



INSTRUKCJA Systemu Kontroli Zarządczej

Urząd Gminy
Kozy

WÓJT GMINY
KOZY

Załącznik Nr 2 do
Zarządzenia Nr 83/2014
Wójta Gminy Kozy
z dnia 24 października 2014 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

ZATWIERDZENIE DOKUMENTU

Sporządził	Sprawdził	Zatwierdził
Łukasz Kastura / Piotr Handzlik	Monika Olma	Krzysztof Fiałkowski

HISTORIA ZMIAN DOKUMENTU

Data	Wydanie	Zmiany dokonał	Miejsce i charakter zmiany
29.08.2011r.	1		
24.10.2014.	2	ASI/ ABI	Aktualizacja podstaw prawnych, zbiorów danych, uwzględnienie zmian infrastruktury, organizacyjnych i strukturalnych Urzędu

Niniejszy dokument jest własnością Urzędu Gminy Kozy. Wszelkie prawa zastrzeżone. Kopiowanie i rozpowszechnianie całości lub części dokumentu wyłącznie za zgodą Pełnomocnika ds. Systemu Kontroli Zarządczej.

Procedura odpowiada wymogom:	Nr dokumentu:	I.15.01
Kontroli zarządczej:	Standard C 15	Data wydania
PN-EN ISO 9001:2009 w punkcie:	-	24.10.2014 r.
PN-ISO/IEC 27001:2007 w punkcie:	-	Wydanie:
		2
	Strona	1 z 22

SPIS TREŚCI

1.	ORGANIZACYJNE I TECHNICZNE ŚRODKI OCHRONY PRZETWARZANYCH DANYCH	3
2.	OGÓLNE ZASADY BEZPIECZEŃSTWA INFORMACJI W URZĘDZIE GMINY KOZY	4
3.	STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM (ZGODNIE Z ROZPORZĄDZENIEM MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI Z DNIA 29 KWIETNIA 2004 R., DZ. U. Z 2004 R. NR 100, POZ. 1024, § 5 PKT. 2 ROZPORZĄDZENIA).....	7
4.	PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONA DLA UŻYTKOWNIKÓW SYSTEMU (ZGODNIE Z ROZPORZĄDZENIEM MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI Z DNIA 29 KWIETNIA 2004 R., DZ. U. Z 2004 R. NR 100, POZ. 1024, § 5 PKT. 3 ROZPORZĄDZENIA)	8
5.	TWORZENIE KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA (ZGODNIE Z ROZPORZĄDZENIEM MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI Z DNIA 29 KWIETNIA 2004 R., DZ. U. Z 2004 R. NR 100, POZ. 1024, § 5 PKT. 4 ROZPORZĄDZENIA).....	9
6.	NOŚNIKI KOPII ZAPASOWYCH, KTÓRE ZOSTAŁY WYCOFANE Z UŻYCIA, JEŻELI JEST TO MOŻLIWE, NALEŻY POZBAWIĆ ZAPISANYCH DANYCH ZA POMOCĄ SPECJALNEGO OPROGRAMOWANIA DO BEZPIECZNEGO USUWANIA ZAPISANYCH PONADTO:	10
7.	SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH (ZGODNIE Z ROZPORZĄDZENIEM MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI Z DNIA 29 KWIETNIA 2004 R., DZ. U. Z 2004 R. NR 100, POZ. 1024, § 5 PKT. 5 ROZPORZĄDZENIA)	12
8.	ZABEZPIECZENIE PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO (ZGODNIE Z ROZPORZĄDZENIEM MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI Z DNIA 29 KWIETNIA 2004 R., DZ. U. Z 2004 R. NR 100, POZ. 1024, § 5 PKT. 6 ROZPORZĄDZENIA).....	13
9.	REALIZACJA WYMOGU UWIERZYTELNIENIA UŻYTKOWNIKA I REJESTRACJI ZDARZEŃ (ZGODNIE Z ROZPORZĄDZENIEM MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI Z DNIA 29 KWIETNIA 2004 R., DZ. U. Z 2004 R. NR 100, POZ. 1024, § 7 UST. 1 PKT. 4 ROZPORZĄDZENIA)	15
10.	PRZEGLĄD I KONSERWACJA SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH	16
11.	POSTĘPOWANIE W PRZYPADKU STWIERDZENIA NARUSZENIA BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO	17
12.	TRYB PRACY PRZY PRZETWARZANIU DANYCH W TYM DANYCH OSOBOWYCH.....	19
13.	AUTORYZACJA NOWYCH URZĄDZEŃ W SIECI LAN URZĘDU GMINY KOZY	21
14.	NADZOROWANIE OTWIERANIA TUNELI VPN W CELACH SERWISOWYCH	22

1. ORGANIZACYJNE I TECHNICZNE ŚRODKI OCHRONY PRZETWARZANYCH DANYCH

1.1. Ochrona fizyczna pomieszczeń służbowych znajdujących się w budynku Urzędu Gminy Kozy

Wejścia do budynku Urzędu Gminy Kozy zabezpieczone są zamkami drzwiowymi klasy C oraz alarmem. Do budynku Urzędu dostać można się wejściem od ulicy Krakowskiej oraz od strony parkingu, mieszczącego się na tyłach budynku. Osoby wchodzące do budynku są rejestrowane za pomocą gminnego systemu monitoringu wideo. Poszczególne pokoje, w których odbywa się przetwarzanie danych i ich składowanie muszą być wyposażone w zamki i muszą być zamykane podczas nieobecności pracownika. Po zakończeniu pracy osoba zamykająca pomieszczenie powinna odnieść klucz do pokoju nr 3. Pozostawienie kluczy w zamkach pomieszczeń gdzie przetwarzane są dane, w tym dane osobowe, jest niedopuszczalne (także podczas pobytu pracownika w pokoju).

1.2. Zabezpieczenie zbiorów przetwarzanych tradycyjnie.

Zbiory danych przetwarzane tradycyjnie (ręcznie) po godzinach pracy przechowywane winny być w szafkach zamkniętych (zamki, klódki). W przypadku przetwarzania takich danych w pomieszczeniu, w którym przebywać mogą osoby nieupoważnione do przetwarzania takich danych (np. interesanci albo inni pracownicy) czynności powinny być przeprowadzane w taki sposób, aby osoby nieupoważnione nie miały wglądu do tych danych.

1.3. Zabezpieczenie zbiorów przetwarzanych cyfrowo.

Stanowiska komputerowe w pomieszczeniach, gdzie przebywać mogą osoby nieupoważnione do przetwarzania danych, w tym danych osobowych (np. interesanci albo inni pracownicy urzędu) winny być umieszczone w sposób, który uniemożliwić takim osobom wgląd do tych danych.

Na wszystkich komputerach, wymagana jest ochrona antywirusowa. Ponadto te, na których realizowane jest przetwarzanie danych wyposażone powinny być w zasilanie awaryjne umożliwiające bezpieczne zakończenie operacji na danych i zamknięcie systemu.

Każdy użytkownik systemu komputerowego korzysta, w celu dostępu do danych, ze stworzonego według określonych zasad konta, o odpowiednio do pełnionych obowiązków przydzielonych mu uprawnieniach dostępu do zasobów tego systemu.

Dostęp do konta możliwy jest po podaniu prawidłowej pary – unikalnej nazwy użytkownika i hasła o długości min. 8 znaków, odpowiedniej złożoności i terminie ważności.

Wymaga się, by w miejscu styku sieci komputerowej urzędowej z siecią publiczną zainstalowane były stosowne urządzenia uniemożliwiające dostęp osób niepowołanych z zewnątrz do jej zasobów, a także pozwalające na kontrolę przepływających danych.

W systemie wykonywane być winny kopie zapasowe a ich nośniki przechowywane w bezpiecznym miejscu.

Nośniki danych używane w procesie przetwarzania danych, które przestają pełnić swoją funkcję zostają fizycznie zniszczone, bądź poddane procesowi „czyszczenia” według określonej procedury uniemożliwiającej ich ponowne odczytanie (Szczegółowe wytyczne dotyczące procedur, nośników danych, zabezpieczeń, haseł, ich tworzenia i przetwarzania danych osobowych w systemach cyfrowych określone zostały w Instrukcji i procedurach zarządzania systemem informatycznym).

1.4. Przebywanie na terenie Urzędu Gminy Kozy

Pracownikom wolno przebywać na terenie Urzędu tylko w wyznaczonych godzinach pracy, a po nich jedynie po zawiadomieniu i uzyskaniu zgody bezpośredniego przełożonego. Przebywanie w Urzędzie w dni wolne od pracy możliwe jest jedynie po uzyskaniu zgody Wójta Gminy Kozy.

2. OGÓLNE ZASADY BEZPIECZEŃSTWA INFORMACJI W URZĘDZIE GMINY KOZY

2.1. Dostęp do zasobów i usług informatycznych

Zasoby informatyczne Urzędu Gminy Kozy służą do realizowania działań służbowych i nie mogą być wykorzystywane w celach prywatnych.

Dostęp do zasobów i usług informatycznych przydzielany jest wyłącznie na podstawie formalnej ścieżki wnioskowania zdefiniowanej w „Procedurze nadawania uprawnień”. Zabrania się ingerowania zarówno w sprzęt komputerowy jak i w jego konfigurację celem zmiany uprawnień z pominięciem w. w. procedury.

Przydzielanie dostępu do zasobów i usług informatycznych (w tym podłączanie „obcych” urządzeń do sieci) należących do Urzędu osobom nie będącym pracownikami Urzędu Gminy Kozy, może odbywać się wyłącznie za zgodą Administratora Bezpieczeństwa Informacji lub Administratora Systemu Informatycznego.

2.2. Hasła

Każdy użytkownik, który ma dostęp do systemów informatycznych, posiada unikalny identyfikator (login) użytkownika i osobiste hasło.

Użytkownik hasła:

- zobowiązany jest uwierzytelniać się w systemie informatycznym wyłącznie na podstawie własnego loginu i hasła (za wyjątkiem hasła początkowego),
- odpowiedzialny jest za wykorzystywanie swojej loginu oraz hasła oraz za wszystkie czynności wykonane przy użyciu swojego loginu i hasła,

W żadnym wypadku nie może ujawniać swojego hasła komukolwiek włącznie ze służbami informatycznymi, przełożonym czy współpracownikami.

Hasło użytkownika nie może być przechowywane w formie możliwej do odczytania, tj. zapisane w plikach tekstem jawnym, skryptach i makrach, zapisane na kartkach i w miejscach, do których mają dostęp osoby nieupoważnione.

Szczegółowe wymogi dotyczące hasła, zasady zabezpieczenia, uzyskania hasła oraz sposób postępowania z hasłem opisane są w rozdziale 3 niniejszej instrukcji „STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM”.

2.3. Ochrona przed szkodliwym oprogramowaniem

Na wszystkich stacjach roboczych wykorzystywanych w Urzędzie Gminy Kozy zainstalowane jest oprogramowanie antywirusowe. Ingerencja w ustawienia w. w. oprogramowania (w szczególności jego wyłączenie lub usuwanie) jest surowo zabroniona.

Każdy pracownik Urzędu Gminy Kozy w przypadku wykrycia szkodliwego oprogramowania na stacji roboczej (lub podejrzenia o zajściu takiego zdarzenia), ma obowiązek bezzwłocznie poinformować o tym fakcie Administratora Systemu Informatycznego i postępować zgodnie z otrzymanymi instrukcjami.

2.4. Wykorzystanie i niszczenie nośników elektronicznych

Nośniki nieprzeznaczone do dalszego użytku (w tym również nośniki kopii zapasowych) winny być przekazane do Administratora Bezpieczeństwa Informacji celem zniszczenia. Sposób niszczenia nośników musi gwarantować brak możliwości odczytania danych na nich zawartych – np. potłamanie płyty CD lub DVD, zmiażdżenie i porwanie taśm streamerów, rozkręcenie twardego dysków i powyginanie talerzy.

2.5. Zasady legalności

Użytkowanie na terenie Urzędu Gminy Kozy programów niezgodnie z zasadami licencji jest zabronione.

Użytkowanie lub powielanie wszelkich nagrań muzycznych, filmów oraz innych dzieł podlegających prawom autorskim, nie będących własnością Urzędu Gminy Kozy jest zabronione. Dotyczy to także prywatnych nagrań muzycznych i filmów nabytych legalnie przez pracowników, których używanie na

terenie Urzędu Gminy Kozy stanowi złamanie 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. 2004 nr 100 poz. 1024).

Zawartość stacji roboczych podlega okresowym przeglądom – fakt zidentyfikowania nielegalnych treści zgłaszany jest przełożonym oraz stanowi incydent bezpieczeństwa i jako taki podlega obsłudze zgodnie z „Procedurą zarządzania incydentami bezpieczeństwa”.

2.6. Zasady przekazywania informacji

Wszyscy pracownicy są zobowiązani do zachowania odpowiedniej dbałości o bezpieczeństwo przesyłanych informacji. W szczególności dotyczy to informacji wysyłanych do organizacji i osób spoza struktur Urzędu Gminy Kozy.

Przy przesyłaniu informacji przy wykorzystaniu poczty elektronicznej, tradycyjnej, urządzeń faksujących oraz telefonów obowiązują następujące zasady:

- należy przestrzegać drogi służbowej w wysyłaniu korespondencji, jeśli taka została zdefiniowana,
- zabronione jest wykorzystywanie poczty Urzędu Gminy Kozy do celów prywatnych i komercyjnych niezwiązanych z realizacją działań służbowych,
- należy upewnić się, że podany został prawidłowy adres odbiorcy informacji,
- należy zapewnić, że wykorzystywane do przesłania informacji urządzenie faksujące nie przechowuje przesyłki w swojej pamięci,
- nie pozostawiać wrażliwych informacji na urządzeniach typu automatyczna sekretarka.

2.7. Zasady bezpiecznego użytkowania laptopów

Laptopy podlegają tym samym regułom ochrony jak komputery stacjonarne, ponadto podlegają szczególnej ochronie prawnej ze względu na traktowanie ich jako przenośna baza danych, a szczególnie:

- powinny być zabezpieczone fizycznie podczas użytkowania, transportu oraz przechowywania przed dostępem osób nieuprawnionych i kradzieżą (np. specjalna torba, zabezpieczenie przed kradzieżą, niepozostawianie w widocznym miejscu w samochodzie),
- w trakcie pracy poza terenem kontrolowanym przez Urząd (np. w pociągu) należy zadbać, aby informacje sklasyfikowane, jako „Chronione prawem” oraz „Szczególnie chronione” nie były dostępne dla osób postronnych.

2.8. Postępowanie w przypadku naruszenia bezpieczeństwa informacji

Wszyscy pracownicy mają obowiązek natychmiastowego zgłaszania zauważonych incydentów bezpieczeństwa bezpośredniemu przełożonemu lub osobie odpowiedzialnej wskazanej w „Procedurze zarządzania incydentami bezpieczeństwa”. Dodatkowo, należy powstrzymać się od wszelkich działań, mogących utrudnić ustalenie okoliczności wystąpienia danego incydentu.

2.9. Zasady bezpiecznej pracy w zakresie ochrony informacji oraz przyjmowania Klientów w Urzędzie Gminy Kozy obowiązują następujące zasady pracy:

- Zasada czystego biurka: dokumenty papierowe i nośniki komputerowe, kiedy nie są używane przechowuje się w specjalnych segregatorach, teczkach, szafach, „korytkach” na półkach, wózkach rozliczeniowych, szczególnie poza godzinami pracy,
- pracownik zobowiązany jest do przechowywania wszystkich dokumentów zgodnie z wymaganiami „Klasyfikacji informacji”.
- Zasada czystego ekranu: w przypadku opuszczania stanowiska pracy, należy zablokować stację roboczą. O ile to możliwe, monitor powinien być ustawiony w taki sposób, by osoby postronne nie miały możliwości wglądu do przetwarzanych aktualnie informacji,
- Wygaszacze ekranu w stacjach roboczych zostały ustawione na 10 minut.
- Zasada odbioru wydruków z drukarki: wszelkie wydruki zawierające dane osobowe klientów, pracowników, informacje o firmie zabierane są natychmiast z drukarki po zakończeniu drukowania.

- Zasada zamykania pomieszczeń: ostatni pracownik opuszczający pomieszczenie zobowiązany jest do zamknięcia okien oraz drzwi zewnętrznych na klucz. Bezwzględnie zakazuje się pozostawiania klucza w zamku po zewnętrznej stronie drzwi.
- Zasada poufności rozmów: w przypadku prowadzenia rozmów (również telefonicznych) zarówno w siedzibie Urzędu Gminy Kozy jak i poza obszarem Urzędu należy zadbać, aby rozmowy nie były prowadzone w obecności osób nieupoważnionych do otrzymania tych informacji.
- Zasada nadzorowania Klientów: Klienci przyjmowani są w pomieszczeniach pracy tylko i wyłącznie pod nadzorem pracowników Urzędu Gminy Kozy,
- Pracownik opiekujący się osobą trzecią, zobowiązany jest, do nie pozostawiania jej bez nadzoru w przypadku, gdy istnieje możliwość spowodowania przez nią incydentu bezpieczeństwa (np. nieuprawnionego dostępu do informacji).

3. STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM (Zgodnie z Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., Dz. U. z 2004 r. Nr 100, poz. 1024, § 5 pkt. 2 rozporządzenia)

3.1. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora, a następnie właściwego hasła:

- Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.
- Identyfikator składa się minimalnie z czterech znaków, znaki identyfikatora nie są rozdzielone spacjami ani znakami interpunkcyjnymi, identyfikator nie zawiera polskich liter,
- Identyfikator wpisuje się do ewidencji, prowadzonej przez administratora bezpieczeństwa informacji, wraz z imieniem i nazwiskiem użytkownika oraz nazwami systemów informatycznych, do których użytkownik uzyskał dostęp i wprowadzany jest przez administratorów systemów informatycznych do właściwych systemów,
- Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego musi być zablokowany oraz nie może być przydzielany innej osobie.

3.2. System informatyczny przetwarzający dane osobowe jest konfigurowany w sposób wymagający bezpieczne zarządzanie hasłami użytkowników:

- hasło przydzielone użytkownikowi musi być zmienione po pierwszym udanym zalogowaniu się do systemu informatycznego przetwarzającego dane osobowe,
- hasła są zmieniane przez użytkownika,
- system informatyczny wyposażony jest w mechanizmy wymuszające zmianę hasła po upływie 30 dni od dnia ostatniej zmiany hasła,
- system informatyczny wyposażony jest w mechanizm pozwalający na wymuszenie jakości hasła, które powinno składać z co najmniej 8 znaków. Hasło powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

3.3. Osoby uprawnione do wykonywania prac administracyjnych w systemie informatycznym posiadają własne konta administracyjne. Zasady zarządzania hasłami są analogiczne, jak w przypadku haseł użytkowników. Nazwy i hasła użytkowników posiadających uprawnienia administratorów systemów informatycznych powinny być przechowywane w zamkniętej szafie, do której dostęp jest w pełni kontrolowany, przy czym dostęp do szafy mają wyłącznie uprawnione osoby. Nazwy użytkowników oraz hasła powinny być przechowywane w opieczętowanej i opatrzonej podpisem administratorów systemu kopercie. W przypadku konieczności awaryjnego użycia nazw i haseł tych użytkowników konieczny jest wpis ilustrujący zaistniałą sytuację w „Dzienniku haseł”, znajdującym się w szafie wraz z kopertą w której znajdują się hasła.

Wpis powinien zawierać następujące informacje:

- imię i nazwisko oraz stanowisko osoby upoważnionej udostępniającej dostęp do szafy, w której znajdują się hasła,
- imię i nazwisko oraz stanowisko osoby, która pobiera nazwy użytkowników i hasła,
- krótki opis sytuacji, która zmusiła do awaryjnego wykorzystania haseł.

O konieczności i okolicznościach awaryjnego użycia nazw i haseł musi niezwłocznie zostać powiadomiony Administrator Bezpieczeństwa Informacji.

4. PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONA DLA UŻYTKOWNIKÓW SYSTEMU (Zgodnie z Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., Dz. U. z 2004 r. Nr 100, poz. 1024, § 5 pkt. 3 rozporządzenia)

- 4.1. Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik obowiązany jest do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych. Szczegółowy opis takich symptomów oraz sposób postępowania w przypadku ich wykrycia został opisany w dokumencie „Polityka Bezpieczeństwa Informacji”.
- 4.2. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.
- 4.3. Maksymalna ilość prób wprowadzenia hasła przy logowaniu się do systemu wynosi trzy.
- 4.4. Po przekroczeniu tej liczby prób logowania system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowania konta może dokonać Administrator Systemu Informatycznego w porozumieniu z Administratorem Bezpieczeństwa Informacji. Użytkownik informuje Administratora Bezpieczeństwa Informacji o zablokowaniu dostępu do zbioru danych.
- 4.5. W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 10 minut automatycznie włączany jest wygaszacz ekranu. Wygaszacze ekranu powinny być zaopatrzone w hasła zbudowane analogicznie do haseł używanych przez użytkownika przy logowaniu.
- 4.6. Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jedno konto użytkownika.
- 4.7. W przypadku, gdy przerwa w pracy na stacji roboczej trwa dłużej niż 60 minut użytkownik obowiązany jest wylogować się z aplikacji i systemu stacji roboczej, na której pracuje oraz sprawdzić czy nie zostały pozostawione bez zamknięcia nośniki informacji zawierające dane osobowe.
- 4.8. W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane.
- 4.9. Zakończenie pracy w systemie informatycznym dokonuje się poprzez wylogowanie użytkownika ze wszystkich aplikacji oraz zamknięcie systemu operacyjnego komputera.

5. TWORZENIE KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA (Zgodnie z Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., Dz. U. z 2004 r. Nr 100, poz. 1024, § 5 pkt. 4 rozporządzenia)

- 5.1. Dane, w tym dane osobowe przetwarzane w systemie informatycznym, podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada Administrator Systemu Informatycznego lub osoba specjalnie do tego celu wyznaczona.
- 5.2. W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych użytkownicy systemu informatycznego zobowiązani są do centralnego przechowywania kopii danych, tak aby możliwe było zabezpieczenie ich dostępności poprzez wykonanie kopii zapasowych. Przez centralne przechowywanie kopii danych rozumie się cotygodniowe przegranie zbioru danych na specjalnie wydzielony do tego celu obszar dysku na serwerze. W przypadku, gdy z przyczyn technicznych jest to niemożliwe użytkownicy systemu są zobowiązani do sporządzania kopii zapasowych baz danych na nośniku wymiennym i centralne ich przechowywanie w miejscu wskazanym przez Administratora Bezpieczeństwa Informacji.
- 5.3. Kopie zapasowe informacji przechowywanych w systemie informatycznym przetwarzającym dane osobowe tworzone są w następujący sposób:
- dzienna kopia zapasowa baz danych - w tym danych osobowych - przetwarzanych przez systemy informatyczne, wykonywana jest codziennie po zakończeniu pracy Urzędu, zapisywana jest na przeznaczonym do tego celu serwerze kopii (serwer backup). Kopie dzienne baz danych przechowywane są na serwerze backup przez okres 2 tygodni.
 - dwutygodniowa kopia zapasowa baz danych - w tym danych osobowych - przetwarzanych przez systemy informatyczne wraz z uprawnieniami użytkowników (z każdego ostatniego dnia tygodnia) wykonywana jest co drugi tydzień na nośniku DVD. Tworzona kopia zawierająca bazy danych - w tym osobowych - przekazywana jest do przechowywania przy zachowaniu odpowiednich zabezpieczeń, w innym pomieszczeniu niż to, w którym znajdują się serwery danych. Zbiorcze (dwutygodniowe) kopie baz danych przechowywane są przez okres 6 lat, po tym terminie kopie są niszczone.
 - ze względu na uwarunkowania techniczne (przyrostowa baza danych) kopie zapasowe zawierają dane z okresów wcześniejszych.
 - kopia zapasowa aplikacji przetwarzających dane oraz danych konfiguracyjnych systemów informatycznych, tworzona jest przynajmniej raz w miesiącu, pomiędzy 1 a 10 jego dniem tak aby czas pomiędzy kopiami nie przekraczał 6 tygodni.
- 5.4. Do tworzenia kopii zapasowych wykorzystywane są dedykowane do tego celu urządzenia wchodzące w skład systemu informatycznego na nośnikach wymiennych adekwatnych do rodzaju urządzenia.
- 5.5. W przypadku przechowywania kopii zapasowych przez okres dłuższy niż 3 lata, wszystkie kopie zapasowe zbiorów danych osobowych, aplikacji przetwarzających dane osobowe oraz danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, których to dotyczy muszą być okresowo (co najmniej raz w roku) sprawdzane pod względem ich dalszej przydatności. Czynności te wykonuje Administrator Systemu Informatycznego. Z przeprowadzonego testu administrator systemu sporządza krótką notatkę uwzględniającą datę testu oraz jego rezultat (kopię notatki przekazuje Administratorowi Bezpieczeństwa Informacji).

6. Nośniki kopii zapasowych, które zostały wycofane z użycia, jeżeli jest to możliwe, należy pozbawić zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych Ponadto:

- Zbiory danych przechowywane są na serwerze obsługującym system informatyczny urzędu. Wszelkie dane przetwarzane w pamięci poszczególnych stacji roboczych oraz komputerów przenośnych są niezwłocznie umieszczane w odpowiednich, przydzielonych dla danego użytkownika przez Administratora Systemów Informatycznych miejscach na serwerze lub innych wskazanych i określonych lokalizacjach.
- Zakazuje się przetwarzania danych, w tym danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą elektroniczną przez użytkowników systemu informatycznego bez ich uprzedniego zaszyfrowania.
- W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego, użytkownik jest zobowiązany do sprawdzenia ich programem antywirusowym oraz oznakowania.
- Nośniki danych typu pendrive, zewnętrzne dyski twarde muszą być spisane. Administrator Systemów Informatycznych prowadzi ewidencję nośników przenośnych użytkowanych w systemie informatycznym urzędu oraz jednoznacznie je przypisuje personelowi.
- Nośniki magnetyczne raz użyte do przetwarzania danych osobowych mogą być wykorzystywane do innych celów, tylko po nadpisaniu danych w trybie kasowania formatującego przy zastosowaniu specjalistycznego oprogramowania lub demagnetyzacji. Nośniki na których nie można powtórnie zapisać informacji powinny być niszczone poprzez pocięcie, zgniecenie lub spopielenie.
- Nośniki magnetyczne z zaszyfrowanymi, jednostkowymi danymi osobowymi są – na czas ich użyteczności, przechowywane w zamkniętych na klucz szafach, a po wykorzystaniu dane na nich zawarte są trwale usuwane lub nośniki są niszczone w trybie niniejszej instrukcji.
- Kopie zapasowe programów i aktualizowane kopie systemu informatycznego urzędu przechowywane są w szafie pancерnej, stojącej w innym pomieszczeniu niż serwery.
- Po wygaśnięciu okresu przydatności tychże kopii (zastąpieniu ich przez aktualne wersje lub zakończeniu okresu trwałości), są one trwale kasowane lub nośniki je przechowujące niszczone mechanicznie.

6.1. Kopie zapasowe są ewidencjonowane przez ASI zgodnie z określonym schematem oznaczenia:

Data1/Nr/CZ

gdzie:

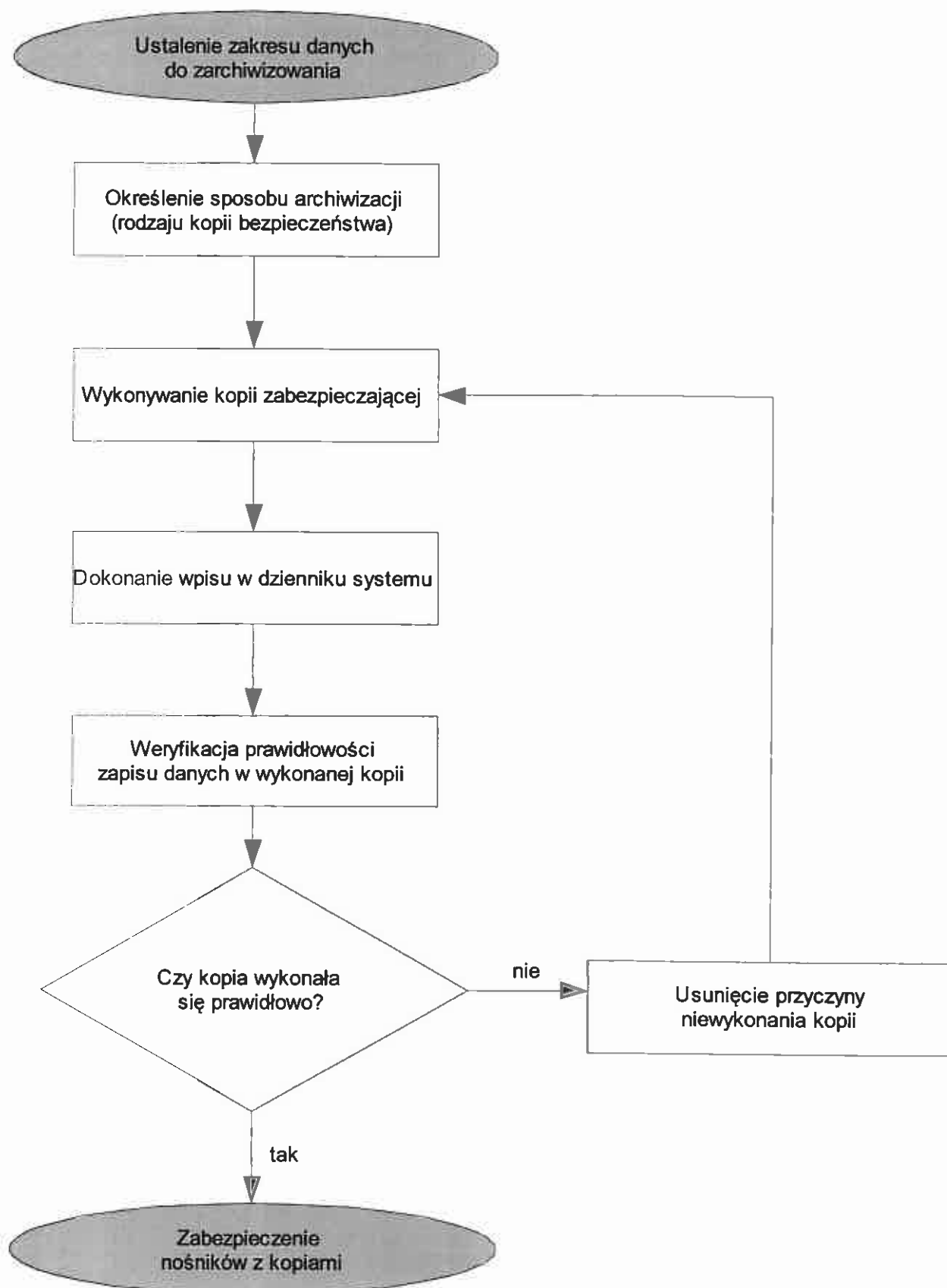
Data1 - czas utworzenia kopii

Nr – kolejny nr nośnika w danej części

CZ – ilość części w danym archiwum

Oznaczenie to jest trwale naniesione na nośnik kopii danych i wpisane do programowego rejestru kopii zapasowych. Kopie można wykonywać na płytach CD, kasetach, streamerach lub dyskach twardych.

Kopie wykonujemy na płytach CD/DVD.



- 7. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH** (Zgodnie z Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., Dz. U. z 2004 r. Nr 100, poz. 1024, § 5 pkt. 5 rozporządzenia)
- 7.1. Nośniki danych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne.
- 7.2. Nośniki danych, w tym danych osobowych oraz wydruki powinny być przechowywane w zamkniętych szafach wewnątrz obszaru przeznaczonego do przetwarzania danych osobowych i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar. Przekazywanie nośników danych osobowych i wydruków poza gmach urzędu powinno odbywać się za wiedzą Administratora Bezpieczeństwa Informacji.
- 7.3. Dane, w tym dane osobowe, przechowuje się w systemach elektronicznych zgodnie z ich okresem archiwizacji, określonym w JRWA. Po przekroczeniu wskazanego w JRWA terminu dane powinny zostać zablokowane przed edycją i podglądem w systemach informatycznych. Usunięcie całkowite danych z baz, tzw. brakowanie, powinno odbyć się równolegle z brakowaniem dokumentów tradycyjnych, poprzez nadpisanie odpowiednich rekordów. Czynność ta musi zostać potwierdzona przez Administratora Systemu Informatycznego oraz Administratora Bezpieczeństwa Informacji protokolarnie.
- 7.4. Dopuszcza się przechowywanie kopii bezpieczeństwa baz danych, z danymi, które uległy brakowaniu. Jest to możliwe jedynie w sytuacji, kiedy z kopii bezpieczeństwa nie można usunąć wybranych rekordów podlegających brakowaniu (ze względów technicznych lub usunięcie ich było by zbyt kosztowne), a pozostałe dane są aktualne i podlegają archiwizacji. W takim przypadku Administrator Systemu Informatycznego ma obowiązek odpowiedniego oznaczenia kopii bezpieczeństwa. W przypadku konieczności odtworzenia danych archiwalnych z kopii, ma obowiązek dopilnować, by nie doszło do odtworzenia danych, które zostały poddane brakowaniu. Każdorazowe użycie kopii bezpieczeństwa zawierającymi dane, które zostały wybrakowane, musi być pisemnie zatwierdzone przez Administratora Bezpieczeństwa Informacji, oraz zostać opisane w dzienniku systemu informatycznego.
- 7.5. W przypadku, gdy nośnik danych, w tym danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie danych z nośnika zgodnie z zasadami opisanymi w niniejszej instrukcji w pkt. 5 „Tworzenie kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania”. Jeżeli wydruk danych, w tym danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki do dokumentów.
- 7.6. W przypadku, gdy kopia zapasowa nie jest dłużej potrzebna, należy przeprowadzić jej zniszczenie lub usunięcie danych z nośnika, na którym się ona zgodnie ze wskazówkami zawartymi w niniejszej instrukcji w pkt. 5 „Tworzenie kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania”.
- 7.7. W przypadku dokonania brakowania dokumentów tradycyjnych lub przekazania ich do Archiwum Państwowego, należy odpowiadające im zapisy w bazach danych usunąć lub zabezpieczyć przed ich odczytaniem. Dokonanie brakowania dokumentów tradycyjnych, potwierdzone protokołem brakowania musi być skorelowane z protokołem brakowania (usunięcia) zapisów z baz danych na serwerach, stacjach roboczych a także z bieżących i archiwalnych kopii bezpieczeństwa.

8. ZABEZPIECZENIE PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO (Zgodnie z Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., Dz. U. z 2004 r. Nr 100, poz. 1024, § 5 pkt. 6 rozporządzenia)

8.1. W związku z tym, że system informatyczny narażony jest na działanie oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu konieczne jest podjęcie odpowiednich środków ochronnych.

Można wyróżnić następujące rodzaje występujących tu zagrożeń:

- nieuprawniony dostęp bezpośrednio do bazy danych,
- uszkodzenie kodu aplikacji umożliwiającej dostęp do bazy danych w taki sposób, że przetwarzane dane osobowe ulegną zafalszowaniu lub zniszczeniu,
- przechwycenie danych podczas transmisji w przypadku rozproszonego przetwarzania danych z wykorzystaniem ogólnodostępnej sieci Internet,
- przechwycenie danych z aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych przez wyspecjalizowany program szpiegowski i nielegalne przesłanie tych danych poza miejsce przetwarzania danych,
- uszkodzenie lub zafalszowanie danych osobowych przez wirus komputerowy zakłócający pracę aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych.

8.2. W celu przeciwdziałania wymienionym zagrożeniom system informatyczny musi posiadać następujące zabezpieczenia:

- fizyczne odseparowanie serwera bazy danych od sieci zewnętrznej,
- autoryzacja użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu,
- stosowanie rygorystycznego systemu autoryzacji dostępu do wszystkich serwerów, na których znajdują się elementy aplikacji umożliwiających przetwarzanie danych osobowych,
- stosowaniu aplikacji w postaci skompilowanej i nie umieszczenie kodu źródłowego aplikacji na powszechnie dostępnych serwerach,
- stosowanie szyfrowanej transmisji danych przy zastosowaniu odpowiedniej długości klucza szyfrującego,
- stosowanie odpowiedniej ochrony antywirusowej na stacjach roboczych wykorzystywanych do przetwarzania danych osobowych.

8.3. Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:

- załączniki do poczty elektronicznej,
- przeglądane strony internetowe,
- pliki i aplikacje pochodzące z nośników wymiennych uruchamiane i odczytywane na stacji roboczej.

8.4. W celu zapewnienia ochrony antywirusowej Administrator Systemu Informatycznego przetwarzającego dane osobowe lub osoba specjalnie do tego celu wyznaczona, jest odpowiedzialna za zarządzanie systemem wykrywającym i usuwającym wirusy. System antywirusowy powinien być skonfigurowany w następujący sposób:

- rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) powinien być stale włączony,
- antywirusowy skaner ruchu internetowego powinien być stale włączony,
- monitor zapewniający ochronę przed wirusami makr w dokumentach MS Office powinien być stale włączony,

- skaner poczty elektronicznej powinien być stale włączony.

8.5. Systemy antywirusowe zainstalowane na stacjach roboczych powinny być skonfigurowane w sposób następujący:

- zablokowanie możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego,
- możliwość centralnego uaktualnienia wzorców wirusów.

System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.

8.6. Użytkownicy systemu informatycznego zobowiązani są do następujących działań:

- bezwzględnego skanowania zawartości nośników wymiennych odczytywanych na stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów - przy każdym odczycie,
- skanowania informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów - na bieżąco.

8.7. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy Administrator Systemu Informatycznego lub inny wyznaczony pracownik powinien podjąć działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:

- usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,
- odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,
- samodzielną ingerencję w zawartość pliku - w zależności od posiadanych kwalifikacji lub skonsultowanie się z zewnętrznymi ekspertami.

8.8. System informatyczny przetwarzający dane osobowe powinien posiadać mechanizmy pozwalające na zabezpieczenie ich przed utratą lub wystąpieniem zafałszowania w wyniku awarii zasilania lub zakłóceń w sieci zasilającej. W związku z tym system informatyczny powinien być wyposażony w co najmniej:

- filtry zabezpieczające stacje robocze przed skutkami przepięcia,
- zasilacze awaryjne serwerów baz danych, serwerów aplikacji oraz urządzeń pamięci masowej pozwalające na bezpieczne zamknięcie aplikacji przetwarzających dane osobowe w sposób umożliwiający poprawne zapisanie przetwarzanych danych.

9. REALIZACJA WYMOGU UWIERZYTELNIENIA UŻYTKOWNIKA I REJESTRACJI ZDARZEŃ (Zgodnie z Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., Dz. U. z 2004 r. Nr 100, poz. 1024, § 7 ust. 1 pkt. 4 rozporządzenia)

- 9.1. System informatyczny przetwarzający dane, w tym dane osobowe musi posiadać mechanizm uwierzytelniający użytkownika, wykorzystujący identyfikator i hasło. Powinien także posiadać mechanizmy pozwalające na określenie uprawnień użytkownika do korzystania z przetwarzanych informacji (np. prawo do odczytu danych, modyfikacji istniejących danych, tworzenia nowych danych, usuwania danych).
- 9.2. System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:
- rozpoczęcie i zakończenie pracy przez użytkownika systemu,
 - operacje wykonywane na przetwarzanych danych, a w szczególności ich dodanie, modyfikację oraz usunięcie,
 - przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu,
 - nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
 - błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.
 - zapis działań użytkownika uwzględnia:
 - identyfikator użytkownika,
 - datę i czas, w którym zdarzenie miało miejsce,
 - rodzaj zdarzenia,
 - określenie informacji, których zdarzenie dotyczy (identyfikatory rekordów).
- 9.3. W ramach możliwości technicznych system informatyczny powinien posiadać mechanizmy pozwalające na automatyczne powiadomienie Administratora Bezpieczeństwa Informacji lub osoby przez niego uprawnionej o zaistnieniu zdarzenia krytycznego (mogącego mieć krytyczne znaczenie dla bezpieczeństwa przetwarzanych danych osobowych).
- 9.4. Ponadto system informatyczny powinien zapewnić zapis faktu przekazania danych, w tym danych osobowych z uwzględnieniem:
- identyfikatora osoby, której dane dotyczą
 - osoby przesyłającej dane,
 - odbiorcy danych,
 - zakresu przekazanych danych osobowych,
 - daty operacji,
 - sposobu przekazania danych.

10. PRZEGLĄD I KONSERWACJA SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

- 10.1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
- 10.2. Prace serwisowe na terenie urzędu prowadzone w tym zakresie mogą być wykonywane wyłącznie przez pracowników urzędu lub przez upoważnionych przedstawicieli wykonawców zewnętrznych będących pod nadzorem pracowników urzędu.
- 10.3. Przed rozpoczęciem prac serwisowych przez osoby spoza Urzędu Gminy Kozy, a nie będących pracownikami urzędu, konieczne jest potwierdzenie tożsamości serwisantów.
- 10.4. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane, w tym dane osobowe, przeznaczone do:
- likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
 - przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
 - naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.
- 10.5. Wszelkie prace serwisowe prowadzone na sprzęcie urzędu w jego siedzibie lub w siedzibie serwisu, muszą być potwierdzone protokołem opisującym czas, datę rozpoczęcia i zakończenia prac, zakres prac oraz osoby prowadzące prace.
- 10.6. W przypadku prowadzenia prac w trybie zdalnym musi być sporządzona notatka lub wpis do dziennika systemu informatycznego, zawierający informacje o:
- czasie trwania prac,
 - ich zakresie,
 - osobie prowadzącej serwis,
- zgodnie z pkt. 13. niniejszej instrukcji.

11. POSTĘPOWANIE W PRZYPADKU STWIERDZENIA NARUSZENIA BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

11.1. Użytkownik zobowiązany jest powiadomić Administratora Systemów Informatycznych lub uprzednio wskazanego przez niego pracownika służb informatycznych Urzędu Gminy Kozy o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:

- naruszeniu identyfikatora i hasła (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła),
- częściowym lub całkowitym braku danych,
- braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera,
- wykryciu wirusa komputerowego,
- zauważeniu elektronicznych śladów próby włamania do systemu informatycznego Urzędu Gminy Kozy,
- podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe,
- zmianie położenia sprzętu komputerowego,
- zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf,

11.2. Do czasu przybycia na miejsce Administratora Systemów Informatycznych należy:

- niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, o ile istnieje taka możliwość,
- następnie uwzględnić w działaniu również ustalenie jego przyczyn i sprawców,
- rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
- zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
- zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku,
- nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia Administratora Systemów Informatycznych.

11.3. Administrator Systemów Informatycznych po otrzymaniu zawiadomienia, o którym mowa w ust.1, powinien niezwłocznie:

- przeprowadzić postępowanie wyjaśniające, w celu ustalenia okoliczności naruszenia ochrony danych osobowych,
- podjąć działania chroniące system przed ponownym naruszeniem,
- w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu, sporządzić raport naruszenia bezpieczeństwa systemu informatycznego Urzędu Gminy Kozy, a następnie niezwłocznie przekazać go Administratorowi Bezpieczeństwa Informacji.

11.4. W dalszym trybie postępowania należy, powiadomić właściwe organy oraz podjąć inne, szczególne czynności zapewniające bezpieczeństwo systemu informatycznego Urzędu Gminy Kozy, bądź podjąć środki ochrony fizycznej. Decyzję podejmuje Wójt Gminy Kozy po zapoznaniu się z otrzymanym od Administratora Systemu Informatycznego raportem o zaistniałym incydencie.

11.5. Administrator Systemów Informatycznych jest zobowiązany do informowania ADO i ABI o awariach systemu informatycznego Urzędu Gminy Kozy, zauważonych przypadkach naruszenia niniejszej instrukcji przez użytkowników danych, w szczególności o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania programów antywirusowych, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z

procedurami ochrony danych osobowych.

12. TRYB PRACY PRZY PRZETWARZANIU DANYCH W TYM DANYCH OSOBOWYCH

12.1. Przy przetwarzaniu danych należy zachować wymogi bezpieczeństwa danych, ich ochrony przed utratą i kradzieżą.

12.2. Tryb pracy na stacjonarnych stacjach roboczych:

- Rozpoczęcie pracy na stacji roboczej, następuje po włączeniu zasilania komputera, a następnie wprowadzeniu indywidualnego, znanego tylko użytkownikowi identyfikatora i hasła.
- W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie użytkownika danych osobowych, Administratora Danych Osobowych lub Administratora Systemów Informatycznych.
- Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać podgląd), wydruki leżące na biurkach oraz w otwartych szafach.
- Stacje robocze wyposażone są we włączające się, po 10 minutach od przerywania pracy, wygaszacze ekranu lub też w systemy wylogowania użytkownika. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła do systemu operacyjnego stacji roboczej lub systemu informatycznego aktualnie użytkowanego.
- W przypadku opuszczenia stanowiska pracy, użytkownik obowiązany jest aktywizować wygaszacz ekranu lub w inny sposób zablokować stację roboczą.
- W przypadku, gdy przerwa w pracy na stacji roboczej może trwać dłużej niż 60 minut użytkownik obowiązany jest wylogować się z aplikacji i systemu stacji roboczej, na której pracuje oraz sprawdzić czy nie zostały pozostawione bez zamknięcia nośniki informacji zawierające dane osobowe
- Obowiązuje zakaz robienia kopii zbiorów danych przez użytkownika stacji roboczej. Całe zbiory danych kopiowane są tylko przez Administratora Systemów Informatycznych lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych.
- Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich 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.
- Jednostkowe dane mogą być przekazywane pocztą elektroniczną pomiędzy komputerami Urzędu Gminy Kozy, a komputerami przenośnymi używanymi przez upoważnionych pracowników Urzędu tylko po ich zaszyfrowaniu.
- Wypisy ze zbiorów danych udostępniane zgodnie z art. 7 ust. 6 ustawy o ochronie danych osobowych można przysyłać pocztą elektroniczną tylko w postaci zaszyfrowanej.
- Obowiązuje zakaz wynoszenia, na jakichkolwiek nośnikach, całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej. W przypadku uzasadnionej konieczności wynoszenia zbiorów danych (aktywów) poza obręb Urzędu Gminy Kozy wymagana jest pisemna zgoda ADO oraz konieczność zarejestrowania tego faktu w rejestrze stwierdzającym fakt pobrania danych i ich zakresu oraz w rejestrze zwrotu zbioru.
- Zakończenie pracy na stacji roboczej następuje po wprowadzeniu danych tego dnia, przetwarzanych w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera.

12.3. Przed opuszczeniem pokoju należy:

- zniszczyć w niszczarce lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe,
- schować do zamykanych na klucz szaf wszelkie akta zawierające dane osobowe,
- umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,
- zamknąć okna,
- Opuszczając pokój należy zamknąć za sobą drzwi na klucz. Klucz do pokoju przechowywany jest w schowku na klucze w pokoju nr 3. Jeśli niemożliwe jest umieszczenie wszystkich dokumentów

zawierających dane osobowe w zamykanych szafach, należy powiadomić o tym ABI, który zgłasza jednorazową rezygnację z wykonania usługi sprzątnia. W takim przypadku także należy zostawić klucz w schowku na klucze w pokoju nr 3.

12.4. Tryb pracy na komputerach przenośnych:

- Na ile to możliwe, przy przetwarzaniu danych osobowych na komputerach przenośnych, obowiązują wymogi dotyczące pracy na komputerach stacjonarnych.
- Komputery przenośne użytkownicy, którym zostały one powierzone, powinni chronić przed uszkodzeniem, kradzieżą i dostępem osób postronnych, szczególną ostrożność należy zachować podczas ich transportu.
- Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone.
- Praca na komputerze przenośnym możliwa jest po wprowadzeniu indywidualnego identyfikatora i osobistego hasła. System automatycznie wymusza systematyczną zmianę hasła przez Administratora Systemów Informatycznych lub użytkownika.
- Pliki zawierające dane osobowe przechowywane na komputerach przenośnych są zaszyfrowane i opatrzone hasłem dostępu.
- Obowiązuje zakaz przetwarzania na komputerach przenośnych całych zbiorów danych nawet w postaci zaszyfrowanej.
- Użytkownicy danych przetwarzanych na komputerach przenośnych obowiązani są raz na kwartał do wprowadzania ich w określone miejsca na serwerze (wprowadzania do systemu informatycznego Urzędu Gminy Kozy), a następnie do nadpisywania tych danych w pamięci powierzonych komputerów przenośnych.
- Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach przenośnych. Wszelkie zmiany mogą być dokonywane tylko pod nadzorem Administratora Systemów Informatycznych, stosownie do wymagań niniejszej instrukcji. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania, należy zgłosić to Administratorowi Systemów Informatycznych.
- Komputery przenośne wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizację sugeruje automatycznie system.
- Wykorzystanie zewnętrznych informatycznych nośników danych wymaga wcześniejszego sprawdzenia pod kątem zawartości szkodliwego oprogramowania każdorazowo przed ich użyciem.

13. AUTORYZACJA NOWYCH URZĄDZEŃ W SIECI LAN URZĘDU GMINY KOZY

13.1. Autoryzacji podlegają wszystkie nowe modele urządzeń mające być użyte w sieci Urzędu Gminy Kozy. Autoryzacji podlega również sprzęt nie będący własnością Urzędu, służący do przetwarzania danych związanych z działalnością (sprzęt osobisty).

13.2. Proces autoryzacji polega na:

- kontroli specyfikacji urządzenia
- o ile zachodzi taka konieczność - testach urządzenia.

13.3. Kontrola specyfikacji urządzenia polega na:

- Sprawdzeniu, czy urządzenie posiada certyfikaty i homologacje wymagane na terenie kraju.
- Sprawdzeniu czy urządzenie spełnia wymagania techniczne dotyczące podłączenia go do infrastruktury Urzędu Gminy Kozy (interfejsy sieciowe)
- Sprawdzeniu czy urządzenie spełnia wymagania bezpieczeństwa systemów, oraz wymagania niniejszej instrukcji w pkt. 9 "Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego"
- Sprawdzenie czy urządzenie posiada funkcjonalność umożliwiającą zastosowanie odpowiednich polityk dostępu.

Wyżej opisane testy mogą polegać na analizie specyfikacji urządzenia, bądź w uzasadnionych przypadkach na testach samego urządzenia.

14. NADZOROWANIE OTWIERANIA TUNELI VPN W CELACH SERWISOWYCH

- 14.1. Firmy zewnętrzne, realizujące usługi serwisowe dla Urzędu Gminy Kozy, uzyskują dostęp do programów i aplikacji znajdujących się na serwerach Urzędu przez szyfrowany tunel VPN.
- 14.2. Serwis zewnętrzny, każdorazowo przed podjęciem usługi musi zawiadomić ASI, o konieczności otwarcia portu VPN po stronie Urzędu. Zgłoszenie musi określać:
- jaki jest cel połączenia VPN (naprawa aplikacji, aktualizacja),
 - która aplikacja będzie serwisowana,
 - jaki jest przewidywany czas połączenia,
- 14.3. Podczas jakichkolwiek działań przeprowadzanych zdalnie na urządzeniach Urzędu, ABI, ASI lub wyznaczony przez nich pracownik Urzędu zobligowani są do ciągłego śledzenia czynności wykonywanych przez osobę zewnętrzną.
- 14.4. Po uzgodnieniu przez serwisującego i osobę nadzorującą zakończenia prac i przetestowaniu prawidłowego działania, ASI ma obowiązek bezwzględnego pozamykania wszystkich otwartych portów VPN.
- 14.5. Bez względu na czas trwania usługi, ASI ma obowiązek zamknąć wszystkie otwarte porty VPN po zakończeniu pracy w danym dniu.
- 14.6. Wszystkie otwarcia portów VPN muszą być ewidencjonowane w Dzienniku Systemu Informatycznego

WÓJT
Krzysztof
mgr Krzysztof Fiatkowski