ZARZĄDZENIE NR 72/2018
STAROSTY CHODZIESKIEGO

z dnia 26 września 2018 r.

w sprawie wprowadzenia "Instrukcji Zarządzania Systemem Informatycznym w Starostwie Powiatowym w Chodzieży".

Na podstawie art. 34 ust. 1 i art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 roku o samorządzie powiatowym (Dz.U. z 2018 r. poz. 995 ze zm.), i art. 24 oraz art. 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych (Dz. U. UE.L z 2016 r. Nr 119, str.1) oraz § 3 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. z 2004 r. Nr 100, poz. 1024) zarzadza się co następuje:

§ 1. W Starostwie Powiatowym w Chodzieży wprowadza się do stosowania: Instrukcję Zarządzania Systemem Informatycznym w Starostwie Powiatowym w Chodzieży stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Wykonanie Zarządzenia powierza się Sekretarzowi Powiatu.

§ 3. Nadzór nad wykonaniem Zarządzenia powierza się Inspektorowi Danych Osobowych.

§ 4. Traci moc załącznik Nr 2 do Zarządzenia Nr 30/08 Starosty Chodzieskiego z dnia 2 kwietnia 2008 r.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
Julian Hermaszczuk

Beata Kapiewska
Radca prawny
Bd P-195

Załącznik do zarządzenia Nr 92/2018
Starosty Chodzieskiego
z dnia 26 września 2018 r.

Instrukcja Zarządzania Systemem Informatycznym Starostwa Powiatowego w Chodzieży

1. Zastosowane w instrukcji określenia oznaczają:
   1) Administrator danych – Starostwo Powiatowe w Chodzieży reprezentowane przez Starostę;
   2) Inspektor Ochrony Danych (IOD) – osoba wyznaczona przez Starostę, w celu sprawowania nadzoru nad przestrzeganiem zasad ochrony przetwarzanych danych;
   3) Administrator systemu informatycznego (ASI) - oznacza osobę wyznaczoną przez Administratora odpowiedzialną za opiekę techniczną i zabezpieczenia Systemu Informatycznego Starostwa Powiatowego w Chodzieży;
   4) Użytkownik - każda osoba zatrudniona w Starostwie Powiatowym w Chodzieży upoważniona do przetwarzania danych osobowych oraz korzystająca lub mająca dostęp do Systemu Informatycznego Starostwa Powiatowego w Chodzieży;
   5) Instrukcja - oznacza niniejszą Instrukcję Zarządzania Systemem Informatycznym Starostwa Powiatowego w Chodzieży;
   6) System Informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
   7) Identyfikator użytkownika - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
   8) Hasło – minimum ośmioznakowy ciąg znaków literowych, cyfrowych, zawierający duże i małe litery oraz znaki specjalne, znany jedynie osobie, której nadano identyfikator użytkownika;
   9) stacja robocza - każdy komputer lub inne urządzenie komputerowe przeznaczone do bezpośredniej pracy (w odróżnieniu od serwera, który tylko udostępnia zdalnie usługi).

2. Instrukcja określa zasady i tryb wykonywania czynności w Systemie Informatycznym Starostwa Powiatowego w Chodzieży związanych z ochroną danych osobowych i składa się z procedur:
   1) Procedura nadawania i cofania uprawnień w Systemie Informatycznym Starostwa Powiatowego w Chodzieży zamieszczona w ust. 3 Instrukcji.
   2) Procedura określająca wymogi oraz sposób użytkowania haseł w Systemie informatycznym zamieszczona w ust. 4 Instrukcji.

3) Procedura rozpoczęcia, zawieszenia i zakończenia pracy dla użytkowników Systemu informatycznego zamieszczona w ust. 5 Instrukcji.
4) Procedura tworzenia kopii zapasowych danych oraz programów i narzędzi programowych służących do przetwarzania danych osobowych w Systemie informatycznym zamieszczona w ust. 6 Instrukcji.
5) Procedura likwidacji nośników cyfrowych zamieszczona w ust. 7 Instrukcji.
6) Procedura określająca metody i częstotliwość sprawdzania obecności szkodliwego/złośliwego oprogramowania służącego do uszkodzenia, przejęcia danych lub kontroli nad Systemem informatycznym przez osobę nieupoważnioną zamieszczona w ust. 8 Instrukcji.
7) Procedura wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych zamieszczona w ust. 9 Instrukcji.
8) Procedura Zarządzania Systemem informatycznym w przypadkach awaryjnych zamieszczona w ust. 10 Instrukcji.
9) Procedura pracy na komputerach przenośnych zamieszczona w ust. 11 Instrukcji.

3. Procedura nadawania i cofania uprawnień w Systemie Informatycznym Starostwa Powiatowego w Chodzieży.

1) Kierownicy wydziałów bądź bezpośredni przełożony (w stosunku do pracowników zatrudnionych na samodzielnych stanowiskach) składają do ASI wniosek o nadanie uprawnień do przetwarzania danych oraz upoważnień do pracy w Systemie Informatycznym Starostwa Powiatowego w Chodzieży, na podstawie, którego Wydział Organizacyjny wyda upoważnienie do przetwarzania danych.
2) Jeden użytkownik może mieć kilka identyfikatorów użytkownika.
3) Identyfikator składa się z ciągu znaków, składających się z imienia i nazwiska. W identyfikatorze pomija się polskie znaki diakrytyczne.
4) Dostęp do Systemu informatycznego ma być możliwy wyłącznie po wprowadzeniu identyfikatora użytkownika i dokonaniu uwierzytelnienia.
5) W przypadku cofnięcia upoważnienia do korzystania z Systemu informatycznego (w tym cofnięcia upoważnienia do przetwarzania danych osobowych):
   - Kierownik komórki organizacyjnej Starostwa zobowiązany jest powiadomić o tym Wydział Organizacyjny;
   - Wyrejestrowania użytkownika z systemu informatycznego dokonuje ASI poprzez unieważnienie bądź zablokowanie identyfikatora i hasła wyrejestrowanego użytkownika oraz podejmuje inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

4. Procedura określająca wymogi oraz sposób użytkowania haseł w Systemie informatycznym.

1) Pierwsze hasło użytkownika do Systemu informatycznego jest zakładane przez ASI oraz inne upoważnione do tego osoby podczas zakładania identyfikatora użytkownika w Systemie informatycznym. Następnie użytkownik musi zmienić hasło wg zasad określonych w punkcie 2.
2) Ustala się następujące zasady tworzenia i funkcjonowania haseł:

a) hasło jest obowiązkowe dla każdego użytkownika posiadającego identyfikator użytkownika w Systemie informatycznym;
b) po założeniu lub zmianie hasła przez ASI lub innej upoważnionej do tego osoby, użytkownik ma obowiązek zarejestrować się do Systemu informatycznego i zmienić hasło;
c) hasło składa się minimalnie z 8 znaków, które nie powinny być łatwe do zidentyfikowania (nie należy używać jako hasła np.: imion, nazwisk, daty urodzenia, identyfikatora w systemie informatycznym, wyrazów lub cyfr będących danymi osobowymi użytkownika lub dotyczących zbioru danych);
d) hasło powinno się składać z małych i wielkich liter, cyfr oraz co najmniej jednego znaku nie będącego literą, ani cyfrą;
e) hasła nie należy nigdzie zapisywać;
f) zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatorem lub hasła innego użytkownika;
g) hasło zmienia się przynajmniej raz z miesiącu;
h) hasła użytkowników muszą być zapisywane w Systemie informatycznym w postaci zaszyfrowanej;
i) hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności;

3) Zmiana hasła, o której mowa w punkcie 2 stanowi podstawowy obowiązek pracownika.

5. <u>Procedura rozpoczęcia, zawieszenia i zakończenia pracy dla użytkowników Systemu informatycznego.</u>
1) Każde zakłócenie w pracy Systemu informatycznego zauważone przez użytkownika wymaga zgłoszenia Administratorowi Systemu Informatycznego.
2) Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwić podgląd).
3) Rozpoczęcie pracy w Systemie informatycznym na stacji roboczej wymaga wykonania następujących czynności:
a) włączenie zasilania stacji roboczej (najczęściej poprzez włączenie listwy zasilającej lub ups);
b) włączenie stacji roboczej;
c) po załadowaniu się systemu operacyjnego – zarejestrowanie się w Systemie informatycznym przy użyciu identyfikatora użytkownika i hasła;
d) po pozytywnym przejściu procedury uwierzytelnienia – uzyskanie dostępu do Systemu informatycznego.
4) Podczas zawieszenia pracy z wykorzystaniem Systemu informatycznego połączonego z jednoczesnym odejściem od stacji roboczej, użytkownik powinien zabezpieczyć stację roboczą przed dostępem osoby nieupoważnionej poprzez zastosowanie wygaszaczy ekranu, zablokowanie stanowiska hasłem lub wyłączenie stacji roboczej.

5) Po zakończeniu pracy na stacji roboczej użytkownik zobowiązany jest:
   a) poprawnie zamknąć wszystkie działające programy i aplikacje;
   b) poprawnie zamknąć systemy operacyjne;
   c) w przypadku gdy stacja robocza nie jest przeznaczona do pracy ciągłej wyłączyć zasilanie (najczęściej poprzez wyłączenie listwy zasilającej lub ups).

6. Procedura tworzenia kopii zapasowych danych oraz programów i narzędzi programowych służących do przetwarzania danych osobowych w Systemie informatycznym.

1) Obowiązuje zakaz robienia kopii całych zbiorów danych. Całe zbiory danych mogą być kopiowane tylko przez ASI lub automatycznie przez system, z zachowaniem procedur ochrony danych.
2) Jednakowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane.
3) Jednostkowe dane mogą być przekazywane pocztą elektroniczną między komputerami Starostwa powiatowego w Chodzieży a komputerami przenośnymi użytkowników tylko po ich zaszyfrowaniu.
4) Obowiązuje zakaz wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz obszernych z nich wypisów, nawet w postaci zaszyfrowanej.
5) Administrator systemu informatycznego jest odpowiedzialny za funkcjonowanie systemu kopii zapasowych oraz objęcie tym systemem wszystkich danych przetwarzanych w Systemie informatycznym jeśli tylko pozwalają na to możliwości techniczne.
6) W przypadku braku możliwości technicznych objęcia części danych systemem kopii zapasowych ASI ustala z użytkownikami sposób, częstotliwość oraz osobę odpowiedzialną za ręczne sporządzanie kopii zapasowej tych danych.
7) Tworzenie kopii zapasowych danych oraz programów i narzędzi programowych służących do ich przetwarzania należy dokonywać z częstotliwością umożliwiającą odtworzenie danych po awarii Systemu informatycznego. Szczegółowy harmonogram tworzenia kopii zapasowych winien być zamieszczony w „Polityce Bezpieczeństwa".
8) Użytkownicy winni przetwarzać dane osobowe w Systemie informatycznym w miejscach zabezpieczonych systemem kopii zapasowych, w innym przypadku zobligowani są do sporządzania osobiście ręcznych kopii zapasowych danych z uwzględnieniem następujących zasad:
   a) Kopie zapasowe należy sporządzać, w zależności od urządzeń obecnych na stanowisku, na następujących nośnikach: płytach CD-R, DVD, zapasowych dyskach twardych, pamięciach przenośnych i innych dostępnych nośnikach cyfrowych będących własnością Starostwa Powiatowego w Chodzieży, z których będzie możliwe poprawne odtworzenie danych w razie awarii systemu informatycznego.

b) Wszystkie wykonane kopie zapasowe Systemu informatycznego powinny być opisane w sposób jednoznacznie określający zawartość kopii, datę i godzinę sporządzenia.

c) Kopie zapasowe należy przechowywać w miejscu wskazanym przez Administratora systemu informatycznego, który jest zobligowany do konsultacji w tym zakresie z Inspektorem ochrony danych.

9) Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym wglądem, przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.

10) Kopii zapasowych nie przechowuje się w tych samych pomieszczeniach, w których są przetwarzane lub przechowywane zbiory danych.

11) Fizyczne nośniki kopii zapasowych przechowuje się w zamykanych szafach.

12) Za sporządzanie kopii zapasowych systemów i danych znajdujących się na serwerach odpowiedzialni są Informatycy oraz inne osoby wyznaczone przez Administratora.

13) W przypadku przekazywania nośników informacji zawierających kopie zapasowe danych osobowych podmiotom zewnętrznym na podstawie zawartych umów celem bezpiecznego ich przechowywania, stosownie wcześniej musi zostać określona procedura przekazywania oraz metody zabezpieczania przekazywania nośników informacji przed dostępem osób nieupoważnionych zarówno podczas transportu, jak i podczas późniejszego przechowywania z zastosowaniem środków ochrony kryptograficznej.

14) Kopie zapasowe należy:

a) okresowo sprawdzać pod kątem dalszej przydatności do odtwarzania danych w przypadku awarii systemu;

b) bezzwłocznie usuwać po ustaniu ich użyteczności.

15) Kopie zapasowe zapisane na nośnikach jednorazowego zapisu, a także na zepsutych nośnikach wielokrotnego zapisu przeznaczonych do likwidacji należy pozbawić zapisu danych w sposób uniemożliwiający ich odtworzenie, to znaczy zniszczyć w odpowiedniej niszczarce lub uszkodzić w trwały sposób zgodnie z procedurą likwidacji nośników cyfrowych określoną w ust. 7 Instrukcji.

7. <u>Procedura likwidacji nośników cyfrowych w tym kart elektronicznych.</u>

1) Nośniki cyfrowe, w tym karty elektroniczne przeznaczone do likwidacji pozbawia się wcześniej zapisu danych na nich zapisanych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.

2) Użytkownicy mogą niszczyć niepotrzebne lub uszkodzone nośniki cyfrowe (z wyłączeniem kart elektronicznych) samodzielnie wyłącznie z użyciem specjalnie do tego przeznaczonych niszczarek, w przeciwnym razie są zobligowani do przekazania nośnika cyfrowego do Informatyków celem likwidacji.

3) Karty elektroniczne po ustaniu ważności należy niezwłocznie przekazywać do Wydziału Organizacyjnego celem likwidacji.

4) Likwidacja dysków twardych oraz kart elektronicznych w Wydziale Organizacyjnym winna zostać potwierdzona w postaci wewnętrznego protokołu likwidacji.

8. Procedura określająca metody i częstotliwość sprawdzania obecności szkodliwego/złośliwego oprogramowania służącego do uszkodzenia, przejęcia danych lub kontroli nad Systemem informatycznym przez osobę nieupoważnioną.
   1) Nadzór nad sprawdzaniem systemu pod kątem obecności szkodliwego/złośliwego oprogramowania prowadzi ASI.
   2) Każdy użytkownik Systemu informatycznego zobowiązany jest do używania w pracy wyłącznie cyfrowych nośników informacji będących własnością Starostwa i przechowywania na nich tylko danych związanych z charakterem pracy.
   3) Nośniki cyfrowe przekazywane Starostwu mogą być użytkowane w Systemie informatycznym wyłącznie po sprawdzeniu ich programem antywirusowym.
   4) Na komputerach stacjonarnych, serwerach i urządzeniach mobilnych należy:
      a) stosować programy antywirusowe monitorujące w czasie rzeczywistym System informatyczny podczas jego pracy oraz skanujące wyżej wymienione maszyny nie rzadziej niż raz na tydzień;
      b) stosować programy przeciwdziałające oprogramowaniu służącemu do przejęcia danych lub kontroli nad systemem informatycznym przez osobę nieuprawnioną.
   5) Programy antywirusowe należy uaktualniać zgodnie z zaleceniami dostawcy programu. Za nadzór nad aktualizacją programów antywirusowych odpowiada ASI.
   6) Procedurę usuwania występujących wirusów komputerowych należy wykonać przy użyciu tylko dopuszczonych do użytkowania programów narzędziowych i antywirusowych.
   7) W celu zabezpieczenia Systemu informatycznego przed atakami szkodliwego/złośliwego oprogramowania ASI wdraża:
      a) identyfikację i uwierzytelnianie użytkowników uzyskujących dostęp do systemu poprzez kontrolę praw dostępu do zasobów systemu informatycznego;
      b) rejestrację informacji o dostępach lub próbach dostępu do zasobów i usług systemu;
      c) rejestrację i śledzenie komunikatów o błędach w pracy systemów informatycznych.

9. Procedura wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.
   1) Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
      a) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie,

b) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawiane są przez podmiot przetwarzający, z którym zawarto umowę powierzenia przetwarzania danych osobowych.

2) Przeglądy i konserwacje Systemu informatycznego służącego do przetwarzania danych, dokonywane przez osoby i podmioty zewnętrzne są możliwe tylko pod warunkiem zawarcia z nimi umowy powierzenia przetwarzania danych osobowych oraz przy obecności ASI lub innej osoby upoważnionej przez Administratora.

10. Procedura Zarządzania Systemem informatycznym w przypadkach awaryjnych.

1) Poprzez przypadek awaryjny należy rozumieć awarię systemu informatycznego służącego do przetwarzania danych osobowych pod nieobecność ASI lub konieczność dokonania czynności administracyjnych przez firmy serwisujące sprzęt i oprogramowanie na podstawie umów z użyciem identyfikatorów i haseł użytkowników systemu.
2) W przypadkach awaryjnych możliwe jest udostępnienie za zgodą Administratora lub osoby przez niego wyznaczonej identyfikatorów i haseł użytkowników uprzywilejowanych (którymi są użytkownicy posiadający uprawnienia na poziomie administratora systemów informatycznych).
3) W przypadku zaistnienia okoliczności określonych w punkcie 2 udostępnienie identyfikatorów i haseł musi odbywać się przy obecności osoby upoważnionej, a po usunięciu awarii hasło musi zostać natychmiast zmienione, lub identyfikator i hasło zablokowane do czasu zmiany hasła.
4) Przypadek awaryjny musi zostać niezwłocznie odnotowany w Systemie informatycznym w postaci notatki służbowej przekazanej Inspektorowi ochrony danych.
5) Identyfikatory i hasła administracyjne do Systemu informatycznego wraz z instrukcją ich użycia w przypadku awaryjnym przechowywane są w zamykanej szafie w Wydziale Organizacyjnym p.109.

11. Procedura pracy na komputerach przenośnych:

1) Użytkownicy, którym zostały powierzone komputery przenośne, powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych; szczególną ostrożność należy zachować podczas ich transportu,
2) Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone,
3) Praca na komputerze przenośnym możliwa jest po wprowadzeniu hasła i indywidualnego identyfikatora użytkownika,
4) Użytkownicy są zobowiązani zmieniać hasła w komputerach przenośnych nie rzadziej niż raz w miesiącu,
5) Pliki zawierające dane osobowe przechowywane na komputerach przenośnych są zaszyfrowane i opatrzone hasłem dostępu,
6) Użytkownicy przetwarzający dane na komputerach przenośnych obowiązani są do systematycznego wprowadzania tych danych w określone miejsca na serwerze

Starostwa Powiatowego, a następnie do trwałego usuwania ich z pamięci powierzonych komputerów przenośnych,

7) Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach przenośnych. Wszelkie zmiany mogą być dokonywane pod nadzorem ASI, stosownie do wymagań niniejszej instrukcji. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zgłosić to ASI.

12. Pozostałe zasady funkcjonowania Systemu informatycznego:

1) Korzystanie z Systemu informatycznego odbywa się za pośrednictwem stanowisk pracy (w szczególności stacji roboczych), do których dostęp jest możliwy wyłącznie pod warunkiem posiadania przez użytkownika identyfikatora użytkownika i hasła do systemu informatycznego.
2) Podczas przekazywania danych osobowych za pomocą urządzeń teletransmisji danych użytkownik powinien:
   a) zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych przed ich udostępnieniem osobom nieupoważnionym w postaci np. identyfikatora i hasła, szyfrowania przesyłanych danych, używania podpisu elektronicznego,
   b) zapewnić kontrolę nad tym jakie dane, kiedy i przez kogo zostały wprowadzone oraz komu są przekazywane.
3) Za nadzór nad bezpieczeństwem przesyłanych danych odpowiedzialny jest ASI lub firma zewnętrzna, z którą Starostwo podpisało umowę na przesył informacji.
4) Komputery, serwery oraz urządzenia, na których jest przetwarzana baza danych oraz serwery służące do przetwarzania danych osobowych muszą posiadać urządzenia podtrzymujące zasilanie wyposażone w oprogramowanie umożliwiające bezpieczne zamknięcie pracujących aplikacji i wyłączenie systemu.
5) Udostępnianie zasobów może odbywać się tylko i wyłącznie w sieciach zabezpieczonych sprzętową lub programową zaporą ogniową (firewall) przed dostępem do publicznej sieci telekomunikacyjnej.
6) W przypadku zdalnego dostępu do systemu i danych lub przesyłania tych danych w publicznej sieci telekomunikacyjnej, należy stosować kryptograficzne środki ochrony wobec danych wykorzystywanych do uwierzytelnienia.
7) Udostępnianie danych osobowych odbiorcom w Systemie informatycznym jest możliwe tylko, jeśli system informatyczny w sposób jednoznaczny i trwały zachowuje informacje o odbiorcy, czasie udostępnienia danych osobowych i zakresie udostępnienia danych osobowych, chyba, że System informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych.

13. Wszystkie procedury, wytyczne i niezbędne instrukcje dotyczące bezpieczeństwa systemu informatycznego zawarte w Polityce Bezpieczeństwa Inspektor ochrony danych przekazuje użytkownikom do wiadomości w zakresie niezbędnym do bezpiecznej pracy w Systemie informatycznym.