INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

Kod dokumentu:	
Wersja:	0.1
Data wersji:	14.05.2018
Utworzony przez:	Adam Szumowski
Zatwierdzony przez:	
Poziom poufności:	Do użytku wewnętrznego

Historia zmian

Data	Wersja	Utworzona przez	Opis zmiany
2018-05-14	0.1	Adam Szumowski	Pierwsza wersja dokumentu

Spis treści

1. Cel, zakres i użytkownicy

Realizując postanowienia art. 19 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) **wprowadza się „Instrukcję Zarządzania Systemami Informatycznymi w Urzędzie Gminy w Janowicach Wielkich "** (zwaną dalej Polityką Instrukcja).

Niniejsza instrukcja określa zasady eksploatacji i zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

Użytkownikami niniejszego dokumentu są wszyscy pracownicy Urzędu Gminy w Janowicach Wielkich, jak również odnośne podmioty zewnętrzne.

2. Dokumenty referencyjne

Polityka Bezpieczeństwa Danych w Urzędzie Gminy w Janowicach Wielkich;

3. Określenia i skróty użyte w Instrukcji Zarządzania Systemami Informatycznymi

Poufność – właściwość informacji zapewniająca jej dostęp wyłącznie dla osób uprawnionych.

Integralność – właściwość informacji zapewniająca możliwość dokonywania w niej zmian tylko przez uprawnione osoby lub procesy, w dozwolony sposób.

Dostępność – właściwość informacji zapewniająca możliwość dostępu do tej informacji przez uprawnione osoby w każdym czasie, gdy dana informacja jest potrzebna.

Bezpieczeństwo informacji – zapewnienie poufności, integralności oraz dostępności informacji.

Polityka - rozumie się przez to Politykę Bezpieczeństwa Danych Osobowych w Urzędzie Gminy w Janowicach Wielkich;

Instrukcja - rozumie się przez to Instrukcję Zarządzania Systemami Informatycznymi w Urzędzie Gminy w Janowicach Wielkich;

Administrator Danych – Urząd Gminy w Janowicach Wielkich reprezentowany przez Wójta Gminy Janowice Wielkie, decydującego o celach i środkach przetwarzania danych osobowych;

Inspektor Ochrony Danych - osobę powołaną przez AD w Urzędzie Gminy w Janowicach Wielkich, wpisaną do prowadzonego przez organ nadzorczy rejestru inspektorów ochrony danych, zwaną dalej „IOD";

Administrator Systemów Informatycznych (ASI) – osobę wyznaczoną przez AD, odpowiedzialny za infrastrukturę techniczną systemów;

Rozporządzenie - Rozporządzenie 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)

Dane osobowe (dane) - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

Zbiór danych - zestaw danych osobowych posiadający określoną strukturę, prowadzony w/g określonych kryteriów oraz celów;

Usuwanie danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

Zgoda osoby, której dane dotyczą - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści;

Baza danych osobowych - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe;

Przetwarzanie danych - wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie;

System informatyczny (system) - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

Administrator systemu - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień;

Użytkownik - pracownik Urzędu Gminy w Janowicach Wielkich posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych;

Zabezpieczenie systemu informatycznego - należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed

modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;
Nośnik komputerowy (wymienny) - nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde, dysku flash, pendrive;
Hasło - ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;
Identyfikator - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie.
Urząd – Rozumie się przez to Urząd Gminy w Janowicach Wielkich

4. Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

Podstawą do nadania uprawnień do przetwarzania danych osobowych w systemie informatycznym Urzędu jest upoważnienie do przetwarzania danych osobowych. Upoważnienie wydawane jest przez Administratora Danych Osobowych
Upoważnienie wydawane jest na wniosek przełożonego danego pracownika, a w przypadku osoby niebędącej pracownikiem Urzędu Gminy w Janowice Wielkie na wniosek pracownika koordynującego działania osoby, dla której upoważnienie jest wydawane.
Stanowisko ds. Kadrowych:
1) w przypadku, gdy dana osoba otrzymuje po raz pierwszy upoważnienie do przetwarzania danych osobowych informuje ją o obowiązkach związanych z zapewnieniem ochrony danych osobowych;
2) odbiera od powyższej osoby podpis pod upoważnieniem do przetwarzania danych osobowych i oświadczeniem o zapoznaniu się z obowiązującymi zasadami ochrony danych osobowych.

Stanowisko ds. kadrowych prowadzi, w imieniu i z upoważnienia Administratora Danych Osobowych, ewidencję osób upoważnionych do przetwarzania danych osobowych. Każda zmiana w zakresie informacji zawartych w ewidencji podlega niezwłocznemu odnotowaniu przez Stanowisko ds. kadrowych.
Uprawnienia dostępu do systemu informatycznego nadawane są na podstawie wniosku przełożonego danego pracownika, a w przypadku osoby niebędącej pracownikiem Urzędu Gminy w Janowicach Wielkich na wniosek pracownika Urzędu koordynującego działania danej osoby. Wniosek niniejszy kierowany jest do IOD i przekazywany ASI.
Za nadanie uprawnień w systemie informatycznym odpowiada ASI. Uprawnienia nie mogą być nadane w przypadku, jeżeli dana osoba nie posiada upoważnienia do przetwarzania danych osobowych w wymaganym zakresie.
ASI informuje osobę wnioskującą o fakcie nadania lub odmowy nadania uprawnień. W przypadku nadawania użytkownikowi uprawnień do danego systemu informatycznego po raz pierwszy, ASI dokonuje nadania użytkownikowi identyfikatora, wygenerowania hasła oraz wpisania identyfikatora do ewidencji osób upoważnionych do przetwarzania danych osobowych.
Identyfikator użytkownika w systemie informatycznym musi być unikalny dla użytkownika. Nie może być to identyfikator, który w przeszłości był już stosowany w systemie informatycznym. Sprawdzenie unikalności identyfikatora odbywa się na podstawie ewidencji osób upoważnionych do przetwarzania danych osobowych.
Hasło użytkownika jest przydzielane indywidualnie każdemu z użytkowników i znane jest tylko użytkownikowi, który się nim posługuje.
ASI przekazuje użytkownikowi identyfikator i hasło.
Użytkownik jest zobowiązany do zmiany hasła przy pierwszym dostępie do systemu informatycznego.

5. Procedura odbierania uprawnień do przetwarzania danych w systemie informatycznym

W przypadku konieczności odebrania lub zmiany zakresu upoważnienia – w związku ze zmianą zakresu obowiązków służbowych pracownika lub zakończeniem pracy – jego przełożony wnioskuje do IOD o wykonanie powyższej czynności. Administrator Danych Osobowych dokonuje, na podstawie informacji przekazanej przez IOD, odebrania lub zmiany zakresu upoważnienia, ASI zaś dokonuje odebrania lub zmiany zakresu uprawnień w systemie informatycznym. O powyższym IOD informuje osobę wnioskującą.
W przypadku konieczności odebrania lub zmiany zakresu upoważnienia dla osób niebędących pracownikami Urzędu Gminy w Janowicach Wielkich o wykonanie powyższej czynności wnioskuje pracownik koordynujący działania danej osoby.

6. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

Użytkownicy systemu informatycznego przetwarzającego dane osobowe wykorzystują w procesie uwierzytelnienia identyfikatory i hasła.
Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi i nie podlega zmianie.

Nowe hasło jest przekazywane użytkownikowi przez ASI.
Po zalogowaniu do systemu z wykorzystaniem otrzymanego hasła użytkownik jest zobowiązany do dokonania jego natychmiastowej zmiany, nawet, jeżeli system informatyczny nie wymusza takiego działania.
Hasła dostępu do systemu informatycznego muszą spełniać poniższe warunki:
1) posiadać długość co najmniej 8 znaków,
2) zawierać litery małe i duże,
3) zawierać cyfry lub znaki specjalne.

Hasło w systemach przetwarzających danych osobowych jest zmieniane przez użytkownika nie rzadziej, niż co 30 dni lub niezwłocznie w przypadku podejrzenia, iż mogły z nim się zapoznać nieuprawnione osoby. Hasło powinno różnić się od poprzednio używanych.
Użytkownik zobowiązany jest do:
1) nieujawniania hasła innym osobom, w tym innym użytkownikom,
2) zachowania hasła w tajemnicy, również po jego wygaśnięciu,
3) niezapisywania hasła,
4) postępowania z hasłami w sposób uniemożliwiający dostęp do nich osobom trzecim,
5) przestrzegania zasad dotyczących, jakości i częstości zmian hasła,
6) wprowadzania hasła do systemu w sposób minimalizujący podejrzenie go przez in. użytkowników systemu.

W przypadku zapomnienia hasła użytkownik powinien zwrócić się do ASI o wygenerowanie nowego hasła.
W przypadku podejrzenia zapoznania się z hasłem przez osobę nieuprawnioną użytkownik jest zobowiązany do natychmiastowej zmiany hasła oraz powiadomienia o zaistniałym fakcie ASI.

7. Procedura rozpoczęcia, zawieszenia i zakończenia pracy przeznaczona dla użytkowników systemu

Rozpoczynając pracę w systemie informatycznym przetwarzającym dane osobowe, użytkownik:
1) uruchamia komputer,
2) wprowadza niezbędne do pracy identyfikatory i hasła,
3) hasła są wprowadzane w sposób minimalizujący ryzyko podejrzenia ich przez osoby trzecie,
4) w przypadku problemów z rozpoczęciem pracy, spowodowanych odrzuceniem przez system wprowadzonego identyfikatora i hasła, natychmiast kontaktuje się z ASI,
5) w przypadku niestandardowego zachowania aplikacji przetwarzającej dane osobowe pracownik natychmiast powiadamia o zaistniałym fakcie ASI.

Zawieszając pracę w systemie informatycznym (w tym odchodząc od stanowiska pracy), użytkownik blokuje stację roboczą. Kontynuacja pracy może nastąpić po odblokowaniu stacji roboczej po wprowadzeniu hasła, w sposób gwarantujący jego niepodejrzenie przez osoby trzecie.
Opuszczając pomieszczenie, w którym przetwarzane są dane osobowe, pracownik zobowiązany jest do zamknięcia pomieszczenia na klucz, jeżeli w pomieszczeniu tym nie przebywa inna osoba upoważniona do przebywania w tym pomieszczeniu. Zabronione jest pozostawianie bez nadzoru w pomieszczeniach, w których przetwarzane są dane osobowe, osób nieupoważnionych.
Kończąc pracę w systemie informatycznym pracownik wylogowuje się ze wszystkich aplikacji, z których korzystał, wyłącza stację roboczą i zabezpiecza nośniki danych. W przypadku, gdy pracownik jest ostatnią osobą opuszczającą pomieszczenie, sprawdza zamknięcie okien, zamyka na klucz drzwi do pomieszczenia oraz zdaje klucz do sekretariat.

8. Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

Za tworzenie i przechowywanie kopii zapasowych odpowiedzialny jest ASI.
Kopie zapasowe systemów przetwarzających dane osobowe tworzone są codziennie poprzez nadpisywanie, tygodniowo oraz miesięcznie całościowe.
Nośniki kopii zapasowych oznaczane są w sposób umożliwiający określenie daty utworzenia kopii oraz nazwy systemu.
Nośniki z kopiami zapasowymi przechowywane są w zamykanej szafie zlokalizowanej w siedzibie Urzędu.
Utworzone kopie zapasowe podlegają weryfikacji ze względu na sprawdzenie możliwości odczytu danych.
ABI określa czas przechowywania poszczególnych kopii zapasowych, w zależności od celu przetwarzania danych zapisanych na kopiach zapasowych.
ASI odpowiedzialny jest za realizację działań odtworzeniowych w przypadku konieczności podjęcia takich działań w związku z awarią systemu informatycznego Urzędu. Po odtworzeniu systemu informatycznego ASI odpowiedzialny jest za przeprowadzenie testów poprawności działania systemu przed jego oddaniem do użytkowania.
ASI przeprowadza weryfikację możliwości odtworzenia danych zapisanych na kopiach zapasowych. Weryfikacja taka powinna być przeprowadzana nie rzadziej niż raz na pół roku.

9. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz nośników kopii zapasowych

Dane osobowe przechowywane są w postaci elektronicznej na:
1) nośnikach elektronicznych wbudowanych w sprzęt informatyczny lub stanowiących element tego systemu,
2) przenośnych nośnikach elektronicznych.
Dane przechowywane są na nośnikach jedynie w przypadkach, gdy jest to konieczne, przez czas niezbędny do spełnienia celu, w jakim zostały one na nośniku zapisane]. Po ustaniu czasu przechowywania zawartość nośnika podlega skasowaniu przy użyciu narzędzi zaakceptowanych do użycia w Urzędzie, a w przypadku nośników optycznych stosuje się niszczenie w niszczarkach umożliwiających niszczenie tego typu nośników.
Dane osobowe w systemie informatycznym przechowywane są przez czas wymagany do spełnienia celu, dla którego są one przetwarzane. Po jego upływie dane podlegają skasowaniu lub anonimizacji.
Przenośne elektroniczne nośniki informacji zawierające dane osobowe są przechowywane przez pracowników w sposób minimalizujący ryzyko ich uszkodzenia lub zniszczenia, w szczególności w zamykanych szafach i meblach biurowych. IOD wyznacza pomieszczenia, w których mogą być przechowywane takie nośniki.
W przypadku wycofania sprzętu komputerowego z użycia dane osobowe na nim zapisane są kasowane przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych zaakceptowanego do użycia w Urzędzie. W przypadku braku możliwości programowego usunięcia danych dysk podlega fiz. zniszczeniu. Za zniszczenie danych odpowiada ASI. Zniszczenie nośnika potwierdzane jest protokołem przechowywanym przez IOD.
Dopuszcza się powierzenie niszczenia nośników danych wyspecjalizowanym podmiotom zewnętrznym, pod warunkiem:
1) zawarcia umowy, o której mowa w art. 31 ustawy,
2) zagwarantowania poufności danych przez usługodawcę,
3) umożliwienia prowadzenia nadzoru nad procesem niszczenia nośników przez IOD lub upoważnionego przez niego pracownika Urzędu Gminy w Janowicach Wielkich,
4) udokumentowania faktu zniszczenia nośników protokołem.

10. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem działania jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

W celu zabezpieczenia systemu informatycznego przed działaniem niebezpiecznego oprogramowania zabrania się:
1) uruchamiania jakiegokolwiek oprogramowania, które nie zostało zatwierdzone do użytku w Urzędzie;
2) samowolnego korzystania z nośników przenośnych;
3) otwierania poczty elektronicznej, której tytuł nie sugeruje związku z pełnionymi obowiązkami służbowymi; w przypadkach wątpliwych należy skonsultować się z IOD;
4) korzystania z Internetu w celach nie związanych z pełnionymi obowiązkami służbowymi;
5) podłączania komputerów do sieci zewnętrznych za pośrednictwem modemów.
W przypadku zauważenia objawów mogących wskazywać na obecność niebezpiecznego oprogramowania użytkownik jest zobowiązany powiadomić IOD. Do objawów powyższych można zaliczyć:
1) istotne spowolnienie działania systemu informatycznego,
2) nietypowe działanie aplikacji,
3) nietypowe komunikaty,
4) utratę danych lub modyfikację danych.
System informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:
1) oprogramowanie antywirusowe,
2) zaporę sieciową,
3) aktualizację oprogramowania systemowego,
4) konfigurację oprogramowania minimalizującą ryzyko naruszenia bezpieczeństwa.
ASI jest odpowiedzialny za nadzór nad działaniem powyższych zabezpieczeń, a w szczególności za:
1) weryfikację aktualności sygnatur systemu antywirusowego i podejmowanie ewentualnych działań korekcyjnych,
2) weryfikację logów systemu antywirusowego i podejmowanie działań korekcyjnych,
3) przegląd logów zapory sieciowej oraz podejmowanie działań mających na celu zablokowanie ataków sieciowych,
4) weryfikację poprawności aktualizacji oprogramowania systemowego.

11. Odnotowanie informacji o udostępnieniu danych osobowych

Urząd udostępnia dane osobowe jedynie w przypadkach prawnie dopuszczalnych.
Odnotowanie faktu udostępnienia danych następuje:
1) w przypadku […] poprzez wprowadzenie przez użytkownika w polu […] informacji o udostępnieniu danych,
2) w przypadku […] poprzez wprowadzenie przez użytkownika w polu […] informacji o udostępnieniu danych. Przy odnotowywaniu przez użytkownika informacji o udostępnieniu danych, użytkownik wprowadza zapis „Dane osobowe w zakresie ››zakres‹‹ udostępniono ››odbiorca‹‹ w dniu ››data‹‹”, wprowadzając zamiast zapisów w nawiasach klamrowych odpowiednie informacje.

12. Procedura wykonywania przeglądu i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

Przegląd i konserwacja sprzętu informatycznego realizowany jest przez upoważnionych pracowników Urzędu Gminy w Janowicach Wielkich oraz przez podmioty zewnętrzne.

Prace serwisowe wykonywane na terenie Urzędu Gminy w Janowicach Wielkich przez podmioty zewnętrzne podlegają bezpośredniemu nadzorowi IOD.

Przekazanie sprzętu teleinformatycznego do naprawy poza teren Urzędu jest dopuszczalne, jeżeli spełnione zostaną poniższe warunki:

1) sprzęt przekazywany jest bez nośników zawierających dane osobowe, zaś fakt usunięcia nośników danych lub stwierdzenia braku nośników danych jest potwierdzany protokołem,
2) przekazanie sprzętu potwierdzane jest protokołem, pozwalającym na jednoznaczne wskazanie osoby przekazującej i osoby odbierającej sprzęt.

Protokoły lub ich kopie przechowywane są przez IOD.

Wszelkie prace serwisowe wykonywane przez podmioty zewnętrzne wymagają sporządzenia protokołu serwisowego, zawierającego co najmniej poniższe informacje:

1) wskazanie osoby przeprowadzającej prace serwisowe oraz podmiotu, którego osoba ta jest pracownikiem,
2) wskazanie osoby nadzorującej przebieg prac serwisowych (dotyczy sytuacji, gdy prace realizowane są w siedzibie Urzędu Gminy w Janowicach Wielkich,
3) przedmiot prac serwisowych (w szczególności identyfikator sprzętu w przypadku prac serwisowych dotyczących sprzętu),
4) zakres prac serwisowych i ich wynik,
5) czas przeprowadzania prac serwisowych.

13. Ważność oraz zarządzanie niniejszym dokumentem

Stwierdza się ważność niniejszego dokumentu na dzień 14.05.2018.

Właścicielem niniejszego dokumentu jest Inspektor Ochrony Danych, który jest odpowiedzialny za weryfikację oraz w razie konieczności aktualizację niniejszego dokumentu, co najmniej raz w roku.

W ocenie efektywności i właściwości niniejszego dokumentu należy wziąć pod uwagę następujące kryteria:

- liczbę pracowników i podmiotów zewnętrznych, których dotyczy proces przetwarzania danych osobowych, a którzy nie zapoznali się z niniejszym dokumentem
- niezgodność dokumentacji przetwarzania danych osobowych z przepisami prawa, obowiązkami branżowymi, zobowiązaniami umownymi oraz innymi dokumentami wewnętrznymi organizacji;
- nieefektywność wdrożenia i obsługi procesu danych osobowych
- niejasny podział odpowiedzialności za wdrożenie dokumentacji przetwarzania danych