Zarządzenie Nr 8/2018
Starosty Aleksandrowskiego
z dnia 16 marca 2018 roku

w sprawie wprowadzenia polityki bezpieczeństwa przetwarzania danych osobowych oraz instrukcji zarządzania systemami informatycznymi w Starostwie Powiatowym w Aleksandrowie Kujawskim.

Na podstawie art.36 oraz art.36a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz.922 ze zm.) 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) w związku z art.35 ust.2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2017r. , poz. 1868) , zarządza się, co następuje:

§ 1.1. W Starostwie Powiatowym w Aleksandrowie Kujawskim wprowadza się dla zapewnienia ochrony przetwarzania danych osobowych:
1)Politykę bezpieczeństwa przetwarzania danych osobowych – stanowiącą załącznik nr 1 do niniejszego zarządzenia,
2)Instrukcję zarządzania systemami informatycznymi -stanowiącą załącznik nr 2 do niniejszego zarządzenia,
3) Instrukcję postepowania w przypadku naruszenia bezpieczeństwa danych osobowych - stanowiącą załącznik nr 3 do niniejszego zarządzenia.
4) Instrukcję korzystania ze służbowych komputerów w tym urządzeń przenośnych - stanowiącą załącznik nr 4 do niniejszego zarządzenia.
5) Instrukcję korzystania z poczty elektronicznej i innych elektronicznych systemów komunikacyjnych - stanowiącą załącznik nr 5 do niniejszego zarządzenia.

2. Dokumentacja, o jakiej mowa w ust.1 ma zastosowanie do wszystkich stanowisk pracy, gdzie przetwarzane są dane osobowe.

§ 2.1. Z treścią dokumentów, o których mowa w § 1 ust.1 zobowiązani są zapoznać się wszyscy pracownicy Starostwa Powiatowego w Aleksandrowie Kujawskim przetwarzający dane osobowe.

2. Zobowiązuje się wszystkich pracowników Starostwa Powiatowego w Aleksandrowie Kujawskim do przestrzegania zasad wynikających z dokumentów, o których mowa w § 1 ust.1.

§ 3.Traci moc Zarządzenie Nr 30/2006 Starosty Aleksandrowskiego z dnia 22 grudnia 2006r. w sprawie wprowadzenia Instrukcji ochrony danych osobowych w Starostwie Powiatowym w Aleksandrowie Kujawskim.

§ 4.Wykonanie zarządzenia powierza się Sekretarzowi Powiatu.

§ 5.Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA ALEKSANDROWSKI

STAROSTA ALEKSANDROWSKI
Dariusz Wochna

Sprawdz. pod wzgl. formaln.-prawnym:
RADCA PRAWNY Anna [illegible]
Toruń, 2018 - 03 - 16

Notatka służbowa z dnia 16.03.2018 r.

W sprawie umieszczenia na stronie internetowej BIP Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemami Informatycznymi w Starostwie Powiatowym w Aleksandrowie Kujawskim.

Zgodnie z zalecaniami GIODO opublikowanymi na stronie https://www.giodo.gov.pl/pl/222/9906 (wydruk załączono do notatki) dokumenty Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemami Informatycznymi należy traktować jako dokumenty wewnętrzne udostępniane jedynie ograniczonemu kręgowi osób, np. tylko tym osobom, którym są niezbędne w związku z powierzonymi im zadaniami.

Osoby, które dysponują wiedzą dotyczącą sposobów zabezpieczenia danych, są zobowiązane te informacje zachować w tajemnicy - zgodnie z art. 39 ust. 2 ustawy o ochronie danych osobowych, a te informacje znajdują się w/w dokumentach.

Administrator
Bezpieczeństwa Informacji
Dariusz Podsiedlak

Nie wolno ujawniać dokumentacji związanej z zabezpieczaniem informacji i danych osobowych

Polityka bezpieczeństwa i Instrukcja zarządzania systemem informatycznym to dokumenty wewnętrzne, które powinny być udostępniane jedynie ograniczonemu kręgowi osób.

Wiele podmiotów często myli dokumenty określające politykę przetwarzania danych osobowych z dokumentami wewnętrznymi określającymi politykę bezpieczeństwa. Tymczasem to dwa różne zestawy informacji, służące zupełnie innym celom.

Polityka przetwarzania danych osobowych (Polityka prywatności)

Polityka przetwarzania danych nazwana tutaj „Polityką przetwarzania danych osobowych" to dokument, w którym administrator danych wskazuje cel, podstawy prawne i zakres przetwarzania danych osobowych, a także informacje o podmiotach, którym dane mogą być udostępnione oraz o prawach przysługujących osobom, których dane są przetwarzane (w zakresie, o których mowa w rozdziale 4 ustawy o ochronie danych osobowych i odpowiednio

(https://www.giodo.gov.pl/photos/thumb/thumb_w1024 /data/gallery/9906/_org/12040.jpg)

rozdziale III rozporządzenia o ochronie danych osobowych). Dokument taki może np. zawierać odesłanie do formularza na stronie internetowej, za pomocą którego można zwrócić się o informacje lub np. wycofać zgodę na przetwarzanie swoich danych. **Dokumenty tego typu nazywane w praktyce „politykami prywatności" udostępniane powinny być każdej zainteresowanej osobie.** Dobrą praktyką jest również publikowanie ich na stronach internetowych administratorów danych, co świadczy m.in. o transparentności działania i umożliwia osobom zainteresowanym, w tym potencjalnym klientom czy interesantom, zapoznanie się szczegółowymi informacjami na temat przetwarzania danych osobowych przez dany podmiot.

Polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym

Natomiast dokument określany jako „Polityka bezpieczeństwa" **służy** wskazaniu środków bezpieczeństwa i procedur bezpiecznego przetwarzania informacji, w tym danych osobowych. Jest opracowywany w związku z koniecznością wypełnienia obowiązku w zakresie udokumentowania stosowanych przez administratora danych osobowych środków technicznych i organizacyjnych, mających na celu zapewnienie ochrony przetwarzanym danym przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Zgodnie z przepisami wykonawczymi do ustawy o ochronie danych osobowych (http://www.giodo.gov.pl/233/id_art/1002/j/pl/), w Polityce bezpieczeństwa należy zamieścić m.in. wykaz zabezpieczeń fizycznych i technicznych, miejsc, gdzie dane są przetwarzane oraz programów zastosowanych do przetwarzania danych osobowych. Udostępnianie na zewnątrz takich informacji może osłabić ich skuteczność przez co zagraża właściwej ochronie danych osobowych. Zapoznanie osób trzecich ze szczegółami rozwiązań w zakresie bezpieczeństwa danych i architekturą systemów zastosowanych do ich przetwarzania może ułatwić przestępcom komputerowym ingerencję w te systemy (np. zatrzymania pracy lub niekontrolowaną modyfikację systemu, przejęcie, zniekształcenie lub usunięcie danych w nim zawartych) poprzez ominięcie zastosowanych zabezpieczeń lub ich „złamanie". Polityka bezpieczeństwa powinna być zatem dokumentem o charakterze wewnętrznym, a **osoby, które dysponują wiedzą dotyczącą sposobów zabezpieczenia danych, są zobowiązane te informacje zachować w tajemnicy - zgodnie z art. 39 ust. 2 ustawy o ochronie danych osobowych.**

Podobny do „Polityki bezpieczeństwa" charakter w zakresie dostępności ma dokument określony w tym samym rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (http://www.giodo.gov.pl/233/id_art/1002/j/pl/) jako „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych". Zawarte w tym dokumencie informacje powinny być udostępniane selektywnie tylko tym osobom, którym są one potrzebne dla wykonywania powierzonych im zadań. Na przykład informacje dotyczące procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu powinny być udostępniane wszystkim użytkownikom, zaś procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania powinny być udostępniane tylko administratorom systemów odpowiedzialnym za ich wykonywanie. Podsumowując, należy przyjąć zasadę, że **dokumenty takie jak Polityka bezpieczeństwa i Instrukcja zarządzania systemem informatycznym należy traktować jako dokumenty wewnętrzne udostępniane jedynie ograniczonemu kręgowi osób,** np. tylko tym osobom, którym są niezbędne w związku z powierzonymi im zadaniami.

Zalecenia zawarte w normie ISO/IEC 27002:2013

W opinii GIODO, warto zwrócić uwagę na to, że przyjęta wyżej zasada dotycząca udostępniania dokumentów zawierających informacje o stosowanych środkach i procedurach bezpieczeństwa jest spójna z zaleceniami normy

ISO/IEC 27002:2013 zatytułowanej „Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji". W normie tej zaleca się, aby polityka bezpieczeństwa na najwyższym poziomie zawierała: definicję bezpieczeństwa informacji, celów i zasad kierowania wszystkimi działaniami związanymi z bezpieczeństwem informacji; ogólną i szczegółową odpowiedzialność w zakresie zarządzania bezpieczeństwem *informacji przypisaną do określonych stanowisk; jak również procesy obsługi odstępstw i wyjątków. Zaleca się* ponadto, aby na niższym poziomie politykę bezpieczeństwa informacji wspierały różne polityki tematyczne odpowiednio dostosowane do specyfiki poszczególnych operacji przetwarzania.

W normie tej zaleca się, aby polityki bezpieczeństwa udostępnione były pracownikom organizacji oraz **odpowiednim** podmiotom zewnętrznym (np. podmiotom z którymi organizacja współpracuje i w związku z tym udostępnia jej niektóre funkcje systemu przetwarzania informacji). W odniesieniu do polityk, które przekazywane są na zewnątrz organizacji wymaga się zachowania ostrożności, aby nie ujawniać w nich informacji poufnych, w tym takich jak rodzaj i konfiguracja stosowanych zabezpieczeń, za których administrowanie i monitorowanie odpowiedzialny jest administrator danego systemu.

Błędy w udostępnianiu dokumentacji

W praktyce zdarza się, że administratorzy danych udostępniają swoją politykę bezpieczeństwa, np. poprzez zamieszczenie ich na stronie internetowej. Dzieje się tak zwłaszcza w sytuacjach, gdy polityka bezpieczeństwa oprócz elementów wskazanych w przepisach wykonawczych do ustawy o ochronie danych osobowych zawiera też *np. opis podstawy prawnej, zakresu, sposobu pozyskiwania i celu przetwarzania danych osobowych* i administratorzy chcą powiadomić o tych okolicznościach osoby, których dane dotyczą. Jednak cel ten należy osiągnąć innymi sposobami, które nie powodują ujawniania szczegółowych rozwiązań dotyczących zabezpieczenia danych osobowych. GIODO zaleca, aby w tym celu przygotować odrębny dokument, który będzie zawierał tylko te informacje, które przeznaczone są do publicznego udostepnienia.

Z doświadczeń GIODO wynika również, że problem przekazywania na zewnątrz Polityki bezpieczeństwa w przypadku podmiotów publicznych może być związany z udostępnianiem jej jako informacji publicznej w rozumieniu przepisów ustawy o dostępie do informacji publicznej.

Przypadki żądania udostępnienia Polityki bezpieczeństwa na podstawie ustawy o dostępie do informacji publicznej były przedmiotem orzeczeń sądów administracyjnych. W wyroku z 8 grudnia 2005 r. (sygn. akt II SA/WA 1539/05, publik. LexPolonica, „Rzeczpospolita" 2005, nr 289, s. C5.), Wojewódzki Sąd Administracyjny w Warszawie wskazał, że biorąc pod uwagę wymaganą przepisami prawa zawartość polityki bezpieczeństwa nie powinna być ona udostępniana publicznie. W ocenie WSA, elementy polityki bezpieczeństwa mają charakter informacji niejawnych i w związku z tym ich udostępnienie podlega ograniczeniu, zgodnie z art. 5 ust. 1 ustawy o dostępie do informacji publicznej. W wyroku z 26 października 2015 r. (sygn. akt II SA/Wa 1135/15 (http://orzeczenia.nsa.gov.pl /doc/4F537DCAB0)) w odniesieniu do innego wniosku o udostępnienie informacji publicznej Sąd wskazał, że „dokument Polityka Bezpieczeństwa Systemu Informatycznego PESEL-SAD wersja [...] podlega szczególnej ochronie, jako że jego ujawnienie może mieć szkodliwy wpływ na wykonywanie zadań m.in. w zakresie właśnie bezpieczeństwa publicznego, czy wymiaru sprawiedliwości. (...) nieuprawniony dostęp do żądanego dokumentu, mógłby nieść ze sobą zagrożenie dla praw i wolności obywateli, ich bowiem dane osobowe w tym systemie, którego dotyczy dokument, są przetwarzane w ramach wykonywania ustawowych zadań".

Załącznik nr 3
do Zarządzenia nr 8/2018 Starosty Aleksandrowskiego
z dnia 16 marca 2018r

Starostwo Powiatowe w Aleksandrowie Kujawskim

INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Data i miejsce sporządzenia dokumentu:	Aleksandrów Kujawski, 12.03.2018
Data aktualizacji dokumentu:	
Wydanie:	pierwsze
Ilość stron:	9
Opracował:	Dariusz Podsiedlak

§1

Celem instrukcji jest określenie sposobu postępowania gdy:

1. Stwierdzono naruszenie zabezpieczeń danych osobowych.
2. W przypadku danych przetwarzanych w formie tradycyjnej stan pomieszczeń, szaf, okien, drzwi, dokumentów lub inne zaobserwowane symptomy mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.
3. W przypadku danych przetwarzanych w formie elektronicznej stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu, jakość komunikacji lub inne zaobserwowane symptomy mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.

§2

Instrukcja określa zasady postępowania wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych w przypadku naruszenia bezpieczeństwa tych danych, zgodne z „Tabelą form naruszeń bezpieczeństwa danych osobowych", stanowiącą załącznik A do niniejszej instrukcji.

§3

Naruszeniem zabezpieczenia danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia lub usunięcia, a w szczególności:

a) nieautoryzowany dostęp do danych,

b) nieautoryzowane modyfikacje lub zniszczenie danych,

c) udostępnienie danych nieautoryzowanym podmiotom,

d) nielegalne ujawnienie danych,

e) pozyskiwanie danych z nielegalnych źródeł.

§4

1. W przypadku stwierdzenia naruszenia zabezpieczeń lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych w Starostwie Powiatowym w Aleksandrowie Kujawskim jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie zgłosić ten fakt bezpośredniemu przełożonemu, Administratorowi Bezpieczeństwa Informacji

lub Administratorowi Danych Osobowych, a następnie postępować stosownie do podjętej przez niego decyzji.

2. Zgłoszenie naruszenia zabezpieczeń danych osobowych powinno zawierać:
   a) opisanie symptomów naruszenia zabezpieczeń danych osobowych,
   b) określenie sytuacji i czasu w jakim stwierdzono naruszenie zabezpieczeń danych osobowych,
   c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia,
   d) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

§5

Administrator Bezpieczeństwa Informacji lub inna upoważniona przez niego osoba podejmuje wszelkie działania mające na celu:

a) minimalizację negatywnych skutków zdarzenia,
b) wyjaśnienie okoliczności zdarzenia,
c) zabezpieczenie dowodów zdarzenia,
d) umożliwienie dalszego bezpiecznego przetwarzania danych.

§6

W celu realizacji zadań wynikających z niniejszej instrukcji Administrator Bezpieczeństwa Informacji lub inna upoważniona przez niego osoba ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:

a) żądania wyjaśnień od pracowników,
b) korzystania z pomocy konsultantów,
c) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

§7

Polecenia Administratora Bezpieczeństwa Informacji lub innej upoważnionej przez niego osoby wydawane w celu realizacji zadań wynikających z niniejszej instrukcji są priorytetowe i winny być wykonywane przed innymi poleceniami, zapewniając ochronę danych osobowych.

§8

Odmowa udzielenia wyjaśnień lub współpracy z Administratorem Bezpieczeństwa Informacji lub inną upoważnioną przez niego osobą traktowana będzie jako naruszenie obowiązków pracowniczych.

§9

Administrator Bezpieczeństwa Informacji po zażegnaniu sytuacji naruszającej bezpieczeństwo danych osobowych opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości. Wzór raportu stanowi załącznik B do niniejszej instrukcji.

§10

Nieprzestrzeganie zasad postępowania określonych w niniejszej instrukcji stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.

§11

Jeżeli skutkiem działania określonego w §10 jest ujawnienie informacji osobie nieupoważnionej, sprawca może zostać pociągnięty do odpowiedzialności karnej wynikającej z przepisów Kodeksu Karnego.

§12

Jeżeli skutkiem działania określonego w §10 jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz Prawa Cywilnego.

STAROSTA
ALEKSANDROWSKI
Dariusz Wachna

Załącznik A
do „Instrukcji postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych"

Tabela form naruszeń bezpieczeństwa danych osobowych

Kod naruszenia	Formy naruszeń	Sposób postępowania
A	Forma naruszenia ochrony danych osobowych przez pracownika zatrudnionego przy przetwarzaniu danych	
A.1	W zakresie wiedzy:	
A.1.1	Ujawnianie sposobu działania aplikacji i systemu jej zabezpieczeń osobom niepowołanym	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić Administratora Bezpieczeństwa Informacji.
A.1.2	Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić Administratora Bezpieczeństwa Informacji.
A.1.3	Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić Administratora Bezpieczeństwa Informacji.
A.2	W zakresie sprzętu i oprogramowania	
A.2.1	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych	Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport.
A.2.2	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji. Sporządzić raport.
A.2.3	Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych i sieci	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji. Sporządzić raport.
A.2.4	Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji. Sporządzić raport.

	danych osobowych przez osoby nie będące pracownikami	
A.2.5	Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymieniona czynność, aby jej zaniechała. Wezwać służby informatyczne w celu odinstalowania programów. Sporządzić raport.
A.2.6	Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę popełniającą wymieniona czynność, aby jej zaniechała. Sporządzić raport.
A.2.7	Odczytywanie dyskietek i innych nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność, aby zaczęła stosować się do wymogów bezpieczeństwa pracy. Wezwać służby informatyczne w celu wykonania kontroli antywirusowej. Sporządzić raport.

A.3	W zakresie dokumentów i obrazów zawierających dane osobowe	
A.3.1	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru	Zabezpieczyć dokumenty. Sporządzić raport.
A.3.2	Przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń sporządzić raport.
A.3.3	Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport.
A.3.4	Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Sporządzić raport.
A.3.5	Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane. Sporządzić raport.
A.3.6	Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą.	Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić Administratora Bezpieczeństwa Informacji. Sporządzić raport.
A.3.7	Utrata kontroli nad kopią danych osobowych	Podjąć próbę odzyskania kopii. Powiadomić Administratora Bezpieczeństwa Informacji. Sporządzić raport.
A.4	W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych	

A.4.1	Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych	Zabezpieczyć (zamknąć) pomieszczenie. Powiadomić przełożonych . Sporządzić raport.
A.4.2	Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Powiadomić przełożonych i Administratora Bezpieczeństwa Informacji. Sporządzić raport.
A.4.3	Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakikolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i Administratora Bezpieczeństwa Informacji. Sporządzić raport.
A.5	W zakresie pomieszczeń w których znajdują się komputery centralne i urządzenia sieci.	
A.5.1	Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.)	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i Administratora Bezpieczeństwa Informacji. Sporządzić raport.
A.5.2	Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych lub ignorowania takiego faktu	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i Administratora Bezpieczeństwa Informacji. Sporządzić raport.

B	Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych	
B.1	Ślady manipulacji przy układach sieci komputerowej lub komputerach	Powiadomić niezwłocznie Administratora Bezpieczeństwa Informacji oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.2	Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.3	Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.4	Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.5	Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.6	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe	Postępować zgodnie z właściwymi przepisami. Powiadomić niezwłocznie Administratora Bezpieczeństwa Informacji. Sporządzić raport.
C	Formy naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem	
C.1	Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej	Powiadomić Administratora Bezpieczeństwa Informacji. Sporządzić raport.
C.2	Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika.	Powiadomić Administratora Bezpieczeństwa Informacji. Sporządzić raport.

Załącznik B
do „Instrukcji postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych"

Wzór raportu końcowego sporządzanego przez administratora bezpieczeństwa informacji po zażegnaniu sytuacji naruszającej bezpieczeństwo danych osobowych

Raport o sytuacji naruszenia bezpieczeństwa danych osobowych

Sporządzający raport:

Imię i nazwisko: .....

stanowisko (funkcja) .....

Dział, pokój, nr telefonu .....

Kod formy naruszenia ochrony danych ..... (wg tabeli)

1) Miejsce, dokładny czas i data naruszenia ochrony danych osobowych (piętro, nr pokoju, godzina, itp.):

.....

.....

....

2) Osoby powodujące naruszenie (które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia ochrony danych osobowych):

.....

.....

3) Osoby , które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych osobowych:

.....

.....

4) Informacje o danych, które zostały lub mogły zostać ujawnione:

.....

.....

5) Zabezpieczone materiały lub inne dowody związane z wydarzeniem:

.....

.....

6) Krótki opis wydarzenia związanego z naruszeniem ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania):

.....

.....

7) Wnioski:

.....

.....

....

(miejsce, data i godzina sporządzenia raportu) (podpis sporządzającego raport)

Załącznik nr 4
do Zarządzenia nr 8/2018 Starosty Aleksandrowskiego
z dnia 16 marca 2018r

Starostwo Powiatowe w Aleksandrowie Kujawskim

Instrukcja korzystania ze służbowych komputerów w tym urządzeń przenośnych

1. Komputery i urządzenia przenośne, przekazywane pracownikom Starostwa Powiatowego w Aleksandrowie Kujawskim, mogą być wykorzystywane tylko i wyłącznie do zadań związanych z merytorycznymi zagadnieniami pracy w Starostwie Powiatowym.
2. Przekazanie sprzętu ewidencjonowane jest przez ASI.
3. Komputery i urządzenia przenośne muszą być zabezpieczone hasłem. Polityka haseł jest taka sama jak w Instrukcji Zarządzania Systemami Informatycznymi.
4. Komputery i urządzenia przenośna podlegają szczególnej ochronie. Ich używanie poza siedzibą urzędu musi mieć uzasadnienie w realizowanych przez użytkownika zadaniach. Zgodę na użytkowanie laptopów i urządzeń przenośnych poza siedzibą wydaje, na pisemny umotywowany wniosek, bezpośredni przełożony, na stanie którego znajduje się dany sprzęt.
5. Obowiązek ochrony komputerów przenośnych poza siedzibą urzędu spoczywa na użytkowniku danego komputera. Zabrania się pozostawiania bez opieki tego typu sprzętu w miejscach, gdzie użytkownik nie ma możliwości sprawowania nad nim skutecznej kontroli.
6. Pracownik użytkujący komputer lub urządzenie przenośne nie może instalować na własną rękę żadnego oprogramowania.
7. Jeżeli występuje potrzeba użytkowania laptopa z prawami administratora systemu, użytkownik zobowiązany jest poinformować o tym wcześniej ASI i otrzymać na to zgodę.
8. W przypadku utraty laptopa użytkownik niezwłocznie powiadamia o tym fakcie swojego bezpośredniego przełożonego, a w przypadku kradzieży, dokonuje również niezwłocznego zgłoszenia popełnienia przestępstwa na policję. W zawiadomieniu użytkownik, poza danymi

ogólnymi. podaje okoliczności utraty komputera oraz opis charakteru utraconych danych, w szczególności w zawiadomieniu należy określić, czy utracone dane miały charakter informacji o danych osobowych,

9. Za utratę lub zniszczenie sprzętu powierzonego do pracy odpowiada dany użytkownik, któremu sprzęt został powierzony.
10. W przypadku przekazywania do użytku zewnętrznego (np. przekazanie innej jednostce), wszystkie składniki sprzętu zawierające nośniki informacji powinny być sprawdzone, czy cala informacja prawnie chroniona oraz licencjonowane oprogramowanie zostały fizycznie usunięte lub bezpiecznie nadpisane. Dotyczy to w szczególności dokumentów zapisanych na tym urządzeniu.
11. Po zakończeniu zadań, do których sprzęt mobilny był przeznaczony, użytkownik zobligowany jest do zwrotu urządzenia. Oddanie sprzętu następuje za pisemnym potwierdzeniem odbioru, po technicznych oględzinach ASI, odpowiedzialnego za ewidencjonowanie sprzętu komputerowego.
12. Poza Urzędem zabrania się korzystania z publicznie dostępnych punktów dostępowych typu HOTSPOT oraz przyłączania do sieci LAN i Wi-Fi. Połączenie urządzenia przenośnego do sieci Internet powinno odbywać się tylko przez służbowe modemy mobilne.
13. Zabrania się korzystania z prywatnych nośników pamięci, a w szczególności kopiowania danych osobowych w celu pracy w domu.
14. Zabrania się korzystania z prywatnych komputerów i urządzeń przenośnych w celu przetwarzania danych osobowych zawartych w zbiorach Starostwa Powiatowego.
15. Zabrania się przyłączania prywatnych komputerów i urządzeń przenośnych do wewnętrznej sieci LAN urzędu.
16. Dozwolone jest korzystanie z służbowych przenośnych nośników pamięci ewidencjonowanych przez ASI, dane w nim przechowywane powinny być zabezpieczone kryptograficznie.

STAROSTA
ALEKSANDROWSKI
Dariusz Wochna

Załącznik nr 5
do Zarządzenia nr 8/2018 Starosty Aleksandrowskiego
z dnia 16 marca 2018r

Starostwo Powiatowe w Aleksandrowie Kujawskim

Instrukcja korzystania z poczty elektronicznej i innych elektronicznych systemów komunikacyjnych

1. Wszyscy pracownicy Starostwa Powiatowego mają dostęp do wewnętrznej poczty elektronicznej.

2. Poczta elektroniczna służy wyłącznie do celów służbowych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów teleinformatycznych Starostwa Powiatowego podlega rejestrowaniu i może być monitorowana. Informacje przesyłane za pośrednictwem sieci Starostwa Powiatowego (w tym do i z Internetu) nie stanowią własności prywatnej użytkownika.

3. Użytkownicy są świadomi, że wiadomości elektroniczne niezwiązane z działalnością Starostwa Powiatowego, a zawierające słowa bądź temat uznane za niedozwolone, zgodnie z zasadami filtrowania komunikacji niepożądanej obowiązującymi w Starostwie Powiatowym, będą zatrzymywane i następnie usuwane z systemu pocztowego.

4. Jedynym sposobem korzystania ze służbowej poczty elektronicznej poza wewnętrzną siecią teleinformatyczną Starostwa Powiatowego jest dostęp poprzez przeglądarkę internetową do dedykowanego serwisu.

5. Zalecanym formatem przesyłanych wiadomości jest „zwykły tekst". O ile nie jest to konieczne, nie należy tworzyć wiadomości w formacie HTML.

6. Użytkownicy obowiązani są do okresowego porządkowania i usuwania wiadomości zbędnych z folderów programu pocztowego tak, aby nie dopuścić do jego zablokowania z powodu przekroczenia dopuszczalnej pojemności skrzynki.

7. Zaleca się wysyłanie poczty zawierającej dane osobowe w formie zabezpieczonej hasłem np. poprzez kompresję do pliku ZIP.

8. Zabronione jest:

a) rozsyłanie z komputerów Starostwa Powiatowego oraz przyznanych użytkownikom kont poczty wiadomości, których treść nie jest związana z wykonywaną pracą,
b) wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu),
c) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi Starostwa Powiatowego,
d) odbieranie przesyłek z nieznanych źródeł,
e) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.,
f) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe,
g) ukrywanie lub dokonywanie zmian tożsamości nadawcy,
h) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika,
i) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem,
j) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy,
k) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb Starostwa Powiatowego lub do poszukiwania dodatkowego zatrudnienia.

STAROSTA
ALEKSANDROWSKI
Dariusz Wochna