ZARZĄDZENIE NR 39/2016
WÓJTA GMINY KLUKOWO

z dnia 6 grudnia 2016 r.

w sprawie wprowadzenia procedur do Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy w Klukowie

Na podstawie: art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz.U. z 2016 poz. 922) oraz § 3 ust. 3, § 4, § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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) oraz art. 33 ust.3 ustawy z dnia 4 kwietnia 2016 r. o samorządzie gminnym (tekst jednolity Dz.U. z 2016 r. poz. 446 ze zm.) zarządza się co następuje:

§ 1. Wprowadzam procedury do **Instrukcji Zarządzania SystememInformatycznym w Urzędzie Gminy w Klukowie**, zwane dalej *Procedurami* stanowiące załącznik nr 1,2,3 i 4 do niniejszego zarządzenia.

§ 2. Nadzór nad wykonaniem zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji.

§ 4. Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT
mgr Piotr Uszyński

Sprawdzono pod względem formalnym i prawnym
dn. 22.12.2016
WOJCIECH SROCKI
RADCA PRAWNY

Załącznik Nr 1 do Zarządzenia Nr 39/2016
Wójta Gminy Klukowo
z dnia 6 grudnia 2016 r.

Procedura Alarmowa

Administrator Danych – .....

dnia ..... w podmiocie o nazwie ..... w celu pełnej kontroli oraz zapobieganiu możliwym zagrożeniom związanym z ochroną danych osobowych na podstawie art. 36.1. ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285)

wdraża dokument o nazwie **„Procedura Alarmowa".**

Zapisy tego dokumentu wchodzą w życie z dniem ..... roku.

Definicje:

Uchybienie - świadome lub nieświadome działania zmierzające do zagrożenia, wskutek których może dojść do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.

Zagrożenie - świadome lub nieświadome działania, wskutek których doszło do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.

ABI -Administrator Bezpieczeństwa Informacji

ADO -Administrator Danych Osobowych

1. Procedura alarmowa

Procedura alarmowa wskazuje na możliwe zagrożenia oraz definiuje „Dziennik Uchybień i Zagrożeń", związany z niewłaściwym przetwarzaniem danych osobowych lub ich wyciekiem. Celem Procedury Alarmowej jest skatalogowanie możliwych uchybień i zagrożeń oraz opisanie procedur działania w przypadku ich wystąpienia, jak i również ograniczenie ich powstania w przyszłości. Integralną częścią Procedury Alarmowej jest „Dziennik Uchybień i Zagrożeń" (załącznik nr 1), „Protokół Zagrożenia"

(załącznik nr 2), „Protokół Uchybienia" -(załącznik nr 3), prowadzony przez ABI w przypadku stwierdzenia naruszenia ochrony danych osobowych w podmiocie.

2. Charakterystyka możliwych „Uchybień i Zagrożeń"

I. Uchybienia i zagrożenia nieświadome wewnętrzne i zewnętrzne

Do uchybień i zagrożeń nieświadomych wewnętrznych i zewnętrznych należą działania pracowników podmiotu lub osób nie będących pracownikami podmiotu, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności. W szczególności są to działania takie jak:

- niewłaściwe zabezpieczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe,

- niewłaściwe zabezpieczenie sprzętu komputerowego,

- dopuszczenie do przetwarzania danych przez osoby nieposiadające upoważnienia,

- pomyłki informatyków, ASI,

- kradzież danych,

- kradzież sprzętu informatycznego,

- działanie wirusów i innego szkodliwego oprogramowania oraz inne działania, wskutek których dojdzie do utraty danych osobowych lub uszkodzenia nośników danych.

II. Uchybienia i zagrożenia umyślne wewnętrzne i zewnętrzne

Do uchybień i zagrożeń umyślnych wewnętrznych i zewnętrznych należą celowe działania pracowników podmiotu, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności. W szczególności są to działania takie jak:

- celowe zniszczenie danych osobowych lub nośników danych,

- kradzież danych osobowych,

- dopuszczenie do przetwarzania danych przez osoby nieposiadające upoważnienia,

- kradzież danych,

- kradzież sprzętu informatycznego,

- działanie wirusów i innego szkodliwego oprogramowania oraz inne działania, wskutek których dojdzie do utraty danych osobowych lub uszkodzenia nośników danych.

III. Uchybienia i zagrożenia losowe

Do uchybień i zagrożeń losowych należą sytuacje losowe, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności. W szczególności są to sytuacje takie jak:

- klęski żywiołowe,

- przerwy w zasilaniu,

- awarie serwera,

- pożar,

- zalanie wodą.

3. Procedura postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych.

Każdy pracownik podmiotu posiadający upoważnienie do przetwarzania danych osobowych, w przypadku stwierdzenia uchybienia lub zagrożenia ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji lub Administratora Danych.

Administrator Bezpieczeństwa Informacji w przypadku stwierdzenia uchybienia ma obowiązek:

1. odnotować każde uchybienie w „Dzienniku Uchybień i Zagrożeń"

2. sporządzić „Protokół Uchybienia"

3. wprowadzić procedury uniemożliwiające ponowne powstanie uchybienia

Administrator Bezpieczeństwa Informacji w przypadku stwierdzenia zagrożenia ma obowiązek:

1. zabezpieczyć dowody, powiadomić policję (w przypadku włamania)

2. zabezpieczyć dane osobowe oraz nośniki danych

3. odnotować każde zagrożenie w „Dzienniku Uchybień i Zagrożeń"

4. sporządzić „Protokół Zagrożenia"

5. wprowadzić procedury uniemożliwiające ponowne powstanie zagrożenia

6. powiadomić o zaistniałej sytuacji Administratora Danych

7. podjąć próbę przywrócenia stanu sprzed zaistnienia zagrożenia w porozumieniu z ASI

8. ADO wyciąga konsekwencje dyscyplinarne wobec osób odpowiedzialnych za zagrożenie

4. Rejestr Uchybień i Zagrożeń oraz szczegółowa instrukcja postępowania dla osób posiadających upoważnienie do przetwarzania danych osobowych w podmiocie

Kod uchybienia lub zagrożenia	Uchybienia i zagrożenia nie świadome wewnętrzne i zewnętrzne	Postępowanie w przypadku uchybienia lub zagrożenia
1	Pomieszczenie w którym przechowywane są dane osobowe pozostaje bez nadzoru.	Należy zabezpieczyć dane osobowe oraz powiadomić ABI. ABI sporządza protokół uchybienia.
2	Komputer nie jest zabezpieczony hasłem.	Należy zabezpieczyć dane osobowe oraz powiadomić ABI. ABI sporządza protokół uchybienia.
3	Dostęp do danych osobowych mają osoby nie posiadające upoważnienia.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić ABI. ABI sporządza protokół uchybienia.
4	Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym.	Należy powiadomić ABI, który przy pomocy ASI powinien sprawdzić system uwierzytelnienia oraz sprawdzić czy nie doszło do kradzieży lub zniszczenia danych. ABI sporządza protokół uchybienia.
5	Próba kradzieży danych osobowych poprzez zewnętrzny nośnik danych.	Należy nie dopuścić do kradzieży danych i powiadomić ABI. ABI powinien zabezpieczyć nośnik danych i powiadomić ADO. ABI sporządza protokół zagrożenia.
6	Próba kradzieży danych osobowych w firmie papierowej.	Należy nie dopuścić do kradzieży danych i powiadomić ABI. ABI powinien zabezpieczyć dane i powiadomić ADO.ABI sporządza protokół zagrożenia.
7	Nieuprawniony dostęp do danych osobowych w formie papierowej.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić ABI. ABI sporządza protokół uchybienia.
8	Dane osobowe przechowywane są w nie zabezpieczonym pomieszczeniu.	Należy powiadomić ABI. ABI powinien zabezpieczyć pomieszczenie. ABI sporządza protokół uchybienia.
9	Próba włamania do pomieszczenia/budynku.	Należy zabezpieczyć dowody i powiadomić ABI. ABI sprawdza stan uszkodzeń, zabezpiecza dowody i wzywa policję. ABI sporządza protokół uchybienia.
10	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania.	Należy zrobić audyt systemów zabezpieczeń a w szczególności systemów antywirusowych, firewall. ABI powinni ocenić, czy nie doszło do utraty danych osobowych i w zależności od tego sporządzić protokół uchybienia lub zagrożenia.
11	Brak aktywnego oprogramowania antywirusowego.	Należy powiadomić ABI. ABI powinien zaktualizować lub nabyć oprogramowanie antywirusowe. ABI sporządza

		protokół uchybienia.
12	Zniszczenie lub modyfikacja danych osobowych w formie papierowej.	Należy zabezpieczyć dowody i powiadomić ABI. ABI sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia ADO. ABI sporządza protokół zagrożenia.
13	Zniszczenie lub modyfikacja danych osobowych w systemie informatycznym.	Należy zabezpieczyć dowody i powiadomić ABI. ABI sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia ADO. ABI sporządza protokół zagrożenia.
14	Uszkodzenie komputerów, nośników danych.	Należy powiadomić ABI. ABI powinien ocenić w wyniku czego doszło do zniszczenia i przywrócić dane z kopii zapasowej. ABI powiadamia ADO i sporządza protokół zagrożenia.
15	Próba nieuprawnionej interwencji przy sprzęcie komputerowym.	Należy uniemożliwić dostęp osób do sprzętu komputerowego oraz powiadomić ABI. ABI sporządza protokół uchybienia.
16	Zdarzenia losowe.	Należy oszacować powstałe straty i sporządzić protokół zagrożenia lub uchybienia.

Załącznik nr 1

do Procedury Alarmowej

„Dziennik Uchybień i Zagrożeń"

Kod	Data i godzina zdarzenia	Rodzaj zdarzenia *(uchybienie/ zagrożenie)*	Opis zdarzenia	Skutki zdarzenia	Działania naprawcze	Podpis ABI

Nazwa i adres podmiotu

Miejscowość i data

.....

.....

Załącznik nr 2

do Procedury Alarmowej

„Protokół Zagrożenia"

Data i godzina wystąpienia zagrożenia

.....

Kod zagrożenia

.....

Opis zagrożenia

.....

.....

Przyczyny powstania zagrożenia

.....

.....

Zaistniałe skutki zagrożenia

.....

.....

.

Podjęte działania naprawczo-zapobiegawcze

.....

.....

Administrator Bezpieczeństwa Informacji

Administrator Danych Osobowych

.....

.....

Nazwa i adres podmiotu

Miejscowość i data

.....

.....

Załącznik nr 3

do Procedury Alarmowej

„Protokół Uchybienia"

Data i godzina wystąpienia uchybienia.....

Kod uchybienia

.....

Opis uchybienia

.....
.....
.....
.....
.....

Przyczyny powstania uchybienia

.....
.....
.....
.....
.....

Zaistniałe skutki uchybienia

.....
.....
.....
.....
.....

Podjęte działania naprawczo-zapobiegawcze

.....
.....
.....
.....
.....

Administrator Bezpieczeństwa Informacji

.....

Administrator Danych Osobowych

.....

Załącznik nr 4

do Procedury Alarmowej

Sprawozdanie roczne stanu systemu ochrony danych osobowych

W celu pełnej kontroli oraz zapobieganiu możliwym zagrożeniom związanych z ochroną danych osobowych na podstawie art. 36.1 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych Administrator Danych wdraża dokument o nazwie "Sprawozdanie roczne stanu systemu ochrony danych osobowych"

1. Sprawozdanie roczne stanu systemu ochrony danych osobowych przeprowadzać się będzie od 2015r. raz w roku. Osoba odpowiedzialna za przygotowanie sprawozdania jest ABI. Sprawozdanie roczne przygotowuje się na podstawie dokumentu „Raport roczny", który stanowi załącznik nr 1.
2. Po przeprowadzeniu analizy stanu ochrony danych osobowych w porozumieniu z ASI ABI uzupełnia raport roczny i zwołuje zebranie w którym uczestniczą: ADO, ABI, ASI, ..., przedstawiciel księgowości (główny księgowy).
3. Podczas zebrania ASI przedstawia uczestnikom stan infrastruktury informatycznej a ABI przedstawia dziennik uchybień i zagrożeń. Na spotkaniu omawiane są procedury zabezpieczające podmiot przed sytuacjami, w których może dojść do zniszczenia danych, wycieku danych lub naruszenia ich poufności.

Załącznik nr 1

do „Sprawozdania rocznego stanu
systemu ochrony danych osobowych"

„Raport roczny"

Nazwa i adres podmiotu	Miejscowość i data .....

Zagadnienia omawiane na zebraniu	**Uwagi/wnioski**
Podsumowanie realizacji wytycznych z poprzedniego „Sprawozdania rocznego stanu systemu ochrony danych osobowych"	
Omówienie zmian procedur w systemie oraz zmian w systemie informatycznym	
Omówienie Dziennika Uchybień i Zagrożeń	
Wnioski oraz zadania do realizacji	

Uczestnicy zebrania	Podpis uczestnika

Podpis ABI	Podpis ADO

Załącznik Nr 2 do Zarządzenia Nr 39/2016
Wójta Gminy Klukowo
z dnia 6 grudnia 2016 r.

Procedura

„Postępowanie w przypadku wystąpienia awarii systemu informatycznego oraz zasady zgłaszania zdarzeń, incydentów i nieprawidłowej pracy sprzętu"

1. Cel

Procedura postępowania w przypadku wystąpienia awarii systemu informatycznego ma na celu zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem danych oraz ochroną krytycznych procesów przed rozległymi awariami lub katastrofami.

2. Awarie systemu informatycznego

Awaria systemu informatycznego - nieprawidłowe działanie systemu informatycznego dotyczące wystąpienia zagrożenia:

1. dostępność danych – brak dostępu do danych dla wszystkich/grupy osób uprawnionych,
2. integralności danych – nieprawidłowe działanie systemu informatycznego skutkujące niezamierzoną utratą lub modyfikacją zgromadzonych danych,
3. poufności danych – nieprawidłowe działanie systemu informatycznego skutkujące ujawnieniem zgromadzonych danych osobom nieuprawnionym.

3. Reagowanie na awarie

3.1. Warunki ogólne

1. Reakcja na awarie musi minimalizować straty, na jakie narażony jest Urząd w wyniku danego zdarzenia.
2. Jeżeli charakter awarii pozwala podejrzewać, że może być naruszona poufność danych, należy podjąć działania mające na celu odcięcie źródła danych od drogi komunikacji, przez którą poufność może być naruszona.

3.2. Czynności do wykonania

1. Użytkownicy systemu informatycznego zobowiązani są do zgłaszania nietypowych zdarzeń, incydentów oraz nieprawidłowej pracy sprzętu bezpośrednio do osoby pełniącej funkcję Administratora Bezpieczeństwa Informacji urzędu.
2. ABI dokonuje analizy i klasyfikacji awarii według następujących kryteriów:
    a. jakich elementów systemu dotyczy awaria bezpośrednio, a jakich pośrednio,
    b. czy awaria jest zagrożeniem dla poufności czy integralności danych,
    c. jakie dane mogą być zagrożone awarią,
    d. czy awaria będzie rozwiązana przez naprawę uszkodzonego elementu, jego wymianę na inny czy przez stworzenie tymczasowych mechanizmów awaryjnych,
    e. jak poważne będą skutki awarii (szczególnie naruszenie dostępności, integralności i poufności informacji).
3. W zależności od charakteru awarii, należy wykonać określone działania opisane w rozdziale **4** niniejszego załącznika.
4. Jeżeli podjęta została decyzja o czasowym wyłączeniu części usług systemu, należy poinformować użytkowników tych usług.
5. Jeżeli awaria jest powiązana z celowymi działaniami mającymi na celu zaatakowanie Urzędu, należy rozważyć poinformowanie Policji.
6. Obsługę sytuacji awaryjnej związanej z poufnością i/lub integralnością informacji należy zakończyć opisaniem jej w notatce służbowej. Notatkę służbową sporządza Administratora Bezpieczeństwa Informacji.
7. Jeżeli system lub dokumentacja (w szczególności Polityka Zarządzania Bezpieczeństwem Informacji) wymaga wprowadzenia modyfikacji, należy podjąć działania mające na celu ich przeprowadzenie.

4. Rodzaje awarii

4.1. Awarie oprogramowania

Jeżeli analiza wykaże, że awaria spowodowana jest przez wadliwie działające oprogramowanie, należy podjąć następujące działania:

1. Określić, czy awaria uniemożliwia dalsze korzystanie z oprogramowania i danych.
    a. Jeżeli dalsza praca jest możliwa i nie zagraża kolejnymi awariami – pracownicy powinni powrócić do normalnej pracy.
    b. Jeżeli dalsza praca jest niemożliwa, należy określić czy tworzenie rozwiązania awaryjnego jest uzasadnione i w razie potrzeby – stworzyć je.
2. Określić, czy znane są okoliczności wystąpienia awarii a także (w miarę możliwości) czy są one powtarzalne.
3. Jeżeli okoliczności są powtarzalne i błędu nie można doraźnie wyeliminować, należy poinformować użytkowników aplikacji, że nie powinni wykonywać określonych operacji.
4. Określić czy istnieją poprawki/nowsze wersje oprogramowania eliminujące zaobserwowaną awarię.
5. Jeżeli poprawki są dostępne, można wdrożyć je, w drodze wyjątku nie poprzedzając wszystkimi działaniami (testami) związanymi z zarządzaniem zmianami. W trakcie aplikowania poprawek, należy zadbać o możliwość przywrócenia pierwotnego stanu, a po przywróceniu sprawności systemu niezwłocznie wykonać wszystkie czynności, których wymaga zarządzanie zmianami.
6. Jeżeli oprogramowanie jest tworzone na zamówienie, należy zgłosić producentowi konieczność stworzenia poprawek, udostępniając potrzebne dane o awarii w sposób minimalizujący ryzyko ujawnienia informacji poufnych.
7. Jeżeli awaria lub proces jej usuwania naruszył integralność danych, należy przywrócić ich poprawny stan.

4.2. Awarie sprzętu

W przypadku, kiedy analiza przyczyn awarii wskaże, że awaria została spowodowana przez sprzęt, należy wykonać następujące działania:

1. Jeżeli uszkodzony sprzęt ma zapewnione mechanizmy redundancji, procesy naprawcze powinny być przeprowadzone jak najszybciej, w sposób najmniej zaburzający pracę Urzędu.
2. Jeżeli szybka wymiana uszkodzonego elementu nie jest możliwa – należy rozważyć przeniesienie funkcji uszkodzonego elementu w inne miejsce. Jeżeli przeniesienie funkcji jest możliwe, rozwiązanie takie należy na bieżąco dokumentować. Ponadto, określić należy, na jaki czas planowane jest użycie rozwiązania zastępczego.
3. Jeżeli awaria lub proces jej usuwania naruszył integralność danych, należy przywrócić ich poprawny stan.
4. Jeżeli uszkodzony sprzęt to nośnik danych, to należy go fizycznie zniszczyć w obecności Administratora Bezpieczeństwa Informacji lub osoby przez niego upoważnionej. W szczególnych przypadkach, jeśli istnieje konieczność odzyskania danych z uszkodzonego nośnika, możliwe jest przekazanie nośnika do naprawy firmie posiadającej stosowne poświadczenie bezpieczeństwa, po podpisaniu z nią umowy na przekazanie przetwarzania danych znajdujących się na nośniku.

Załącznik Nr 3 do Zarządzenia Nr 39/2016
Wójta Gminy Kłukowo
z dnia 6 grudnia 2016 r.

Procedura

„Przeglądy i konserwacje systemów"

1. Cel

Przeprowadzanie przeglądów i konserwacji ma na celu wczesne wykrycie i usunięcie nieprawidłowości, zanim doprowadzą one do poważniejszych w skutkach awarii czy ujawnienia danych chronionych.

2. Przeglądy i konserwacje systemów

2.1. Warunki ogólne

1. Przeglądy systemów przeprowadza administrator , za wyjątkiem przeglądu głównych usług autoryzacyjnych oraz systemu ochrony styku z siecią publiczną, których przeglądy należy przeprowadzać co najmniej raz w roku.
2. Przeglądom podlegają następujące elementy:
    a. Usługi autoryzacyjne systemów.
    b. Systemy ochrony na styku z siecią publiczną.
    c. Serwery.
    d. Infrastruktura sieciowa.
    e. Systemy zasilania.
    f. Konfiguracja stacji roboczych.
3. Przegląd systemu może być dokonany poprzez analizę danych pozyskanych przez systemy monitorowania zasobów.
4. Konserwacja wskazana jest tam, gdzie przeglądy wykażą taką konieczność, oraz tam, gdzie jest zalecana przez producentów rozwiązania. Działania konserwacyjne nie mogą przebiegać w sposób sprzeczny z wymogami Polityki Bezpieczeństwem Informacji (PBI) o ile nie ma to ważnego, udokumentowanego uzasadnienia.

2.2. Czynności do wykonania

Przegląd działania istotnych elementów systemu powinien przebiegać według podobnego schematu, tj.:

1. Tam, gdzie jest to możliwe, pozyskać systemowe dzienniki zdarzeń generowanych przez badany element w okresie od ostatniego przeglądu.
2. Dokonać analizy pozyskanych dzienników w zakresie wystąpienia zdarzeń zdefiniowanych przez producenta rozwiązania jako błędy lub ostrzeżenia, ze szczególnym uwzględnieniem możliwości spowodowania sytuacji zagrażających bezpieczeństwu.
3. Przejrzeć zgłoszenia serwisowe, które zostały ocenione jako powiązane z badanym elementem systemu.
4. Pozyskać od producentów rozwiązania, dla wszystkich zaobserwowanych nieprawidłowości, informacje dotyczące przyczyn i skutków tych sytuacji oraz sugerowanych działań naprawczych.
5. Porównać wynik przeglądu i zapisu w dzienniku przeglądów z poprzednim wynikiem dla tego samego elementu.
6. Przeprowadzić analizę skutków wdrożenia wszystkich działań naprawczych w odniesieniu do innych systemów.
7. Przedstawić Sekretarzowi Urzędu raport z przeglądu z propozycją działań naprawczych, ich skutkami i kosztami.
8. Wdrożyć działania naprawcze.
9. Wszystkie działania powinny być zgodne z PBI.

10. W przypadku braku działań naprawczych raportu nie sporządza się, fakt przeprowadzenia raportu odnotowuje się w dzienniku przeglądów.

3. Usługi autoryzacyjne

Należy pamiętać, że usługi autoryzacyjne świadczone są zarówno przez Windows Active Directory (główne usługi autoryzacyjne), jak i przez inne systemy i aplikacje, w zakresie dostępu do nich.

4. Przegląd systemów ochrony na styku z siecią publiczną

Poza pobraniem i analizą dzienników zdarzeń z tych systemów, należy:

1. Sprawdzić reguły ustawione na systemach firewall i Proxy porównując je z założeniami PBI oraz wymogami działania Urzędu.
2. Sprawdzić z sieci publicznej usługi i porty udostępniane przez sieć Urzędu.

5. Przegląd serwerów

Poza pobraniem i analizą dzienników zdarzeń, działanie serwerów powinno być sprawdzone pod kątem:

1. Aktualności poprawek systemowych.
2. Poprawności konfiguracji serwerów baz .
3. Poprawności działania podzespołów takich jak pamięci, dyski, karty sieciowe, wentylatory. Do kontroli takiej może być użyte oprogramowanie diagnostyczne np. dostarczane z serwerem.
4. Stopnia zajętości dysków.
5. Średniego obciążenia procesora.

6. Przegląd infrastruktury sieciowej

W przypadku infrastruktury sieciowej, pobranie dzienników zdarzeń może być niemożliwe. Tym większy nacisk należy położyć na dodatkowe źródła informacji o kondycji systemu. W szczególności, podczas przeglądu należy:

1. Narysować faktyczny sposób połączeń i przeanalizować pod kątem nieprawidłowości.
2. Sprawdzić stopień wykorzystania przepustowości kluczowych połączeń.
3. Tam, gdzie to możliwe, zbadać obciążenie (stopień wykorzystania) urządzeń.
4. Sprawdzić częstotliwość wystąpień błędów transmisji w dostępnych źródłach.
5. Przeprowadzić skanowanie sieci w celu wykrycia wszystkich urządzeń i sprawdzenia prawidłowości adresacji.

7. Przegląd systemów zasilania

W przypadku urządzeń zasilających, pobranie dzienników zdarzeń może być niemożliwe. Tym większy nacisk należy położyć na dodatkowe źródła informacji o kondycji systemu. W szczególności, podczas przeglądu należy:

1. Sprawdzić obciążenie zasilaczy awaryjnych.
2. Sprawdzić wiek lub raportowaną przez urządzenie kondycję akumulatorów.
3. Dla wybranych urządzeń przeliczyć, czy czas gwarantowanego podtrzymania zasilania jest wystarczający do zapewnienia bezpiecznego wyłączenia chronionych urządzeń.
4. Wyrywkowo sprawdzić parametry zasilania tam, gdzie zapewniane jest ono przez urządzenia typu on-line.

5. Wyrywkowo sprawdzić czy do chronionej sieci zasilającej nie są wpięte niepożądane urządzenia.
6. Sprawdzić ochronę przed nieautoryzowanym dostępem zarówno do centralnego UPS-a jak i do tablic rozdzielczych kluczowych elementów systemu informatycznego.
7. Uwaga! Testy systemów zasilania powinny być przeprowadzane po godzinach pracy Urzędu.
8. Uwaga! Nie należy przeprowadzać testów wyłączników różnicowoprądowych, do których podłączone są działające elementy systemu Urzędu.

8. Przegląd konfiguracji stacji roboczych

Stacje robocze pracowników stanowią istotny element infrastruktury teleinformatycznej Urzędu, a ze względu na potencjalnie dużą dostępność dla nieupoważnionych osób oraz z powodu różnorodnej działalności użytkowników często ich konfiguracja odbiega od wymaganej. Szczególną uwagę należy zwrócić na stacje użytkowane przez osoby o dużych uprawnieniach (pracownicy Wydziału Informatyki, kierownicy wszystkich szczebli). Ze względu na dużą liczbę stacji do podstawowego przeglądu konieczne jest użycie oprogramowania narzędziowego. Należy skontrolować:

1. Zainstalowane systemowe pakiety poprawek (service pack).
2. Oprogramowanie zainstalowane i uruchamiane.
3. Zgodność nazewnictwa stacji z przyjętymi regułami.
4. Stopień zajętości dysków.

Wzór: Dziennik przeglądów i konserwacji systemów

Lp.	Data przeglądu	Nazwa systemu	Nazwisko i imię osoby przeprowadzającej przegląd	Uwagi

Str. .....

Załącznik Nr 4 do Zarządzenia Nr 39/2016
Wójta Gminy Klukowo
z dnia 6 grudnia 2016 r.

Procedura

„Postępowanie w zakresie wykonywania i obsługi kopii zapasowych oraz okresowego badania nośników służących do przechowywania informacji"

1. Cel

Celem procedury wykonywania i obsługi kopii zapasowych jest zapewnienie bezpieczeństwa przetwarzanych informacji, tj. zapewnia możliwość powrotu do stanu sprzed awarii lub innego zdarzenia związanego z naruszeniem danych. W celu zapewnienia bezpieczeństwa przetwarzania informacji wykonuje się kopie zapasowe i archiwalne. Archiwizacja jest procesem zbliżonym do wykonywania kopii zapasowych (backupu). Najistotniejsza różnica polega na przeznaczeniu skopiowanej informacji. Kopie zapasowe mają za zadanie umożliwić doraźne odtworzenie danych po awarii, niepożądanej zmianie lub skasowaniu, podczas gdy rolą kopii archiwalnych jest z jednej strony umożliwienie wglądu w dane historyczne, z drugiej – zapewnienie możliwości odzyskania danych w sytuacji, gdy dane z backupu zawiodą.

2. Wykonywanie kopii zapasowych (backup) i archiwizacja

2.1. Warunki ogólne

1. Harmonogram wykonywania kopii:
   a. zapasowych - co najmniej raz na tydzień,
   b. archiwalnych - nie rzadziej niż raz w miesiącu.
2. Termin przechowywania kopii:
   a. zapasowych – 2 tygodnie,
   b. archiwalnych - co najmniej tak długo, aby możliwe było odtworzenie z nich danych, do przechowywania których Urząd jest zobowiązany. Jeżeli kilka kopii archiwalnych zawiera te same wymagane dane lub, jeżeli dane z jednej kopii są podzbiorem drugiej – przechowywanie nadmiarowej kopii archiwalnej nie jest konieczne.
3. Kopie zapasowe zawierają wszystkie pliki i programy z wyjątkiem:
   a. danych o charakterze tymczasowym, które nie są niezbędne do odtworzenia stanu systemu,
   b. danych o dużej objętości i pomijalnym znaczeniu dla systemu informatycznego Urzędu.
   c. danych przechowywanych na dyskach lokalnych stacji roboczych.
4. Archiwizacji podlegają wszystkie pliki i programy z wyjątkiem:
   a. danych dla których nie wykonuje się kopii zapasowych opisanych w punkcie 3,
   b. danych, które można łatwo pozyskać z innych (zaufanych i zewnętrznych) źródeł, a których objętość mogłaby być uciążliwa w procesie archiwizacji
   c. danych o pomijalnym znaczeniu dla systemu informatycznego Urzędu,
   d. danych z systemów będących w eksploatacji, których archiwizacja nie jest wymagana żadnymi przepisami prawa.
5. W trakcie wykonywania kopii zapasowych i archiwalnych należy weryfikować nośniki, poprzez włączenie w wykorzystywanym oprogramowaniu opcji „weryfikacji" kopii.
6. Pracownicy korzystający z poszczególnych aplikacji zobowiązani są do zgłoszenia pracownikowi wykonującemu kopie konieczności aktualizacji listy danych podlegających backupowi i archiwizacji.
7. Proces archiwizacji prowadzony jest w sposób zapewniający maksymalną ochronę przed uszkodzeniem danych przez czynniki zewnętrzne takie jak zalanie, pożar czy kradzież.
8. Jeżeli kopia zapasowa spełnia wszystkie wymagania stawiane kopii archiwalnej dopuszczalne jest przeniesienie nośnika z kopią zapasową do archiwum i uznanie go za kopię archiwalną. Przeniesienie takie wymaga odnotowania w wykazie nośników archiwalnych i oznaczenia nośnika w sposób przyjęty dla nośników archiwalnych.

9. Kopie archiwalne przechowuje się w lokalizacji innej niż lokalizacja w jakiej znajdują się dane oryginalne.
10. Kopie zapasowe i archiwalne wykonuje się na przenośnych nośnikach wysokiej trwałości lub na urządzeniach zapewniających odpowiednią trwałość i bezpieczeństwo zapisu.
11. Nośniki zawierające kopie zapasowe i archiwalne muszą być chronione przed dostępem osób nieuprawnionych.
12. Nośniki przechowywane w sposób niezgodny z zaleceniami producenta muszą być wyłączone z użycia.
13. Zarówno nośniki jak i sprzęt nie mogą być użytkowane dłużej i do większej ilości kopii niż jest to określone przez producenta.
14. Jakiekolwiek podejrzenia co do jakości i trwałości nośnika wykluczają jego użycie do czasu dokładnego zweryfikowania podejrzeń.
15. Należy dążyć do eliminacji pojedynczego punktu awarii w zakresie sprzętu wykorzystywanego do wykonywania kopii zapasowych i archiwalnych.

2.2. Czynności do wykonania – kopie zapasowe

Pracownik odpowiedzialny za wykonanie kopii zapasowych ma obowiązek realizować następujące czynności:

1. Zaktualizować listy danych podlegających backupowi, jeżeli zgłoszono mu nowe dane do zabezpieczenia. Listy przechowywane są w oprogramowaniu do wykonania kopii zapasowej.
2. Wybrać nośnik i typ backupu odpowiedni do szczegółowego harmonogramu. Szczegółowy harmonogram zapisany jest w oprogramowaniu wykorzystywanym do wykonania kopii zapasowych.
3. Zapisać w dzienniku kopii identyfikator nośnika, zakres, z czasem wykonania i wersją oprogramowania stosowanego do backupu. Dane te mogą być automatycznie zapisywane w wykorzystywanym oprogramowaniu. Okres przechowywania wpisów w dzienniku wynosi 30 dni od daty wykonania kopii zapasowej.
4. Wykonać kopię zapasową zgodnie z dokumentacją producenta oprogramowania oraz producenta sprzętu wykorzystywanego do wykonania kopii zapasowej.
5. Zweryfikować i zanotować w dzienniku status backupu zgłaszany przez oprogramowanie. Czynność ta może zostać wykonana automatycznie przez wykorzystywane oprogramowanie. Okres przechowywania wpisów w dzienniku wynosi 30 dni od daty wykonania kopii zapasowej.

2.3. Czynności do wykonania – kopie archiwalne

Pracownik odpowiedzialny za wykonanie kopii archiwalnych ma obowiązek realizować następujące czynności:

1. Zaktualizować listy danych podlegających archiwizacji, jeżeli zgłoszono mu nowe dane do zabezpieczenia. Listy przechowywane są w oprogramowaniu do wykonania kopii archiwalnej.
2. Wybrać nośnik służący do zapisu kopii archiwalnej.
3. Zapisać w dzienniku kopii archiwalnych identyfikator nośnika, zakres wraz z czasem wykonania, wersją oprogramowania stosowanego do wykonania kopii. Dane te mogą być automatycznie zapisywane w wykorzystywanym oprogramowaniu. Okres przechowywania wpisów w dzienniku wynosi 30 dni od daty wykonania kopii archiwalnej.
4. Wykonać kopię zgodnie z dokumentacją producenta oprogramowania oraz producenta sprzętu wykorzystywanego do wykonania kopii archiwalnej.

5. Zweryfikować i zanotować w dzienniku status operacji zgłaszany przez oprogramowanie. Czynność ta może zostać wykonana automatycznie przez wykorzystywane oprogramowanie. Okres przechowywania wpisów w dzienniku wynosi 30 dni od daty wykonania kopii archiwalnej.
6. Uzupełnić wykaz nośników archiwalnych o nowy nośnik. Wykaz jest prowadzony w formie elektronicznej, plik z wykazem przechowywany jest w systemie obiegu dokumentów.
7. Jeśli to możliwe, zabezpieczyć nośnik przed przypadkowym wykasowaniem informacji.
8. Opisać nośnik w sposób gwarantujący trwałe związanie opisu z nośnikiem. Opis zawierać musi te same dane, które zawiera wpis w wykazie nośników archiwalnych.
9. Przenieść użyte nośniki w miejsce ich przechowywania.

3. Odtwarzanie

3.1. Warunki ogólne

1. Odtworzenie danych może dotyczyć ich dowolnego zakresu.
2. Podczas odtwarzania należy zachować szczególną ostrożność, aby w sposób niezamierzony nie zniszczyć (nadpisać) innych danych przechowywanych na serwerze.
3. Do odtwarzania powinny być użyte nośniki z puli kopii zapasowych. Jeżeli ich zastosowanie nie pozwala osiągnąć zamierzonego celu – użyć można kopii archiwalnych.
4. Jeżeli dane produkcyjne zostały od czasu stworzenia kopii zmodyfikowane, po odtworzeniu kopii zapasowej należy uzupełnić dane odtworzone stosownie do możliwości technicznych i faktycznych potrzeb.

3.2. Czynności do wykonania

Pracownik odpowiedzialny za wykonanie kopii zapasowych w trakcie odtwarzania realizuje następujące czynności:

1. Sprawdzić w dzienniku kopii zapasowych i ewentualnie w dzienniku kopii archiwalnych na którym nośniku znajdują się dane mające zostać odtworzone.
2. Pobrać nośniki z lokalizacji, w której są przechowywane.
3. Wykonać odtworzenie zgodnie z procedurami producenta sprzętu i oprogramowania.
4. Sprawdzić w dzienniku oprogramowania czy odtworzenie danych przebiegło bez błędów. Jeśli wystąpiły błędy należy sprawdzić przyczyny błędu i je usunąć. W razie uszkodzenia nośnika kopii należy odtworzyć dane z innej kopii. Uszkodzony nośnik należy usunąć zgodnie z procedurą.
5. Przenieść odtworzone dane na system produkcyjny.

4. Okresowe badanie nośników służących do przechowywania informacji (kopii archiwalnych / nośników archiwalnych)

4.1. Warunki ogólne

1. Weryfikacja kopii archiwalnych może odbywać się poza środowiskiem produkcyjnym.
2. Weryfikacji podlegają wyrywkowo wybrane nośniki, należy jednak zwrócić uwagę, aby badaniu podlegały kopie archiwalne zapisane na wszystkich rodzajach nośników oraz we wszystkich okresach.
3. Tam, gdzie producent to zaleca, należy wykonać przewinięcie (retencję) taśm i inne prace konserwacyjne w sposób i z częstotliwością określoną przez producenta.

4. O ile to możliwe, kopie niepełnowartościowe powinny być zastępowane identycznymi funkcjonalnie kopiami o jakości nie budzącej zastrzeżeń.
5. Okresowo raz w roku należy przeprowadzić analizę:
   a. dostępności danych zgromadzonych na nośnikach oraz analizę używanych rozwiązań archiwizacyjnych. W uzasadnionych przypadkach należy zaopatrzyć archiwum w odpowiednie produkty umożliwiające dostęp do danych archiwalnych.
   b. aktualności kopii archiwalnych, kopie po dacie ważności należy przeznaczyć do likwidacji.

4.2. Czynności do wykonania

Pracownik Wydziału Informatyki odpowiedzialny za wykonanie kopii archiwalnych ma obowiązek realizować następujące czynności:

1. Przejrzeć archiwum pod kątem jego stanu zewnętrznego i braków nośników.
2. Wyznaczyć nośniki do weryfikacji bazując między innymi na ich znaczeniu, czasie powstania i czasie ostatniej weryfikacji.
3. Wykonać wyrywkowe próbne odtworzenie, połączone w miarę możliwości ze sprawdzeniem sum kontrolnych.
4. Zanotować wynik weryfikacji, datę, identyfikator nośnika oraz dane wykonującego w dzienniku weryfikacji.
5. O ile zostały pobrane z archiwum – zwrócić nośniki i dziennik weryfikacji.
6. W sytuacji, w której weryfikacja danych archiwalnych wykazuje, że ich odzyskanie jest niemożliwe, a istnieje inne, równoważne źródło tych danych – archiwum należy uzupełnić korzystając ze źródła równoważnego.

5. Przechowywanie

5.1. Warunki ogólne

1. Kopie przechowywane są w sposób zapewniający maksymalną ochronę przed utratą danych przez czynniki zewnętrzne takie jak zalanie, pożar czy kradzież.
2. Kopie archiwalne powinny być przechowywane w innej lokalizacji niż miejsce przetwarzania danych.
3. Kopie archiwalne muszą być przechowywane co najmniej tak długo, aby możliwe było odtworzenie z nich danych, do przechowywania których Urząd jest zobowiązany. Jeżeli kilka kopii archiwalnych zawiera te same wymagane dane lub, jeżeli dane z jednej kopii są podzbiorem drugiej – przechowywanie nadmiarowej kopii archiwalnej nie jest wymagane.
4. Okres przechowywania dla kopii archiwalnych danych i systemów będących nadal w użyciu:
   a. kopie miesięczne – 3 lata
   b. kopie roczne – 5 lat.
5. Nie należy przechowywać zbędnych kopii danych. Większa liczba kopii zwykle przekłada się na większe trudności z zapanowaniem nad ich stanem, liczbą i lokalizacją, co może prowadzić do ich gorszego zabezpieczenia i narazić na nieuprawniony dostęp.
6. Kopie archiwalne powinny, o ile to możliwe, gwarantować że zapisane na nich dane nie zostaną w sposób niezauważalny zmodyfikowane.
7. Nośniki z kopiami archiwalnymi powinny być w sposób jednoznaczny oznaczane identyfikatorem. Należy prowadzić wykaz nośników archiwalnych zawierający identyfikatory nośników, datę wykonania kopii oraz opis zawartości.

5.2. Czynności do wykonania

Pracownik odpowiedzialny za wykonanie kopii zapasowych i archiwalnych ma obowiązek realizować następujące czynności:

1. Niezwłocznie po wykonaniu kopii zweryfikować jej poprawność. Weryfikacja poprawności może zostać przeprowadzona automatycznie przez oprogramowanie – wynik weryfikacji jest zapisywany w dzienniku aplikacji.
2. Dla kopii archiwalnych zabezpieczyć nośnik przed modyfikacją. Następnie nadać identyfikator, w wykazie nośników archiwalnych odnotować datę wykonania i zawartość.
3. Przenieść nośnik do lokalizacji przewidzianej do przechowywania kopii.
4. Raz w roku sprawdzić dla których kopii upłynął już termin przechowywania i po zweryfikowaniu, że dana kopia nie jest już potrzebna, przeprowadzić jej likwidację.

6. Likwidacja kopii

Wszelkie zbędne kopie oraz uszkodzone nośniki kopii należy likwidować w sposób uniemożliwiający odzyskanie i odczyt z nich danych. Likwidacja może polegać na zamazaniu danych poprzez zapis innych danych na tym samym nośniku, lub na fizycznym zniszczeniu nośnika.

Likwidacja nośnika archiwalnego powinna zostać zatwierdzona przez Administratora Bezpieczeństwa Informacji.