III Rozdział

Wzory dokumentów

III.1 Wzór raportu z naruszenia zasad bezpieczeństwa systemu informatycznego w Urzędzie Gminy

Wzór

RAPORT
z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie Gminy Wilkowice

1. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje))

2. Lokalizacja zdarzenia:

.....
(np. nr pokoju, nazwa pomieszczenia)

3. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....
.....

4. Podjęte działania:

.....
.....

5. Przyczyny wystąpienia zdarzenia:

.....
.....

6. Postępowanie wyjaśniające:

.....
.....

.....
data, podpis Administratora Bezpieczeństwa Informacji

III.2 Wzór wykazu osób, które zapoznały się z „Polityką bezpieczeństwa systemów informatycznych" służących do przetwarzania danych osobowych w Urzędzie Gminy

Wzór

....., dnia .....200..r.

Lp	Imię	Nazwisko	Stanowisko	Podpis

III.3 Rejestr osób upoważnionych do przetwarzania danych osobowych

W z ó r

N.Znak: ....., dnia .....200..r.

Upoważnienie imienne uprawniające

do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz Polityki Bezpieczeństwa Systemów Informatycznych przetwarzających dane w tym dane osobowe upoważniam Pana:

.....

(imię i nazwisko osoby upoważnionej)

zatrudnionego w

Urzędzie Gminy Wilkowice

.....

(nazwa jednostki i komórki organizacyjnej)

na stanowisku:

do przetwarzania danych osobowych w zakresie:

1. **Odczytu danych osobowych zawartych w informatycznym programie .....,**
2. **Dostępu do akt administracyjnych spraw prowadzonych Urzędzie Gminy Wilkowice**

.....

(podpis Administratora Danych Osobowych)

....

(podpis osoby upoważnionej) *(miejscowość data)*

Do wiadomości:

1. Pan/Pani ..... - Administrator Bezpieczeństwa Systemu,

Upoważnienie przyjęto do akt osobowych pracownika: .....

(data, podpis)

III.4 Rejestr osób upoważnionych do wprowadzania danych osobowych

Wzór

N.Znak:

REJESTR UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

W Urzędzie Gminy Wilkowice

wydanych w oparciu o Politykę Bezpieczeństwa Systemów Informatycznych

Założono dnia ..... 2009 r.

Wzór

Lp.	Nazwisko i imię	Numer upoważnienia, data	Nazwa zbioru	Okres dostępu	Podpis ABI
1				Do odwołania upoważnienia	
2				Do odwołania upoważnienia	
3				Do odwołania upoważnienia	
4				Do odwołania upoważnienia	
5				Do odwołania upoważnienia	

III.5 Dziennik systemu informatycznego

Wzór

Dziennik systemu informatycznego

ZAŁĄCZNIK NR .....
DO INSTRUKCJI ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM

Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu informatycznego, a w szczególności:

- *w przypadku awarii - opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski;*
- *w przypadku konserwacji systemu – opis podjętych działań, wnioski*

Lp	Data, godzina zgłoszenia zdarzenia – incydentu	Podjęte działania, opis materiału dowodowego	Wnioski i działania korygujące	Podpis osoby

III.6 Karta zakresu uprawnień pracownika

Wzór

logo	**ZAKRES UPRAWNIEŃ, OBOWIĄZKÓW I ODPOWIEDZIALNOŚCI PRACOWNIKA** **W URZĘDZIE GMINY WILKOWICE**
I CZĘŚĆ A.	
A1. DATA SPORZĄDZENIA	1. Data
II A2. DANE IDENTYFIKACYJNE PRACOWNIKA	
2. Imię i nazwisko	
3. Identyfikator pracownika w systemie informatycznym	
4. Stanowisko służbowe	
5. Stanowisko pracy	
6. Komórka organizacyjna	
7. Inne funkcje pełnione w Urzędzie (pełnomocnictwa, stałe zespoły)	
III CZĘŚĆ B.	
8. Podległość	
9. Współpraca	
IV. CZĘŚĆ C.	
V. C1. ZAKRES UPRAWNIEŃ	
10. Uprawnienia	
VI. C2. ZAKRES OBOWIĄZKÓW	
11. Obowiązki	
VII. C3. ZAKRES ODPOWIEDZIALNOŚCI	

12. Odpowiedzialność

VIII. CZĘŚĆ D.

IX. D1. DOKUMENT SPORZĄDZIŁ	X. D2. DOKUMENT ZATWIERDZIŁ
13. Pieczęć, data i podpis	14. Pieczęć, data i podpis

XI. D3. PRZYJĄŁ DO WIADOMOŚCI

Przyjmuję do wiadomości i stosowania niniejszy zakres uprawnień, obowiązków i odpowiedzialności oraz oświadczam, że znane mi są przepisy obowiązujące w realizacji zadań na danym stanowisku pracy.

15. Imię i nazwisko, data i podpis

ROZDZIELNIK:

LP.	ADRESAT
1.	Pracownik
2.	Przełożony pracownika
3.	Akta osobowe

III.7 Wykaz osób upoważnionych do obioru korespondencji

Wzór

WYKAZ OSÓB UPOWAŻNIONYCH

DO ODBIORU KORESPONDENCJI

KOMÓRKA ORGANIZACYJNA	SYMBOL	NAZWA

L.P.	IMIĘ I NAZWISKO OSOBY UPOWAŻNIONEJ	PODPIS OSOBY UPOWAŻNIONEJ

.....

data, pieczęć i podpis Kierownika komórki org.

III.8 Karta sprzętu - stanowiska komputerowego i jego stanu technicznego

Wzór

A. SPRZĘT KOMPUTEROWY			
I. A1. INFORMACJE O SPRZĘCIE			
L.p.	**RODZAJ SPRZĘTU**	pozytywny	negatywny*
	JEDNOSTKA CENTRALNA nr		
1.	parametry pozwalające na komfortową pracę z wybranymi aplikacjami i zapewnienie stabilności systemu		
2.	działające przyciski zasilania		
3.	cicha praca wentylatorów		
4.	aktywne diody sygnalizujące pracę komputera		
5.	stan czystości urządzenia		
	MONITOR nr		
1.	czytelne i jaskrawe znaki wyświetlane na monitorze		
2.	brak migotania obrazu, męczącego wzrok (odświeżanie)		
3.	możliwość regulacji i kąta położenia monitorów		
4.	nasycenie barw i kontrastu		
5.	brak uszkodzeń i przetarć na kablach i wtyczkach łączących monitor z komputerem oraz kablach zasilających		
6.	stan czystości urządzenia		
	DRUKARKA nr		
1.	czytelność wydrukowanego dokumentu		
2.	cicha praca		
3.	brak zacięć		
4.	działające przyciski uruchamiania oraz sterujące menu		

	drukarki		
5.	brak uszkodzeń i przetarć na kablach i wtyczkach łączących drukarkę z komputerem oraz kablach zasilających		
6.	stan czystości urządzenia		
	MYSZKA KOMPUTEROWA		
1.	Sprawność i stan czystości urządzenia		
	KLAWIATURA		
1.	Sprawność i stan czystości urządzenia		
	INNE ..... nr		
1.	Sprawność i stan czystości urządzenia		

II. A2. UWAGI

III. B. OPROGRAMOWANIE

IV. B1. SYSTEM OPERACYJNY

Nazwa	Nr licencji

V. B2. OPROGRAMOWANIE BIUROWE

Nazwa	Nr licencji
Nazwa	Nr licencji
Nazwa	Nr licencji
Nazwa	Nr licencji
Nazwa	Nr licencji

VI. B3. INNE OPROGRAMOWANIE UŻYTKOWE

Nazwa	Nr licencji
Nazwa	Nr licencji
Nazwa	Nr licencji

	Nazwa	Nr licencji
	Nazwa	Nr licencji
	Nazwa	Nr licencji

VII. B4. UWAGI

VIII. C. OCENA PRZYDATNOŚCI SPRZĘTU DO DALSZEJ EKSPLOATACJI

☐ przydatny ☐ nieprzydatny

IX. D. PODPISY

X. D1. DANE I PODPIS UŻYTKOWNIKA

Nazwisko i imię	Symbol komórki org.	Nr pokoju	Data	Podpis

D2. DANE I PODPIS OSOBY DOKONUJĄCEJ SPISU

Nazwisko i imię	Data	Podpis

* dla pozycji określonych jako negatywne w części A1, wskazać przyczyny w części A2. UWAGI

III.9 Zgłoszenie awarii sprzętu komputerowego

W z ó r

NR .....

I. RODZAJ I TYP URZĄDZENIA	II. NUMER INWENTARZOWY

III. OBJAWY

IV. D. PODPISY

V. D1. DANE I PODPIS UŻYTKOWNIKA ZGŁASZAJĄCEGO AWARIĘ

Nazwisko i imię	Symbol komórki org.	Nr pokoju	Data i godz.	Podpis

D2. DANE I PODPIS OSOBY PRZYJMUJĄCEJ ZGŁOSZENIE

Nazwisko i imię	Data	Podpis

III.10 Protokół z awaryjnego przeglądu/naprawy sprzętu komputerowego

Wzór

NR .....

RODZAJ I TYP URZĄDZENIA	NUMER INWENTARZOWY / użytkownik

STWIERDZONE USTERKI

GWARANCJA	Miejsce wykonania przeglądu-naprawy/wydania	Upoważniona osoba dokonująca czynności
[ ] TAK [ ] NIE		Nazwisko i imię

INFORMACJA O DALSZYCH DZIAŁANIACH

Data	Imię	Nazwisko	Podpis

IV Rozdział

Załączniki

IV.1 *Załącznik nr 1 – Audyt aplikacji przetwarzających dane osobowe*

LISTA KONTROLNA		
Nazwa i numer zadania audytowego:	**Audyt aplikacji przetwarzających dane osobowe**	Nr:
Nr dok. rob.		Data:
Wykonał:		
Organizacja:		Strona: ... / ...

1.	Czy stanowiska przeznaczone do przetwarzania danych osobowych są oznaczone?	
2.	Czy ustawienie monitorów jest zgodne z ustawą o ODO?	
3.	Czy jest ustanowiony ABI?	
4.	Czy jest ustanowiony ASI?	
5.	Czy mają zdefiniowane zakresy obowiązków?	
6.	Czy administrator prowadzi ewidencję osób upoważnionych do dostępu do DO?	
7.	Czy wszystkie osoby mające dostęp do danych osobowych	
7.1	zostały zapoznane z przepisami o ochronie danych osobowych?	
7.2.	zostały przeszkolone w zakresie zabezpieczeń systemu informatycznego?	
7.3.	uzyskały wpis do swojej karty zadań, określający indywidualny zakres odpowiedzialności danej osoby za ochronę danych osobowych?	
7.4.	złożyły oświadczenie według wzoru?	
8.	Czy oświadczenie, o którym mowa w pkt. 7.4 zostało dołączone do akt osobowych pracownika?	
9.	Czy w celu przetwarzania danych osobowych wdrożono odpowiedni poziom zabezpieczeń?	
10.	Czy zostały podjęte odpowiednie kroki lub zastosowane odpowiednie środki administracyjne ograniczające możliwość wystąpienia zagrożeń ze strony Internetu (zwłaszcza poczty elektronicznej) w systemach przetwarzających dane osobowe?	
11.	Czy w ramach nadzoru nad dostępem użytkowników do systemu informatycznego stosuje się procedurę przydziału uprawnień?	
12.	Czy uprawnienia dostępu do systemu informatycznego udzielone są wyłącznie osobom zatrudnionym przy	

LISTA KONTROLNA

Nazwa i numer zadania audytowego: **Audyt aplikacji przetwarzających dane osobowe**

Nr:

Nr dok. rob.

Data:

Wykonał:

Organizacja:

Strona: ... / ...

	przetwarzaniu danych osobowych?	
13.	Czy osoby niezatrudnione a wykonujące doraźne prace mają dostępu do danych osobowych?	
14.	Czy osoby mające dostęp do danych osobowych zobowiązywane są do zachowania danych w tajemnicy, także po ustaniu zatrudnienia?	
15.	Czy przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą?	
16.	Czy administrator danych nie zmienia celu przetwarzania danych?	
17.	Czy dane przechowywane są w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania?	
18.	Czy miało miejsce udostępnianie danych osobom nieupoważnionym ?	
18.1.	umyślne	
18.2.	nieumyślne	
19.	Czy w przypadku danych osobowych przechowywanych w postaci zapisu elektronicznego stwierdzono:	
19.1.	kradzież danych?	
19.2.	uszkodzenie danych?	
19.3.	zniszczenie danych?	
20.	Czy system informatyczny dla każdej osoby, której dane są w nim przetwarzane odnotowuje:	
20.1	datę pierwszego wprowadzenia danych tej osoby	
20.2	identyfikator wprowadzającego dane	
20.3	informację: komu, kiedy i w jakim zakresie dane zostały udostępnione, jeśli przewidziane jest udostępnianie danych innym podmiotom, chyba że dane te traktuje się jako dane powszechnie dostępne	
20.4	sprzeciw, o którym mowa w art. 32 ust. 1 pkt 7 ustawy o ochronie danych osobowych, po jego uwzględnieniu, oraz sprzeciwu określonego w art. 32 ust. 1 pkt 8 ustawy.	

LISTA KONTROLNA

Nazwa i numer zadania audytowego: **Audyt aplikacji przetwarzających dane osobowe**

Nr:

Nr dok. rob.

Data:

Wykonał:

Organizacja:

Strona: ... / ...

20.5	źródła pochodzenia danych	
21	Czy system informatyczny umożliwia udostępnienie na piśmie, w powszechnie zrozumiałej formie, treści danych o każdej osobie, której dane są przetwarzane, wraz z informacjami, o których mowa w § 31 ODO?	
22	Czy system informatyczny przetwarzający dane osobowe jest monitorowany w zakresie zabezpieczeń?	
23	Czy istnieje harmonogram monitorowania systemu informatycznego przetwarzającego dane osobowe?	
24	Czy ewidencjonowano i analizowano przypadki podejrzenia naruszenia zabezpieczeń danych osobowych oraz przypadki naruszenia zabezpieczeń systemu informatycznego?	
25	Czy ABI prowadzi rejestr, o którym mowa w ustawie?	
26	Czy przeprowadzono kontrolę ABI w zakresie sposobu prowadzenia rejestru, o którym mowa w ustawie ODO?	
27	Czy miejsce przechowywania informacji jest należycie zabezpieczone?	
28	Czy dane osobowe przechowywane są w postaci:	
28.1	wydruków?	
28.2	elektronicznej?	
29	Czy wydruki, zawierające dane osobowe przechowywane są w pomieszczeniach chronionych lub obiektach [np. szafach] odpowiednio zabezpieczonych?	
30	Czy wydruki, zawierające dane osobowe niszczone są niezwłocznie po ich wykorzystaniu?	

OBJAŚNIENIA UŻYTYCH ZNAKÓW I SKRÓTÓW

X	Dla pytań zamkniętych oznacza odpowiedź TAK lub NIE Dla pytań otwartych oznacza, że nie udziela się odpowiedzi TAK/NIE
ODO	Ochrona danych osobowych
ABI	Administrator Bezpieczeństwa Informacji
ASI	Administrator Systemu Informatycznego
DO	Dane osobowe

IV.2 *Załącznik nr 2 – Audyt bezpieczeństwa IT*

LISTA KONTROLNA		
Nazwa i numer zadania audytowego:	**Audyt bezpieczeństwa IT**	Nr:
Nr dok. rob.		
Wykonał:		Data:
Organizacja:		Strona: ... / ...
PLANY AWARYJNE		
1.	Czy istnieją plany awaryjne dla systemów informatycznych?	
2.	Czy wskazano kluczowe dane, systemy i procesy, których działania należy przywrócić?	
3.	Czy istnieje procedura szkolenia pracowników z planów awaryjnych IT?	
4.	Czy plany awaryjne są znane pracownikom organizacji?	
5.	Czy kopia planów awaryjnych przechowywana jest w bezpiecznym miejscu?	
6.	Czy plany awaryjne są systematycznie aktualizowane?	
7.	Czy w przypadku zmian w oprogramowaniu uaktualniane są kopie zapasowe?	
8.	Czy plany awaryjne systemów informatycznych zawierają:	
8.1.	wykaz osób odpowiedzialnych za przywrócenie funkcjonowania systemu	
8.2.	wykaz obowiązków i instrukcje postępowania dla członków zespołów awaryjnych,	
8.3.	sposoby informowania pracowników o sytuacjach awaryjnych,	
9.	Czy plan awaryjny IT jest testowany przynajmniej raz w roku?	
10.	Czy testowanie przeprowadzane jest dla wszystkich krytycznych zasobów?	
11.	Czy istnieje dokumentacja potwierdzająca przeprowadzenie testów planów awaryjnych?	
12.	Czy procedury bezpieczeństwa IT obejmują zasady tworzenia i przechowywania kopii zapasowych?	
13.	Czy ustalono czas niezbędny dla ponownego uruchomienia systemu po zaistnieniu awarii?	
POLITYKA BEZPIECZEŃSTWA I PROCEDURY		
1.	Czy organizacja opracowała politykę bezpieczeństwa IT w celu przeciwdziałania potencjalnym zagrożeniom?	
2.	Czy polityka bezpieczeństwa IT określa wymogi w zakresie bezpieczeństwa fizycznego?	
3.	Czy polityka bezpieczeństwa IT określa wymogi w zakresie bezpieczeństwa logicznego?	
4.	Czy polityka bezpieczeństwa IT definiuje standardy bezpieczeństwa, według których określany jest stopień wrażliwości informacji i aplikacji?	

LISTA KONTROLNA		
Nazwa i numer zadania audytowego:	**Audyt bezpieczeństwa IT**	Nr:
Nr dok. rob.		
Wykonał:		Data:
Organizacja:		Strona: ... / ...
5.	Czy podział zadań, obowiązków i odpowiedzialności w zakresie bezpieczeństwa IT jest jasno określony?	
6.	Czy istnieje procedura szkolenia pracowników z bezpieczeństwa IT?	
7.	Czy polityka bezpieczeństwa jest znana wszystkim pracownikom ?	
8.	Czy organizacja zarządza kontrolą dostępu fizycznego do urządzeń głównych?	
9.	Czy organizacja zarządza kontrolą dostępu logicznego do urządzeń głównych?	
10.	Czy istnieje procedura kontrolowania przyznanych praw dostępu do obszarów chronionych w celu weryfikacji ich aktualności?	
ZABEZPIECZENIA FIZYCZNE		
1.	Czy budynki są zabezpieczone [np. objęte monitoringiem, całodobową ochroną]?	
2.	Czy istnieją procedury zabezpieczenia fizycznego całego obiektu?	
3.	Czy plan ochrony fizycznej budynku i zastosowane sposoby ochrony odpowiadają wymaganym standardom w zakresie bezpieczeństwa?	
4.	Czy istnieją procedury dotyczące zabezpieczenia mienia przed kradzieżą?	
5.	Czy są wydzielone obszary chronione?	
6.	Czy pomieszczenia, w których znajdują się serwery są wyposażone w systemy przeciwpożarowe?	
7.	Czy pomieszczenia, w których znajdują się serwery są wyposażone w systemy antywłamaniowe?	
8.	Czy pomieszczenia, w których znajdują się serwery są zabezpieczone przed zalaniem?	
9.	Czy zostały zidentyfikowane inne zagrożenia fizyczne dla środowiska IT [sprzęt komputerowy, sieć itp.]?	
10.	Jeżeli zidentyfikowano „inne zagrożenia fizyczne", to czy opracowano odpowiednią procedurę postępowania?	
11.	Czy w pomieszczeniach, w których znajdują się serwery jest zainstalowana poprawnie działająca klimatyzacja?	
12.	Czy istnieje zasilanie awaryjne [np. agregaty prądotwórcze]?	
13.	Czy są przeprowadzane testy zasilania awaryjnego?	
14.	Czy istnieje dokumentacja powykonawcza zasilania awaryjnego?	
15.	Czy regularnie sprawdzane jest działanie systemu UPS?	
16.	Czy zainstalowane zamki posiadają atesty?	

LISTA KONTROLNA

Nazwa i numer zadania audytowego: **Audyt bezpieczeństwa IT** Nr:

Nr dok. rob.

Wykonał: Data:

Organizacja: Strona: ... / ...

17.	Czy wejścia/wyjścia obszarów chronionych są kontrolowane przez zamki mechaniczne?	
18.	Czy istnieją procedury przechowywania kluczy?	
19.	Czy klucze przechowywane są w bezpiecznym miejscu?	
20.	Czy istnieją procedury dotyczące wydawania i zdawania kluczy?	
21.	Czy istnieje rejestr pobierania i zdawania kluczy?	
22.	Czy wejścia/wyjścia obszarów chronionych są kontrolowane przez zamki szyfrowe?	
23.	Czy istnieje procedura opisująca częstotliwość zmian kodu dostępu?	
24.	Czy wejścia/wyjścia obszarów chronionych są kontrolowane przez komputerowy system dostępu do drzwi [np. kodowane karty magnetyczne]?	
25.	Jeżeli wykorzystywany jest komputerowy system kontroli dostępu, to czy:	
25.1	istnieje procedura nadawania praw dostępu do urządzeń kontrolnych (wydawania kart magnetycznych),	
25.2	istnieje rejestr wszystkich wejść i wyjść w określonym okresie czasu,	
25.3	zasilanie systemu jest zabezpieczone przez UPS,	
25.4	jest opracowana procedura na wypadek nietypowych lub awaryjnych zdarzeń związanych z działaniem systemu sterowania	
26.	Czy okna wychodzące na zewnątrz posiadają ochronę antywłamaniową [np. kraty, folia antywłamaniowa itp.]?	
27.	Czy ściany i drzwi są wykonane z właściwych materiałów?	
28.	Czy wszystkie urządzenia krytyczne znajdują się w obszarze chronionym?	
29.	Czy nie ma innych wejść do serwerowni poza kontrolowanymi drzwiami?	
30.	Czy fizyczne zabezpieczenia stanowisk komputerowych stanowią wystarczającą ochronę przed nieuprawnionym dostępem?	
ZABEZPIECZENIA LOGICZNE		
1.	Czy opracowano procedurę dotyczącą rejestracji zakupionego sprzętu i oprogramowania?	
2.	Czy opracowano procedurę dotyczącą dystrybucji [wydawanie / zdawanie] sprzętu i oprogramowania?	
3.	Czy rejestr posiadanego sprzętu i oprogramowania jest na bieżąco aktualizowany?	
4.	Czy prowadzony jest rejestr sprzętu użyczanego,	

LISTA KONTROLNA		
Nazwa i numer zadania audytowego:	**Audyt bezpieczeństwa IT**	Nr:
Nr dok. rob.		
Wykonał:		Data:
Organizacja:		Strona: ... / ...

	wynoszonego poza budynek?	
5.	Czy został wprowadzony system wykrywania prób uzyskania dostępu do danych przez nieuprawnionych użytkowników zewnętrznych?	
6.	Czy został wprowadzony system wykrywania prób uzyskania dostępu do danych przez nieuprawnionych użytkowników wewnętrznych?	
7.	Czy dostęp do systemu i danych wrażliwych jest zabezpieczony regularnie zmienianymi hasłami?	
8.	Czy dostęp i konto pracownika lub konsultanta jest niezwłocznie likwidowane po jego odejściu z pracy lub zmianie stanowiska?	
9.	Czy jest sprawdza skuteczność stosowanych haseł i zabezpieczeń (stosując np. specjalne oprogramowanie)?	
10.	Czy organizacja ogranicza zakres informacji dostępnej konsultantom, dostawcom, ewentualnie pracownikom zatrudnionym czasowo do niezbędnego minimum?	
11.	Czy stosuje się ochronę antywirusową?	
12.	Czy opracowano procedurę ochrony transmisji danych?	
13.	Czy opracowano procedurę wykonywania backupów?	
14.	Czy są wykonywane kopie danych znajdujących się na serwerach?	
15.	Czy częstotliwość i sposób wykonywania kopii gwarantuje możliwość odtworzenia danych sprzed awarii [utrata danych nie większa niż 1 dzień roboczy]?	
16.	Czy trwałość używanych nośników gwarantuje możliwość odtworzenia danych przez okres, co najmniej 5 lat?	
17.	Czy nośniki są odpowiednio katalogowane i przechowywane?	
18.	Czy nośniki przechowywane są w bezpiecznym miejscu poza budynkiem [np. skrytka bankowa]?	

Podpisano w dniu:.....

..... Podpis audytora

..... Podpis audytowanego