Załącznik nr 8
do Polityki Bezpieczeństwa Informacji
w Urzędzie Gminy w Kozielicach.

Kozielice, dn. 08.03.2021 r.

INSTRUKCJA
ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM
Urzędu Gminy w Kozielicach.

I. POSTANOWIENIA OGÓLNE.

1. Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Urzędzie Gminy w Kozielicach, zwaną dalej „Instrukcją", określa:
   1) Zasady, tryb postępowania i zalecenia Administratora Systemów Teleinformatycznych, które należy stosować w trakcie przetwarzania danych osobowych w systemie informatycznym.
   2) Zasady dostępu użytkowników do systemu informatycznego w urzędzie, w tym sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności, sposób rejestrowania i wyrejestrowywania użytkowników oraz osoby odpowiedzialne za te czynności.
   3) Zasady i procedury rozpoczynania i kończenia pracy.
   4) Zasady i częstotliwość tworzenia kopii bezpieczeństwa.
   5) Zasady korzystania i przechowywania elektronicznych nośników informacji oraz sporządzania wydruków.
   6) Sposoby zabezpieczenia danych w systemie informatycznym.
   7) Zasady korzystania z oprogramowania, internetu, bankowości elektronicznej, poczty elektronicznej.
   8) Zasady dokonywania przeglądów i konserwacji systemu i zbioru danych.
   9) Zasady postępowania w przypadku naruszenia bezpieczeństwa systemu informatycznego w urzędzie.
2. Instrukcja została przyjęta w celu wykazania, że dane w systemie informatycznym Urzędu Gminy w Kozielicach przetwarzane są w sposób zgodny z przepisami prawa w zakresie ochrony danych osobowych, bezpieczeństwa informatycznego, w tym zgodnie z zasadami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej: RODO).

II. DEFINICJE.

Terminom używanym w niniejszej Instrukcji nadaje się znaczenia określone w Polityce.

III. ZASADY DOSTĘPU UŻYTKOWNIKA DO SYSTEMU.

1. Za bezpieczeństwo danych przetwarzanych w systemie informatycznym oraz za właściwe funkcjonowanie systemu informatycznego odpowiedzialny jest Administrator Systemów Teleinformatycznych **(AST).**
2. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania, mogą być dopuszczeni wyłącznie użytkownicy.

3. Po upoważnieniu osoby do przetwarzania danych w systemie informatycznym zostaje jej nadany odrębny identyfikator oraz hasło. Z chwilą nadania identyfikatora użytkownik może uzyskać dostęp do systemu informatycznego w zakresie wynikającym z jego upoważnienia.
4. Dostęp do systemu informatycznego mają także inne podmioty tylko i wyłącznie w zakresie i na zasadach określonych w umowach powierzenia przetwarzania danych osobowych pod nadzorem Administratora Systemów Teleinformatycznych.

IV. METODY I ŚRODKI UWIERZYTELNIANIA ORAZ ZARZĄDZANIE NIMI.

1. W systemie informatycznym stosowane jest uwierzytelnianie na poziomie dostępu do systemu operacyjnego. Do uwierzytelnienia stosowane są identyfikator oraz hasło.
2. Identyfikator składa się z minimum sześciu znaków. W identyfikatorze pomija się polskie znaki diakrytyczne.
3. Identyfikator nowego użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielony innej osobie.
4. Identyfikator przydzielony użytkownikowi, który utracił uprawnienie dostępu do systemu informatycznego, winien zostać niezwłocznie zablokowany. W takim wypadku AST podejmuje również inne działania, które okażą się konieczne w celu zapobieżenia nieuprawnionemu dostępowi do systemu informatycznego oraz naruszeniu zasad ochrony danych.
5. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
6. Hasło nie może być identyczne z identyfikatorem użytkownika, ani z jego imieniem lub nazwiskiem.
7. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom. Hasła utrzymywane są w tajemnicy również po upływie ich ważności.
8. Hasła muszą spełniać wymogi zawarte w Rozporządzeniu 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 w zależności od poziomu zabezpieczenia. Zgodnie z §4 pkt 2 rozporządzenia. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 8 znaków."
9. Hasła nie mogą być przechowywane w formie jawnej w żadnej postaci: elektronicznej lub tradycyjnej (pliki tekstowe, zapisy w skryptach logowania, makrach, zdefiniowane jako klawisze funkcyjne terminali, inne dowolne zapisy tradycyjne).
10. W przypadku przechowywania w formie niejawnej, hasła nie mogą być przechowywane szczególnie w miejscach, gdzie może dojść do nieautoryzowanego dostępu ze strony osób trzecich.
11. Hasła muszą być natychmiast zmienione jeśli istnieje podejrzenie, że zostały odkryte lub wiadomo, że znajdują się w posiadaniu osoby nieupoważnionej.
12. Zmiana hasła użytkownika powinna być automatycznie wymuszana oprogramowaniem.
13. Zabrania się używania identyfikatora lub hasła innego użytkownika.
14. Użytkownicy odpowiedzialni są za administrowanie programem wygaszacza ekranu zabezpieczającym dostęp do komputera w momencie nieobecności na stanowisku pracy.
15. Wygaszacz musi być zabezpieczony hasłem, automatycznie uruchamiany po określonym czasie braku aktywności użytkownika.
16. Użytkownicy odpowiadają również za utworzenie haseł na poziomie aplikacji oprogramowania systemowego.

V. OBOWIĄZKI ZWIĄZANE Z ROZPOCZĘCIEM, ZAWIESZENIEM I KOŃCEM PRACY W SYSTEMIE INFORMATYCZNYM.

1. Przed uruchomieniem komputera użytkownik winien sprawdzić, czy nie zostało do niego podłączone żadne niezidentyfikowane urządzenie.
2. Przed przystąpieniem do pracy w systemie informatycznym, użytkownik winien upewnić się, że spełnione są podstawowe warunki bezpieczeństwa wymagane przy przetwarzaniu danych w systemie informatycznym, a w szczególności ustawienie urządzenia odtwarzającego obraz ze stacji roboczej (np. monitora) w sposób uniemożliwiający osobom trzecim wgląd w dane.
3. Po uruchomieniu komputera użytkownik dokonuje uwierzytelnienia się przy pomocy hasła oraz identyfikatora.
4. Przy każdorazowym opuszczeniu stanowiska komputerowego użytkownik powinien dopilnować, aby na ekranie nie były wyświetlane dane.
5. Wychodząc z pomieszczenia, w którym przetwarzane są dane z systemu informatycznego użytkownik powinien sprawdzić czy zamknięte są okna i wejście do pomieszczenia.
6. Przy opuszczaniu stanowiska komputerowego na czas dłuższy niż 5 minut użytkownik zobowiązany jest ustawić wygaszacz ekranu.
7. Po zakończeniu pracy w systemie informatycznym użytkownik zobowiązany jest wylogować się z tego systemu.

VI. WYREJESTROWANIE UŻYTKOWNIKA.

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje AST na wniosek kierownika komórki organizacyjnej.
2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.
3. Wyrejestrowanie następuje poprzez zablokowanie konta użytkownika.
4. Przyczyną zablokowania użytkownika z systemu informatycznego jest:
   1) Nieobecność w pracy trwająca dłużej niż 31 dni kalendarzowych.
   2) Zawieszenie w pełnieniu obowiązków służbowych.
   3) zwolnienie z pełnienia obowiązków służbowych.
5. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.

VII. ZASADY I CZĘSTOTLIWOŚĆ TWORZENIA KOPII ZAPASOWYCH.

1. Dla zabezpieczenia integralności danych AST wykonuje kopie zapasowe poprzez archiwizację wszystkich danych zapisanych w systemie informatycznym, w tym danych osobowych.
2. Kopie awaryjne tworzy się automatycznie w systemie ciągłym, z wykorzystaniem odrębnego nośnika.
3. Administrator Systemów Teleinformatycznych przegląda okresowo kopie awaryjne i ocenia ich przydatność do odtworzenia zasobów systemu w przypadku jego awarii.
4. AST zabezpiecza nośniki z kopiami zapasowymi przed dostępem do nich osób nieupoważnionych oraz przed ich zniszczeniem.
5. Zabrania się przechowywania kopii awaryjnych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.

VIII. ZASADY KORZYSTANIA I PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ORAZ SPORZĄDZANIA WYDRUKÓW.

1. Osoby użytkujące przenośne nośniki informatyczne, służące do przetwarzania danych osobowych, zobowiązane są niezwłocznie informować AST o zakresie, rodzaju zbieranych danych osobowych oraz celu ich przetwarzania.

2.Użytkownicy zobowiązani są przechowywać wszelkie elektroniczne nośniki informacji, które nie są przeznaczone do udostępnienia, w warunkach uniemożliwiających dostęp do nich osobom nieuprawnionym. Nośniki te winny być przechowywane w zamkniętych szafkach znajdujących się w pomieszczeniach biurowych na terenie urzędu.
3.Dane zapisane na elektronicznych nośnikach informacji mogą być usuwane albo poprzez fizyczne zniszczenie nośnika albo poprzez wielokrotny zapis nieistotnych informacji w obszarze zajmowanym przez dane kasowane.
4.Użytkownicy nie są upoważnieni do wynoszenia elektronicznych nośników informacji, na których zapisane są dane, z urzędu, chyba że jest to uzasadnione celami przetwarzania. O takiej sytuacji bezwzględnie musi być powiadomiony AST. W takim przypadku elektroniczne nośniki informacji muszą być zabezpieczone w sposób zapewniający poufność i integralność danych.
5.AST może żądać usunięcia danych, co do których zachodzi uzasadnione podejrzenie, że nie są przetwarzane zgodnie z zasadami określonymi w przepisach o ochronie danych osobowych.
6.Osoba użytkująca przenośny komputer, tablet itp. służący do przetwarzania danych osobowych, zobowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego sprzętu poza obszarem ochrony danych w celu zapobieżenia dostępowi do tych danych osobie niepowołanej.
7.Użytkownik sporządzający wydruki, które zawierają dane osobowe jest odpowiedzialny za zachowanie szczególnej ostrożności przy korzystaniu z nich, a zwłaszcza za zabezpieczenie ich przed dostępem osób nie posiadających imiennego upoważnienia oraz nieuprawnionych do wglądu.
8.Wydruki zawierające dane osobowe, które są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie wykorzystując w tym celu niszczarki.

IX. ZABEZPIECZENIE DANYCH W SYSTEMIE INFORMATYCZNYM.

1.Administrator Systemów Teleinformatycznych stosuje zabezpieczenie danych poprzez ochronę systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawionego dostępu do systemu informatycznego oraz przed działaniami inicjowanymi z sieci zewnętrznej.
2.Administrator Systemów Informatycznych stosuje również fizyczne zabezpieczenie danych, które polega na tym, że:
1)Jednostki komputerowe podłączone są pod zasilacze UPS.
2)Ochrona serwera przed zanikiem zasilania polega na stosowaniu zasilacza zapasowego UPS
3)Ochrona przed utratą zgromadzonych danych polega na tworzeniu kopii zapasowych na zewnętrznym dysku sieciowym.
4)Ochrona przed awarią podsystemu dyskowego, systemu operacyjnego oraz serwera polega na wykorzystywaniu macierzy dyskowych.
3.W celu zabezpieczenia przed nieautoryzowanym dostępem do baz danych Administratora Danych Osobowych poprzez sieć internetową AST stosuje:
1)Firewall sprzętowy.
2)Firewall programowy oraz oprogramowanie antywirusowe monitorujące próby włamania oraz skanujące pocztę elektroniczną.
3)Blokowanie i filtrowanie niektórych usług.
4)Monitorowanie przez system antywirusowy danych ściąganych z sieci internetowej.
5)Zabezpieczenie kluczami WPA2 elementów sieci bezprzewodowej.
4.System informatyczny jest automatycznie skanowany przez program antywirusowy przynajmniej raz na 24 godziny.

5.Do obowiązków AST należy aktualizacja oprogramowania służącego do sprawdzania w systemie obecności wirusów komputerowych.
6.Użytkownik jest uprawniony do dostępu do systemu informatycznego wyłącznie przy zastosowaniu komputera, na którym uruchomiony jest program antywirusowy z włączoną ochroną systemu plików w czasie rzeczywistym.
7.Komputery i inne urządzenia oraz elektroniczne nośniki informacji, na których zapisane są dane, przekazywane poza pomieszczenia biurowe urzędu muszą być zabezpieczone w sposób zapewniający poufność i integralność danych.
8.Hasło umożliwiające dostęp do sieci bezprzewodowej jest udostępniane przez Administratora Systemów Teleinformatycznych wyłącznie użytkownikom.

X. ZASADY KORZYSTANIA Z OPROGRAMOWANIA.

1.Użytkownik zobowiązany jest do korzystania wyłącznie z oprogramowania legalnego i dopuszczonego do stosowania w urzędzie.
2.Użytkownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione przez AST. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych płyt CD, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe.

XI. ZASADY KORZYSTANIA Z INTERNETU.

1.Dopuszcza się korzystanie przez pracowników ze stron internetowych w celach służbowych, a także okazjonalnie w celach prywatnych. Podczas korzystania z sieci internetowych niedozwolone jest przeglądanie, a także ściąganie materiałów, których treści są prawnie zakazane, naruszają dobre obyczaje lub uznawane są za obraźliwe.
2.Od pracowników wymaga się także zachowania szczególnej ostrożności w przypadku żądania lub prośby podania kodów, PIN-ów, haseł, numerów kart płatniczych przez internet, w szczególności dotyczy to żądania podania takich informacji przez rzekomy bank.
3.W zakresie dozwolonym przepisami prawa, ADO zastrzega sobie prawo kontrolowania sposobu korzystania przez użytkownika z internetu pod kątem wyżej opisanych zasad oraz ma prawo blokować dostęp do wybranych stron internetowych.

XII. ZASADY KORZYSTANIA Z BANKOWOŚCI ELEKTRONICZNEJ.

1.Użytkownicy, którzy w zakresie obowiązków maja za zadanie korzystania z bankowości elektronicznej, zobowiązani są do regularnej zmiany hasła oraz nieprzechowywania go w formie pisemnej wraz z loginem.
2.Zabrania się opuszczania stanowiska pracy bez wylogowania się i zamknięcia przeglądarki.
3.Użytkownik logujący się do bankowości elektronicznej nie powinien korzystać z nieznanych sieci bezprzewodowych.
4.W celu zalogowania się do systemu bankowości elektronicznej pracownik nie powinien wchodzić na stronę internetową banku za pośrednictwem linków znajdujących się w korespondencji elektronicznej.

XIII. ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ.

1.Użytkownik jest zobowiązany do korzystania z przyznanego mu adresu mailowego wyłącznie w celach służbowych.
2.Podczas przesyłania danych należy zachować szczególną ostrożność przy wpisywaniu adresu odbiorcy dokumentu. Zaleca się, aby użytkownik podczas przesyłania danych osobowych pocztą elektroniczną zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

3.W przypadkach gdy wiadomość jest kierowana jednocześnie do kilku adresatów należy używać metody „Ukryte do wiadomości -UDW”.
4.ADO może poznawać treść wiadomości elektronicznych znajdujących się we wszystkich systemach internetowych administratora, jeżeli zostały one wysłane lub odebrane przez użytkowników.
5.Zabronione jest otwieranie wiadomości e-mail pochodzących od nieznanego nadawcy bądź z podejrzanym tytułem (tzw. phishing e-mail).
6.Zabronione jest otwieranie linków bądź pobieranie plików zapisanych w wiadomości email od nieznanego nadawcy. Zabrania się także rozsyłania za pośrednictwem poczty elektronicznej „łańcuszków szczęścia”, itp.
7.Do przesyłania danych przy połączeniach w sieci publicznej (internet), z uwagi na przekazywane dane osobowe, powinny być wykorzystywane tylko kanały transmisji wykorzystywane przez autoryzowane programy wykorzystywane również w innych urzędach oraz instytucjach państwowych i w oparciu o przepisy prawne regulujące sposób wysyłania tych danych.
8.Użytkownicy powinni na bieżąco kasować niepotrzebne wiadomości (tj. spam, oferty handlowe itp.).
9.Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

XIV. PRZEGLĄDY I KONSERWACJE SYSTEMU INFORMATYCZNEGO.

1.Doraźnych przeglądów i konserwacji systemu informatycznego dokonuje AST.
2.Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać do naprawy, do likwidacji dopiero po uprzednim uzyskaniu zgody AST.
3.Bardziej skomplikowane i szczegółowe przeglądy oraz konserwacje systemu informatycznego powinny być wykonywane przez profesjonalne podmioty w oparciu o umowy zawarte na piśmie, w tym umowy powierzenia przetwarzania danych osobowych.
4.Przy dokonywaniu przeglądów i konserwacji systemu informatycznego należy przestrzegać następujących zasad:
1)Przed rozpoczęciem prac serwisowych dane znajdujące się w systemie informatycznym, powinny zostać zarchiwizowane lub w inny sposób zabezpieczone przed ich usunięciem lub zmianą.
2)Prace serwisowe powinny być wykonywane w obecności AST.
3)Prace serwisowe należy ewidencjonować w książce zawierającej informacje o rodzaju prac serwisowych, datach rozpoczęcia i zakończenia prac oraz osobach dokonujących prac serwisowych).

XV. NARUSZENIE BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO.

1.Każdy przypadek naruszenia ochrony danych osobowych, które mogą wskazywać na naruszenie bezpieczeństwa podlega zgłoszeniu do AST.
2.Obowiązek dokonania zgłoszenia, o którym mowa w ust 1, spoczywa na każdym użytkowniku, który powziął wiadomość o naruszeniu ochrony danych osobowych.
3.W przypadku naruszenia integralności bezpieczeństwa sieciowego, obowiązkiem AST jest natychmiastowe wstrzymanie udostępniania zasobów dla użytkowników i odłączenie serwerów od sieci.
4.Użytkownik sieci i AST w porozumieniu z Inspektorem Ochrony Danych Osobowych ustalają przyczyny naruszenia integralności bezpieczeństwa sieciowego.

5.Przywrócenie udostępniania zasobów użytkownikom może nastąpić dopiero po ustaleniu i usunięciu przyczyny naruszenia integralności bezpieczeństwa sieciowego.

XVI. PRZEPISY KOŃCOWE.

W sprawach nieuregulowanych niniejszą instrukcją mają zastosowanie przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej: RODO), ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.