbiorach i ewidencjach prowadzonych przez Starostwo Powiatowe w Pucku w zakresie w jakim jest to niezbędne do wykonywania obowiązków służbowych. Upoważnienie to obejmuje również uprawnienie do przetwarzania danych osobowych w systemie informatycznym Starostwa Powiatowego w Pucku.

Upoważnienie niniejsze zostaje udzielone na czas nieoznaczony z tym, że wygasa ono z chwilą wcześniejszego ustania stosunku pracy Pani/Pana..... w Starostwie Powiatowym w Pucku.

Załącznik nr 3 do Instrukcji

Ewidencja upoważnień do przetwarzania danych osobowych

L.p.	Nazwisko	Imię	Stanowisko służbowe	Data udzielenia	Czas na jaki zostało udzielone	Zakres udzielonego upoważnienia lub pełnomocnictwa	Numer
1							
2							
3							
4							
5							
6							
7							
8							
9							

Załącznik nr 5 do Instrukcji

.... dnia .....r.
(akceptacja powołującego komisję)

Protokół nr .....
zniszczenia uszkodzonych nośników komputerowych
.....
(jednostka, komórka organizacyjna)

Dnia ..... komisja powołana przez .....
(data) (imię, nazwisko i stanowisko osoby powołującej komisję)

w składzie:
1. Przewodniczący: .....
2. Członkowie: .....
.....

dokonała trwałego zniszczenia nośników komputerowych:

L.p.	Nazwa	Nr ewidencyjny	Sposób zniszczenia	Uwagi

Dokonanie w/w czynności zostaje potwierdzone własnoręcznymi podpisami członków komisji:

.....

.....

.....

Załącznik nr 6 do Instrukcji

DZIENNIK PRACY ADMINISTRATORA

L.p.	Data	Godzina	Opis wydarzenia	System TI	Podpis administratora	Uwagi