ZARZĄDZENIE Nr 11/2017
Dyrektora Centrum Usług Wspólnych w Gminie Żabia Wola
w Gminie Żabia Wola

z dnia 4 kwietnia 2017 r.

w sprawie wprowadzenia Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Centrum Usług Wspólnych w Gminie Żabia Wola

Na podstawie: art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. 2016 r. poz. 922) oraz § 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)zarządza się, co następuje:

§ 1.

1. Wprowadza się do stosowania w Centrum Usług Wspólnych w Lidzbarku Warmińskim Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Centrum Usług Wspólnych w Gminie Żabia Wola, w brzmieniu stanowiącym ***Załącznik*** do niniejszego zarządzenia.
2. Do stosowania zasad określonych w Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Centrum Usług Wspólnych w Gminie Żabia Wola zobowiązani są wszyscy pracownicy Jednostki oraz inne osoby mające dostęp do informacji podlegających ochronie.

§ 2.

Zarządzenie wchodzi w życie w dniem podpisania.

DYREKTOR
Justyna Wodnicka-Żuk

ZAŁĄCZNIK do Zarządzenia Nr 11/2017
Dyrektora Centrum Usług Wspólnych w Gminie
Żabia Wola z dnia 4 kwietnia 2017 r. w sprawie
wprowadzenia Instrukcji zarządzania systemami
informatycznymi służącymi do przetwarzania
danych osobowych
w Centrum Usług Wspólnych
w Gminie Żabia Wola

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH W CENTRUM USŁUG WSPÓLNYCH W GMINIE ŻABIA WOLA

§ 1.
WPROWADZENIE

1. Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Centrum Usług Wspólnych w Gminie Żabia Wola zwana dalej „**instrukcją**" określa zasady eksploatacji i zarządzania systemami zgodne z obowiązującymi wymaganiami prawnymi, w szczególności:
   1) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*t. j. Dz. U. 2016 r. poz. 922*);
   2) Ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (*tekst jednolity: Dz. U. 2014 r. poz. 1114 z późn. zm.);*
   3) Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (*Dz. U. 2012 r. poz. 526);*
   4) Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. (*Dz. U. z 2004 r. nr 100, poz. 1024*).
2. Każda osoba przetwarzająca dane osobowe za pośrednictwem systemów informatycznych zobowiązana jest do zapoznania się z treścią niniejszej instrukcji i do bezwzględnego stosowania zawartych w niej zasad. Zapoznanie z instrukcją potwierdzone jest poprzez złożenie pisemnego oświadczenia, którego wzór stanowi ***Załącznik Nr 8 do Polityki bezpieczeństwa i ochrony przetwarzania danych osobowych.***
3. Ewidencję osób zapoznanych z niniejszą instrukcją prowadzi Administratora Danych

Osobowych (wzór ewidencji stanowi ***Załącznik Nr 1 do Instrukcji***).

4. W instrukcji stosuje się następujące skróty:
   1) **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
   2) **Administrator Danych Osobowych (ADO)** – Centrum Usług Wspólnych w Gminie Żabia Wola reprezentowane przez Dyrektora;
   3) **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
   4) **Stacja robocza** – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie;
   5) **Przetwarzanie danych osobowych** - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie;
   6) **Osoba upoważniona** - osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych lub osobę przez niego uprawnioną dopuszczona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu;
   7) **Użytkownik systemu** - osoba posiadająca uprawnienia do przetwarzania danych osobowych w systemie informatycznym;
   8) **Ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych *(t. j. Dz. U. 2016 r. poz. 922*);
   9) **Rozporządzenie** - rozporządzenie 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 r. nr 100, poz. 1024).*

§ 2.

PROCEDURA NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI

1. Podstawą do nadania uprawnień do przetwarzania danych osobowych w systemie informatycznym Centrum jest upoważnienie do przetwarzania danych osobowych.

Upoważnienie wydawane jest przez Administratora Danych Osobowych. (wzór upoważnienia stanowi ***Załącznik Nr 5 do Polityki bezpieczeństwa***)

2. Administrator Danych Osobowych
   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.
3. Oryginał upoważnienia zostaje przekazany pracownikowi (za potwierdzeniem odbioru) natomiast kopia trafia do jego akt osobowych.
4. Administratora Danych Osobowych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, która stanowi ***Załącznik Nr 6 do Polityki bezpieczeństwa***. Każda zmiana w zakresie informacji zawartych w ewidencji podlega niezwłocznemu odnotowaniu przez ADO.
5. W przypadku nadawania użytkownikowi uprawnień do danego systemu informatycznego po raz pierwszy, ADO lub osoba przez niego upoważniona, dokonuje nadania użytkownikowi identyfikatora, wygenerowania hasła oraz wpisania identyfikatora do upoważnienia oraz ewidencji osób upoważnionych do przetwarzania danych osobowych.
6. 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.
7. Hasło użytkownika jest przydzielane indywidualnie każdemu z użytkowników i znane jest tylko użytkownikowi, który się nim posługuje.
8. ADO lub osoba przez niego upoważniona przekazuje użytkownikowi identyfikator i hasło.
9. Użytkownik jest zobowiązany do zmiany hasła przy pierwszym dostępie do systemu informatycznego.

§ 3.
PROCEDURA ODBIERANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH W SYSTEMIE INFORMATYCZNYM

1. W związku ze zmianą zakresu obowiązków służbowych pracownika lub zakończeniem jego pracy Administrator Danych Osobowych dokonuje, odebrania lub zmiany zakresu upoważnienia.

2. W przypadku konieczności odebrania lub zmiany zakresu upoważnienia dla osób nie będących pracownikami Centrum o wykonanie powyższej czynności wnioskuje pracownik Centrum koordynujący działania danej osoby.

§ 4.

STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

1. Użytkownicy systemu informatycznego przetwarzającego dane osobowe wykorzystują w procesie uwierzytelnienia identyfikatory i hasła.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi i nie podlega zmianie.
3. Nowe hasło jest przekazywane użytkownikowi przez ADO.
4. Po zalogowaniu do systemu z wykorzystaniem otrzymanego hasła użytkownik jest zobowiązany do dokonania jego natychmiastowej zmiany, nawet, jeżeli system informatyczny nie wymusza takiego działania.
5. Hasła dostępu do systemu informatycznego muszą spełniać poniższe warunki:
   1) posiadać długość co najmniej 8 znaków;
   2) zawierać przynajmniej jedną cyfrę oraz znak specjalny/ zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
6. Hasło 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.
7. 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 innych użytkowników systemu.
8. W przypadku zapomnienia hasła użytkownik powinien zwrócić się do ADO o wygenerowanie nowego hasła.
9. W przypadku podejrzenia zapoznania się z hasłem przez osobę nieuprawnioną lub podejrzenia naruszenia bezpieczeństwa działania systemu informatycznego służącego do przetwarzania danych osobowych poprzez np. brak możliwości zalogowania pomimo wprowadzenia poprawnego identyfikatora oraz hasła lub stwierdzenie fizycznej ingerencji, użytkownik jest

zobowiązany do natychmiastowej zmiany hasła oraz powiadomienia o zaistniałym fakcie ADO. Administrator Danych Osobowych po otrzymaniu zgłoszenia o naruszeniu lub podejrzeniu naruszenia bezpieczeństwa i ochrony danych przetwarzanych za pośrednictwem systemu informatycznego przeprowadza sprawdzenie doraźne zgodnie z procedurą określoną w Polityce Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych.

10. Co najmniej raz w roku ADO przeprowadza kontrolę dotyczącą posiadania przez użytkowników stosownych upoważnień do przetwarzania danych osobowych.

§ 5.
PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONA DLA UŻYTKOWNIKÓW SYSTEMU

1. 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 ADO;
   5) w przypadku niestandardowego zachowania aplikacji przetwarzającej dane osobowe pracownik natychmiast powiadamia o zaistniałym fakcie ADO.
2. W przypadku bezczynności użytkownika przez okres dłuższy niż 5 min automatycznie włączy się wygaszacz ekranu Kontynuacja pracy może nastąpić po odblokowaniu stacji roboczej po wprowadzeniu hasła, w sposób gwarantujący jego niepodejrzenie przez osoby trzecie.
3. Zmianę użytkownika systemu informatycznego każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jeden identyfikator. W przypadku, gdy przerwa w pracy ma trwać dłużej niż 60 minut użytkownik obowiązany jest wylogować się z systemu informatycznego oraz sprawdzić czy nie zostały pozostawione bez zamknięcia nośniki informacji zawierające dane osobowe.

4. W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne monitory stanowisk dostępu do danych są ustawione w taki sposób żeby uniemożliwić tym osobom wgląd w dane.
5. 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.

6. Dostęp do pomieszczeń Centrum, w którym przetwarzane są dane osobowe zabezpieczony jest poprzez wprowadzenie środków technicznych i organizacyjnych określonych w Polityce Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych.
7. Dokładną lokalizację elementów wchodzących w skład infrastruktury informatycznej określa ***Załącznik Nr 2 do Instrukcji***.
8. 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 oraz zamyka na klucz drzwi do pomieszczenia.

§ 6.
PROCEDURA TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. Za tworzenie i przechowywanie kopii zapasowych odpowiedzialny jest pracownik Centrum, który je wytwarza.
2. Nośniki elektroniczne zawierające kopie zapasową zbiorów danych osobowych przechowywane są w innych pomieszczeniach niż systemy informatyczne, na których zostały utworzone w sposób uniemożliwiający dostęp do nich przez osoby nieupoważnione.
3. ADO odpowiada za prowadzenie ewidencji wykonania kopii zapasowych. (***Załącznik Nr 3 do Instrukcji***)
4. Administrator Danych Osobowych określa czas przechowywania poszczególnych kopii zapasowych, w zależności od celu przetwarzania danych zapisanych na kopiach zapasowych.
5. Kopie zapasowe:
   1) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
   2) usuwa się niezwłocznie po ustaniu ich użyteczności.

§ 7.
SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ NOŚNIKÓW KOPII ZAPASOWYCH

1. Dane osobowe przechowywane są w postaci elektronicznej na:

1) nośnikach magnetycznych wbudowanych w sprzęt informatyczny lub stanowiących element tego systemu;
2) przenośnych dyskach zewnętrznych.

2. Dane przechowywane są na dyskach przenośnych 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 dysku podlega skasowaniu przy użyciu narzędzi zaakceptowanych do użycia w Jednostce.
3. 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.
4. Przenośne dyski zewnętrzne z informacjami zawierającymi dane osobowe są przechowywane przez pracowników w sposób minimalizujący ryzyko ich uszkodzenia lub zniszczenia, w szczególności w zamykanych szafach i meblach biurowych. ADO wyznacza pomieszczenia, w których mogą być przechowywane takie nośniki.
5. 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 Centrum. W przypadku braku możliwości programowego usunięcia danych dysk podlega fizycznemu zniszczeniu. Za zniszczenie danych odpowiada zewnętrzna firma informatyczna.
6. Dopuszcza się powierzenie niszczenia dysków z danymi wyspecjalizowanym podmiotom zewnętrznym, pod warunkiem:
   1) zawarcia umowy, o której mowa w art. 31 UODO;
   2) zagwarantowania poufności danych przez usługodawcę;
   3) umożliwienia prowadzenia nadzoru nad procesem niszczenia dysków przez ABI lub upoważnionego przez niego pracownika Centrum;
   4) udokumentowania faktu zniszczenia dysków protokołem.

§ 8.

SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM DZIAŁANIA JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

1. W celu zabezpieczenia systemu informatycznego przed działaniem niebezpiecznego oprogramowania zabrania się:

1) uruchamiania jakiegokolwiek oprogramowania, które nie zostało zatwierdzone do użytku w Centrum;
2) otwierania poczty elektronicznej, której tytuł nie sugeruje związku z pełnionymi obowiązkami służbowymi; w przypadkach wątpliwych należy skonsultować się z ADO;
3) korzystania z Internetu w celach nie związanych z pełnionymi obowiązkami służbowymi;

2. W przypadku zauważenia objawów mogących wskazywać na obecność niebezpiecznego oprogramowania użytkownik jest zobowiązany powiadomić ADO. Do objawów powyższych można zaliczyć:
   1) istotne spowolnienie działania systemu informatycznego;
   2) nietypowe działanie aplikacji;
   3) nietypowe komunikaty;
   4) utratę danych lub modyfikację danych.
3. System informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:
   1) działanie oprogramowania antywirusowego;
   2) zaporę sieciową;
   3) automatyczną aktualizację oraz pobranie nowej bazy wirusów (nie rzadziej niż raz dziennie);
   4) konfigurację oprogramowania minimalizującą ryzyko naruszenia bezpieczeństwa.

§ 9.
SPOSÓB REALIZACJI WYMOGÓW ODNOTOWANIA INFORMACJI O ODBIORCACH

1. Systemy informatyczne odnotowują:
   1) datę pierwszego wpisu do systemu;
   2) identyfikator użytkownika wprowadzającego dane osobowe do systemu;
   3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
   4) informacje o odbiorach danych osobowych;
   5) informacji o wniesieniu sprzeciwu wobec przetwarzania danych osobowych.
2. Odnotowanie to odbywa się automatycznie.
3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, systemy zapewniają sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1 niniejszego paragrafu.

§ 10.

PROCEDURA WYKONYWANIA PRZEGLĄDU I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Przegląd i konserwacja sprzętu informatycznego realizowany jest przez podmioty zewnętrzne.
2. Prace serwisowe wykonywane na terenie Jednostki przez podmioty zewnętrzne podlegają bezpośredniemu nadzorowi ADO.
3. Przed rozpoczęciem prac serwisowych przez osoby postronne konieczne jest potwierdzenie tożsamości serwisantów. Urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe, przeznaczone do:
   1) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
   2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
   3) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej.
4. 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 Centrum);
   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.

§ 11.

POSTANOWIENIA KOŃCOWE

W sprawach nieokreślonych niniejszą Instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych w Centrum urządzeń i programów.

DYREKTOR
Justyna Wodnicka-Żuk

ZAŁĄCZNIK NR 1
do Instrukcji Zarządzania Systemami Informatycznymi
w Centrum Usług Wspólnych w Gminie Żabia Wola

EWIDENCJA OSÓB

ZAPOZNANYCH Z INSTRUKCJĄ ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI W CENTRUM USŁUG WSPÓLNYCH W GMINIE ŻABIA WOLA

Przyjąłem/am do wiadomości i stosowania zapisy
Instrukcji zarządzania systemami informatycznymi

Lp.	Nazwisko i imię	Data i podpis
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		

LOKALIZACJA ELEMENTÓW WCHODZĄCYCH W SKŁAD INFRASTRUKTURY INFORMATYCZNEJ

Elementy infrastruktury sieciowej (modemy, routery, switch'e, hub'y):

Lp.:	Nazwa i model urządzenia	Lokalizacja
1.	Router Archer D7 TP-Link	Pomieszczenie 1
2.	Switch TL-SG1008D TP-Link	Pomieszczenie 3
3.	Switch D-Link DES-1008D	Pomieszczenie 3

Elementy służące do przetwarzania danych osobowych (serwery, stacje robocze, terminale, dyski sieciowe):

Lp.	Nazwa / model	Lokalizacja	Zastosowana metoda dostępu
1.	Dysk sieciowy QNAP TS-251	Pomieszczenie 3	za pośrednictwem sieci lokalnej
2.	Stacja robocza NTT	Pomieszczenie 3	za pośrednictwem sieci lokalnej
3.	Stacja robocza NTT	Pomieszczenie 3	za pośrednictwem sieci lokalnej
4.	Stacja robocza DELL Vostro 3800 Series	Pomieszczenie 2	za pośrednictwem sieci lokalnej
5.	Stacja robocza DELL OptiPlex 5040	Pomieszczenie 2	za pośrednictwem sieci lokalnej
6.	Laptop Toshiba Satellite Pro R50-B-119	Pomieszczenie 1	za pośrednictwem sieci lokalnej

ZAŁĄCZNIK NR 3
do Instrukcji Zarządzania Systemami Informatycznymi
w Centrum Usług Wspólnych w Gminie Żabia Wola

wzór

EWIDENCJA WYKONYWANYCH KOPII ZAPASOWYCH

Lp.	Nazwa zbioru:	Imię i nazwisko osoby sporządzającej kopię	Data sporządzenia kopii	Częstotliwość wykonywania kopii zapasowej (dzienna/ tygodniowa/ miesięczna)	Rodzaj nośnika:	Sposób wykonania kopii zapasowej:	Miejsce przechowywania:	Informacja o zniszczeniu
1.								
2.								
3.								
4.								
5.								