ZARZĄDZENIE NR 11
WÓJTA GMINY RACZKI

z dnia 28 lutego 2020 r.

w sprawie wprowadzenia w Urzędzie Gminy Raczki Instrukcji Zarządzania Systemami Informatycznymi Służącymi do Przetwarzania Danych Osobowych

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (t.j. Dz. U. z 2019 r. poz. 506, 1309, 1571, 1696, 1815) w związku z art. 24 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 Wójt Gminy Raczki postanawia co następuje:

§ 1. Wprowadza się Instrukcję Zarządzania Systemami Informatycznymi Służącymi do Przetwarzania Danych Osobowych stanowiącą załącznik do niniejszego Zarządzenia.

§ 2. Zobowiązuje się Sekretarza Gminy do zapoznania pracowników Urzędu Gminy Raczki z treścią Instrukcji.

§ 3. Monitorowanie przestrzegania postanowień zawartych w Instrukcji powierza się Inspektorowi Ochrony Danych.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt

Andrzej Szymulewski

Załącznik do zarządzenia Nr 11

Wójta Gminy Raczki

z dnia 28 lutego 2020 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY RACZKI

Rozdział 1.
1
Postanowienia ogólne

§ 1. Instrukcja określa przepisy mające na celu zapewnienie bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych użytkowanych w Urzędzie.

§ 2. Użyte w instrukcji określenia oznaczają:

1) **aplikacja** - wydzielona i niezależna jednostka oprogramowania użytkowego przystosowana do instalowania i eksploatowania, jako składowa postaci eksploatacyjnej systemu informatycznego;
2) **platforma systemowa** - środowisko eksploatacyjne tworzone przez oprogramowanie systemowe i narzędziowe;
3) **urządzenia** - elementy tworzące infrastrukturę techniczną systemu informatycznego i urządzeń klienckich, a w szczególności:
   a) serwery,
   b) macierze dyskowe i biblioteki taśmowe,
   c) urządzenia aktywne sieci lokalnych i rozległych,
   d) urządzenia komputerowe i urządzenia peryferyjne;
4) **zbiór danych systemu informatycznego** - każda forma przechowywania informacji w systemie informatycznym, a w szczególności:
   a) bazy danych lub systemy plików wykorzystywane przez systemy zarządzania bazami danych, służące do stałego składowania danych,
   b) informacje zarchiwizowane, w szczególności na macierzach, bibliotekach taśmowych oraz na nośnikach magnetycznych oraz magneto - optycznych w celu przechowywania długoterminowego.

Rozdział 2.
2
Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemach informatycznych oraz wskazanie osoby odpowiedzialnej za te czynności

§ 3. 1. Przy nadawaniu uprawnień do przetwarzania danych osobowych w systemach należy stosować dedykowaną do tego procedurę, zgodnie z Polityką Bezpieczeństwa.

2. Do przetwarzania zbiorów danych systemów dopuszcza się wyłącznie osoby uprawnione.

3. Założenie konta użytkownika, nadanie uprawnień, ich modyfikacja lub odwołanie następuje po zatwierdzeniu wniosku odpowiednio przez Wójta Gminy

4. Niedopuszczalna jest praca w systemie na koncie innego użytkownika. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

§ 4. Nadanie lub odebranie uprawnień osobie, która nie jest pracownikiem Urzędu, a która realizuje zadania na podstawie umowy powierzenia przetwarzania danych osobowych zawartej pomiędzy Urzędem, a podmiotem zewnętrznym realizowane jest zgodnie z rozporządzeniem 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).

§ 5. 1. Uprawnienia są niezwłocznie odbierane użytkownikowi, gdy nie są mu niezbędne do wykonywania powierzonych zadań.

2. Inspektor ds. obsługi informatycznej urzędu niezwłocznie blokuje użytkownikowi konto, w przypadku: rozwiązania lub wygaśnięcia stosunku pracy, odwołania jego upoważnienia oraz w sytuacji naruszenia bezpieczeństwa danych.

3. W sytuacji naruszenia bezpieczeństwa przetwarzania zbiorów danych w systemach informatycznych, inspektor ds. obsługi informatycznej urzędu zabezpiecza wszelkie dowody dotyczące zdarzenia.

§ 6. Identyfikator konta użytkownika powinien:

1) składać się z minimum trzech znaków;

2) być niepowtarzalnym w skali systemu;

3) być przypisany tylko do jednego użytkownika.

§ 7. Identyfikator konta użytkownika nie może być zmieniany, a po zablokowaniu konta nie może być wykorzystywany do identyfikowania innego użytkownika.

Rozdział 3.
3
Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 8. 1. Wszystkie systemy przetwarzające dane osobowe w Urzędzie muszą być wyposażone w mechanizmy uwierzytelniania użytkownika oraz kontroli dostępu do danych.

2. Uwierzytelnianie użytkowników systemów Urzędu musi być oparte na unikalnym identyfikatorze i haśle użytkownika.

§ 9. 1. Użytkownik jest zobowiązany zmienić hasło inicjujące pracę w systemie po pierwszym zalogowaniu się do systemu.

2. Hasło do pracy w systemie, tzw. hasło startowe, inicjuje inspektor ds. obsługi informatycznej urzędu w obecności użytkownika, który następnie dokonuje zmiany na własne.

3. Zabrania się użytkownikowi udostępniania swoich haseł innym użytkownikom oraz przełożonym.

4. Hasło użytkownika musi być zmieniane, co najmniej raz na 30 dni.

§ 10. 1. Zobowiązuje się użytkowników do:

1) używania haseł składających się z przemieszanych cyfr, wielkich i małych liter oraz znaków specjalnych, zawierających, co najmniej 8 pozycji;

2) tworzenia hasła nie zawierającego więcej niż jedno powtórzenie tej samej litery lub cyfry;

3) nieużywania, jako hasła identyfikatora użytkownika;

4) nietworzenia hasła mającego związek z danymi osobistymi użytkownika tzn. imieniem, nazwiskiem, przezwiskiem, pseudonimem, datą urodzenia zarówno jego jak i jego najbliższych osób, numerem telefonu, numerem dowodu osobistego, numerem rejestracyjnym samochodu, nazwami rzeczy itp.;

5) nieużywania prostych sekwencji klawiszy, np. qwerty, 123abc;

6) nietworzenia haseł podobnych do haseł używanych poprzednio;

7) niewykorzystywania przykładowych haseł, zapożyczonych z książek omawiających problemy bezpieczeństwa;

8) niestosowania tych samych haseł w kilku systemach.

2. Jeżeli dostęp do danych przetwarzanych w systemach informatycznych posiadają, co najmniej dwie osoby, wówczas należy zapewnić, aby:

1) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;

2) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

Rozdział 4.
4
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

§ 11. Założenie konta użytkownika, nadanie uprawnień, modyfikacja upoważnień użytkownika do systemu odbywa się zgodnie z § 3 Instrukcji.

§ 12. 1. Użytkownicy są zobowiązani do postępowania zgodnego z obowiązującymi instrukcjami, podręcznikami i procedurami dotyczącymi administrowania, eksploatacji i użytkowania systemów oraz stosowania się do zaleceń inspektora ds. obsługi informatycznej urzędu.

2. Na wszystkich urządzeniach dopuszcza się instalację tylko legalnego, licencjonowanego oprogramowania.

3. Zakończenie pracy w systemie służącym do przetwarzania danych osobowych następuje poprzez wylogowanie się z tego systemu.

4. Pomieszczenia lub części pomieszczeń, w których są przetwarzane dane osobowe przy wykorzystaniu systemów, muszą znajdować się w obszarze ograniczonego i kontrolowanego dostępu.

5. Drzwi do pomieszczeń, w których są przetwarzane dane osobowe muszą być wyposażone w zamki.

6. Drzwi do pomieszczeń, w których są przetwarzane dane osobowe muszą być zamykane podczas każdego wyjścia z tych pomieszczeń wszystkich osób w nich pracujących.

7. W pomieszczeniach, w których przetwarzane są dane osobowe, osoby postronne mogą przebywać tylko w obecności osób w nich zatrudnionych.

Rozdział 5.
5
Procedury tworzenia kopii bezpieczeństwa zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

§ 13. 1. Obowiązkowo należy tworzyć kopie bezpieczeństwa następujących plików:

1) platformy systemowej;

2) serwerów aplikacyjnych;

3) baz danych;

4) danych użytkowników.

2. Częstotliwości i sposób tworzenia kopii bezpieczeństwa określone są w dedykowanej do tego procedurze, zawartej w Polityce Bezpieczeństwa Urzędu Gminy Raczki.

3. W procesie tworzenia kopii bezpieczeństwa należy uwzględniać proces starzenia się elektronicznych nośników informacji oraz warunków ich pracy i przechowywania. Zaleca się, w celu zmniejszenia wpływu tego procesu, stosowanie jednej z dwóch zasad wymiany nośnika na nowy:

1) czasowej - po określonym czasie użytkowania;

2) ilościowej - po wykonaniu określonej liczby zapisów.

§ 14. 1. Za sporządzanie kopii bezpieczeństwa zbiorów danych, ich weryfikację i poprawność odczytu odpowiadają bezpośrednio pracownicy wykonujący kopię. Dodatkowo inspektor ds. obsługi informatycznej urzędu wykonuje kopie zapasowe zgodnie z Polityką Bezpieczeństwa Urzędu Gminy.

2. Kopia bezpieczeństwa przechowywana jest na innym dedykowanym do tego celu urządzeniu np. na innym przystosowanym do tego nośniku informacji, w zamykanym pomieszczeniu, poza dostępem osób nieupoważnionych.

3. Bazy z danymi osobowymi, jako kopie bezpieczeństwa na nośnikach, po ustaniu ich użyteczności powinny być z nich usunięte, a gdy nie jest to możliwe, nośniki danych uszkadza się fizycznie, w sposób uniemożliwiający odczytanie zapisanych danych. Z tych czynności inspektor ds. obsługi informatycznej urzędu sporządza protokół/notatkę.

Rozdział 6.
6
Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii bezpieczeństwa

§ 15. Przechowywanie nośników informacji zawierających dane osobowe musi odbywać się w warunkach zapewniających ochronę, znajdujących się na tych nośnikach danych osobowych, przed ich ujawnieniem osobom nieupoważnionym, przejęciem przez osobę nieuprawnioną, nieuprawnioną zmianą, uszkodzeniem lub zniszczeniem.

§ 16. 1. Nośniki informacji przeznaczone do przechowywania danych osobowych muszą charakteryzować się trwałością zapisu, odpowiednią do planowanego okresu przechowywania na nich danych.

2. Warunki środowiskowe pomieszczeń, w których przechowuje się nośniki informacji zawierające dane osobowe, muszą odpowiadać wymaganiom określonym przez ich producenta.

3. Oznaczenie nośników informacji powinno umożliwiać identyfikację zawartości nośnika bez konieczności używania urządzeń do ich odczytu.

§ 17. 1. Za prawidłowość oznakowywania i przechowywania nośników informacji odpowiada wykonujący kopię bezpieczeństwa.

2. Prawidłowość oznakowywania i przechowywania nośników informacji kontrolują kierownicy referatów oraz inspektor ds. obsługi informatycznej urzędu.

§ 18. 1. Pomieszczenia służące do przechowywania kopii bezpieczeństwa powinny być zamykane, a dostęp do nich osób postronnych powinien być ograniczony.

2. Kopie bezpieczeństwa należy przechowywać w sejfach lub odpowiednio zabezpieczonych szafach metalowych.

3. Sejfy i szafy przeznaczone do przechowywania kopii bezpieczeństwa powinny umożliwiać przechowywanie tych kopii w sposób uporządkowany.

4. Dostęp do kopii bezpieczeństwa mogą mieć wyłącznie osoby odpowiedzialne za przechowywanie tych kopii i ich przełożeni.

§ 19. 1. Podczas tworzenia kopii bezpieczeństwa należy dokonywać weryfikacji poprawności zapisu i ich przydatności do odczytu w przyszłości.

2. Weryfikacji poprawności kopii bezpieczeństwa pod kątem ich dalszej przydatności do odtworzenia danych, dokonuje inspektor ds. obsługi informatycznej urzędu.

§ 20. Opakowania, w których przetrzymywane są kopie bezpieczeństwa, powinny zabezpieczać je przed zniszczeniem lub uszkodzeniem oraz powinny być oznaczone w sposób umożliwiający identyfikację nośników zawierających dane osobowe.

Rozdział 7.
7
Usuwanie danych osobowych zapisanych na nośnikach informacji

§ 21. 1. Dane osobowe przechowywane na nośnikach informacji powinny być z nich usuwane (uwzględniając ograniczenia technologiczne) w momencie ustania przyczyn, dla których zostały na tych nośnikach zapisane lub po upływie czasu przewidzianego do ich przechowywania.

2. Dane osobowe zapisane na nośnikach informacji należy usuwać, gdy sprzęt, w którym są zainstalowane jest przekazywany podmiotom nieuprawnionym do dostępu do tych danych.

§ 22. 1. Usunięcia danych zapisanych na nośnikach informacji dokonują osoby, które dysponują tymi nośnikami lub osoby przez nie upoważnione.

2. Usunięcia danych zapisanych na nośnikach informacji, zarówno papierowych jak i elektronicznych, dokonuje się poprzez fizyczne niszczenie nośników informacji lub poprzez modyfikację zapisanych na nośnikach danych, w taki sposób, aby nie było możliwe ustalenie tożsamości osoby, której dane dotyczą.

3. Usunięcie danych zapisanych na papierowych nośnikach informacji poprzez modyfikację można dokonywać zamalowując lub zacierając informacje w taki sposób, aby nie było możliwe ustalenie tożsamości osoby, której dane dotyczą.

4. Niszczenie papierowych nośników informacji w szczególności należy realizować w niszczarce dokumentów.

Rozdział 8.
8
Sposób zabezpieczenia systemu informatycznego przed działalności oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych

§ 23. Za zorganizowanie skutecznego systemu ochrony przed szkodliwym oprogramowaniem w poszczególnych systemach odpowiedzialny jest inspektor ds. obsługi informatycznej urzędu.

§ 24. 1. Oprogramowanie antywirusowe i firewall należy instalować na tych urządzeniach, wchodzących w skład eksploatowanych w Urzędzie systemów, które są narażone na działanie oprogramowania szkodliwego, a w szczególności na tych, które mają dostęp do sieci publicznej Internet.

2. Oprogramowanie antywirusowe i firewall musi być systematycznie aktualizowane. Za aktualność oprogramowania odpowiada inspektor ds. obsługi informatycznej urzędu.

§ 25. 1. Do identyfikowania sytuacji powstawania zagrożeń ze strony szkodliwego oprogramowania oraz przeciwdziałania tym zagrożeniom zobowiązani są wszyscy użytkownicy.

2. Użytkownicy muszą zwracać uwagę na nietypowe zachowania systemu informatycznego, takie jak: nieoczekiwane efekty dźwiękowe, nieznane nowe pliki lub foldery, nagłe zmniejszenie się wolnego miejsca na dysku, niespodziewane komunikaty itp. oraz zgłaszać takie sytuacje do inspektora ds. obsługi informatycznej urzędu.

3. Kontynuowanie pracy przez użytkowników, po wykryciu wirusów komputerowych, jest dopuszczalne tylko wtedy, gdy program antywirusowy automatycznie usunie zagrożenie, bez konieczności interwencji inspektora ds. obsługi informatycznej urzędu.

4. Wypadki wykrycia wirusów komputerowych, które nie dają się usunąć przy pomocy dostępnego oprogramowania antywirusowego, użytkownicy zgłaszają do inspektora ds. obsługi informatycznej urzędu, który odłączają zawirusowane urządzenie od systemu do czasu usunięcia wirusa.

§ 26. 1. Inspektor ds. obsługi informatycznej urzędu, któremu zostało zgłoszone wykrycie szkodliwego oprogramowania komputerowego w systemie, dokonuje jego usunięcia z zainfekowanego urządzenia przy użyciu licencjonowanego oprogramowania antywirusowego, wykonując zalecenia producenta oprogramowania antywirusowego lub własną procedurę naprawczą.

2. Inspektor ds. obsługi informatycznej urzędu jest zobowiązany dokonywać, nie rzadziej niż raz w tygodniu, kontroli antywirusowych całego systemu plików na serwerach poszczególnych systemów informatycznych.

§ 27. Nośniki informacji, wpływające z zewnątrz do jednostek organizacyjnych Urzędu, podlegają obowiązkowej kontroli antywirusowej. W przypadku niezaufanego źródła, kontrolę należy wykonać na odseparowanym od sieci wewnętrznej urządzeniu.

Rozdział 9.
9
Sposób zapewnienia odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia

§ 28. 1. W systemie służącym do przetwarzania danych osobowych odnotowywane są informacje o odbiorcach danych, a w szczególności imię i nazwisko lub nazwa odbiorcy, data udostępnienia oraz zakres udostępnienia.

2. W przypadku, gdy w systemie służącym do przetwarzania danych osobowych nie jest możliwe odnotowywanie takich informacji, wyznaczeni pracownicy, odnotowują w prowadzonych na stanowiskach rejestrach udostępnienia danych osobowych.

Rozdział 10.
10
Procedury dokonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

§ 29. 1. Przeglądy i konserwacje urządzeń realizowane są zgodnie z zaleceniami producenta oraz bieżącymi potrzebami, a także w wypadkach, gdy zostanie stwierdzone naruszenie bezpieczeństwa systemu informatycznego.

2. Przeglądy i konserwacje urządzeń mogą być dokonywane przez inspektora ds. obsługi informatycznej urzędu albo jednostki serwisowe spoza Urzędu w ramach gwarancji producenta, a także przez jednostki serwisowe, z którymi Urząd ma zawarte umowy na świadczenie takich usług.

3. We wszystkich umowach na zakup i serwisowanie sprzętu informatycznego konieczne jest zawarcie klauzuli gwarantującej pozostawienie w Urzędzie nośników danych zawierającego dane, a w szczególności dane osobowe.

Rozdział 11.
11
Sposób postępowania w zakresie komunikacji w sieciach komputerowych

§ 30. W przypadku outsourcingu usług sieci WAN, za zarządzanie siecią odpowiedzialny jest operator sieci, zgodnie z obowiązującą umową na usługi operatorskie sieci WAN.

§ 31. Za zarządzanie komunikacją w sieciach komputerowych Urzędu oraz zapewnienie ciągłego, bezawaryjnego i bezpiecznego ich funkcjonowania odpowiedzialny jest inspektor ds. obsługi informatycznej urzędu.

§ 32. Zabrania się użytkownikom:

1) nawiązywania połączeń lub prób nawiązywania połączeń z systemami, do których obsługi lub użytkowania nie posiadają upoważnień;

2) udostępniania osobistego konta innym osobom;

3) instalowania wszelkiego oprogramowania na komputerach, jeżeli nie posiadają do tego upoważnień.

§ 33. Użytkownik dopuszczony do korzystania z usług systemu Urzędu, musi być przeszkolony przez inspektora ds. obsługi informatycznej urzędu w zakresie:

1) inicjowania pracy komputerów pracujących w sieci (włączanie i wyłączanie komputera, logowanie się do systemu, wylogowanie się z systemu, korzystanie z aplikacji, zmiana i dobór hasła) oraz wykorzystywania urządzeń telekomunikacyjnych;

2) postępowania w wypadku wykrycia awarii lub wystąpienia nietypowych zdarzeń (niemożność zalogowania się, korzystanie przez nieznaną osobę z konta itp.).

§ 34. Inspektor ds. obsługi informatycznej urzędu odpowiedzialny za funkcjonowanie sieci lokalnej dba o właściwy sposób funkcjonowania sieci. Do jego zadań należy w szczególności:

1) reakcja na zgłoszenia użytkowników o nietypowych zachowaniu się eksploatowanego systemu informatycznego;

2) dbanie o zabezpieczenia fizyczne węzłów sieci (switche, routery itp.) uniemożliwiające dostęp do nich przez osoby niepowołane.

§ 35. Inspektor ds. obsługi informatycznej urzędu dba o to, aby informacja dotycząca rodzaju serwerów, urządzeń telekomunikacyjnych, teletransmisyjnych, sposobu połączeń i systemu łączności była chroniona.

§ 36. Nadzór nad funkcjonowaniem procedur przyznawania uprawnień do korzystania z usług Internetu i poczty elektronicznej oraz procedur cofania lub zawieszania tych uprawnień sprawuje Inspektor ds. obsługi informatycznej w uzgodnieniu z Sekretarzem Gminy.

Rozdział 12.
12
Postanowienia końcowe

§ 37. 1. W razie stwierdzenia lub podejrzenia zaistnienia zdarzenia zagrażającego bezpieczeństwu systemu informatycznego należy postąpić zgodnie z procedurami obowiązującymi w Urzędzie.

2. Przestrzeganie postanowień niniejszej instrukcji przez użytkowników stanowi podstawę bezpiecznego posługiwania się systemami informatycznymi Urzędu.