Zarządzenie nr 496/2021
Burmistrza Miasta i Gminy Syców
z dnia 3 marca 2021 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Ochrony Danych Osobowych - instrukcji uzupełniającej dla Urzędu Miasta i Gminy w Sycowie.

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2020 r. poz.713 ze zm.) zarządzam co następuje:

§ 1. Wprowadzam do stosowania Politykę Bezpieczeństwa Ochrony Danych Osobowych - instrukcję uzupełniającą dla Urzędu Miasta i Gminy w Sycowie stanowiącą załącznik do niniejszego zarządzenia.
§ 2. Wykonanie zarządzenia powierzam Sekretarzowi Miasta i Gminy Syców.
§ 3. Zarządzenie wchodzi w życie z dniem podjęcia.

BURMISTRZ
Dariusz Maniak

SEKRETARZ MIASTA I GMINY
Paweł Kwaśny

Załącznik do Zarządzenie nr 496 / 2021
Burmistrza Miasta i Gminy Syców
z dnia 3 marca 2021 r.

POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

- INSTRUKCJE UZUPEŁNIAJĄCE-

Zatwierdził	Stanowisko	Data	Podpis

SPIS TREŚCI

01	INSTRUKCJA WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI.

Celem instrukcji jest zapewnienie ciągłości działania systemów informatycznych przetwarzających dane osobowe oraz zabezpieczenie danych osobowych przed ich nieuprawnionym udostępnieniem.

Przeglądy i konserwacje systemu oraz aplikacji mają na celu zapewnienie:

1. Bezawaryjną pracę systemu IT, w tym: stacji roboczych, aplikacji serwerowych, baz danych, poczty email.
2. Optymalizację zasobów serwerowych, wielkości pamięci i dysków.
3. Sprawdzanie poprawności działania systemu IT, w tym: stacji roboczych, serwerów, drukarek, baz danych, poczty email.
4. Identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.

Sprzęt stanowiący zasób teleinformatyczny, podlega konserwacji według ustalonego planu wynikającego z zaleceń jego producenta oraz wskutek uwarunkowań wynikających z gwarancji.

Zasady wykonywania / zlecania napraw podmiotom zewnętrznym:

1. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego, mogą być prowadzone jedynie przez pracowników odpowiedzialnych za utrzymanie i bezpieczeństwo systemu informatycznego jednostki lub podmiot zewnętrzny świadczący tego rodzaju usługi na podstawie umowy lub w ramach gwarancji.
2. Konserwacja i naprawy sprzętu, na którym przetwarzane są dane osobowe odbywa się po uprzednim zawarciu umowy powierzenia.
3. Umowy serwisowe zawierane ze stronami trzecimi, w zakresie usług informatycznych i zabezpieczeń związanych z dostarczanymi usługami, muszą zawierać klauzulę, która zapewni wdrożenie, wykonywanie oraz utrzymanie przez stronę trzecią odpowiedniego poziomu usług i jakości mechanizmów ich zabezpieczenia.
4. W przypadku, gdy na nośnikach informacji, stanowiących integralną część sprzętu przekazywanego do naprawy, znajdują się dane osobowe, sprzęt taki naprawiany jest po uprzednim zawarciu umowy powierzenia przetwarzania danych osobowych z podmiotem wykonującym usługi naprawcze.

5. Czynności konserwacyjne i naprawcze wykonywane doraźnie przez osoby nie posiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych), muszą być wykonywane pod nadzorem osób upoważnionych.
6. Przed przekazaniem uszkodzonego sprzętu komputerowego z danymi osobowymi do naprawy poza obszar przetwarzania należy:
    a. wymontować nośniki z danymi osobowymi;
    b. trwale usunąć dane osobowe z użyciem specjalistycznego oprogramowania;
    c. nadzorować proces naprawy przez osobę upoważnioną przez administratora systemu, gdy nie ma możliwości usunięcia danych z nośnika.
7. Jeżeli w ramach naprawy gwarancyjnej, istnieje konieczność zwrotu urządzenia służącego do przechowywania danych osobowych lub informacji, dane osobowe lub **informacje muszą zostać z niego trwale usunięte.**
8. W przypadku zbywania lub przekazywania sprzętu do ponownego użytku, wszystkie składniki sprzętu zawierające nośniki, na których znajdują się dane osobowe lub informacje powinny być sprawdzone, czy dane osobowe lub informacje oraz licencjonowane oprogramowanie zostały fizycznie usunięte lub bezpiecznie nadpisane (zapisanie nośnika innymi informacjami).

Aktualizacje oprogramowania

1. ASI nadzoruje aktualizację oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki).
2. AD odpowiada za zapewnienie licencjonowanego oprogramowania do przetwarzania danych osobowych.

Zabezpieczenie oprogramowania

1. Oprogramowanie używane w systemie informatycznym jednostki musi być chronione przed niekontrolowaną modyfikacją, nieautoryzowanym usunięciem oraz dostępem osób nieupoważnionych.
2. Przed zainstalowaniem nowego oprogramowania należy sprawdzić jego działanie pod kątem bezpieczeństwa systemu informatycznego jednostki i zainstalowanych urządzeń, przy czym sprawdzenia dokonuje upoważniony pracownik lub firma zewnętrzna odpowiedzialna za utrzymanie i bezpieczeństwo system informatycznego jednostki.
3. W systemie informatycznym jednostki może być używane tylko i wyłącznie legalne oprogramowanie.
4. Lista oprogramowania tworzona i aktualizowana jest przez ASI lub osobę przez niego upoważnioną.
5. Oprogramowanie może być używane tylko zgodnie z postanowieniami licencji.
6. Za zgodą ASI dopuszcza się możliwość użytkowania otwartego oprogramowania (open source).

02	INSTRUKCJA REAGOWANIA NA INCYDENTY W OBSZARZE DANYCH OSOBOWYCH.

Celem procedury alarmowej jest skatalogowanie możliwych uchybień i zagrożeń oraz opisanie procedur działania w przypadku ich wystąpienia, jak i również ograniczenie ich powstania. Integralną częścią procedury alarmowej jest:

a. Dziennik uchybień i zagrożeń - Załącznik nr 1
b. Protokół Zagrożenia / Uchybienia - Załącznik nr 2
c. Procedura działań korygujących i zapobiegawczych
d. Procedura bieżącego szacowania ryzyka i wdrażanie wypracowanych wniosków

1. **Każdy pracownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować bezpośredniego przełożonego lub Inspektora Ochrony Danych (IOD).**
2. Do typowych incydentów w obszarze bezpieczeństwa danych osobowych należy:
   a. Niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
   b. Niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
   c. Nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek);
   d. Zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
   e. Zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych);
   f. Umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
3. Za naruszenie ochrony danych osobowych uznaje się przypadki, gdy:
   a. Stwierdzono naruszenie zabezpieczenia systemu ochrony danych osobowych;
   b. Stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.
4. W przypadku stwierdzenia incydentu (naruszenia), IOD prowadzi postępowanie wyjaśniające w toku, którego:
   a. Ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały;
   b. Zabezpiecza ewentualne dowody;
   c. Ustala osoby odpowiedzialne za naruszenie;
   d. Podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);
   e. Inicjuje działania dyscyplinarne;

f. Wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości, dokumentuje prowadzone postępowanie.

5. Osoba, która stwierdziła lub uzyskała informację wskazującą na naruszenie ochrony tego zbioru/ bazy danych zobowiązana jest do niezwłocznego:
   a. Zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu;
   b. Jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania;
   c. Powiadomienia o tym fakcie ASI bądź IOD.
6. ASI jest zobowiązany do niezwłocznego:
   a. Przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.;
   b. Podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym m.in. :
      - fizycznego odłączenia urządzeń i segmentów sieci które mogły umożliwić dostęp do bazy danych osobie niepowołanej;
      - wylogowania użytkownika podejrzanego o naruszenie ochrony danych;
      - zmianę hasła na koncie administratora i użytkownika, poprzez którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu.
   a. Szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych.
   b. Przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy/ zbioru danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą.

Po przywróceniu normalnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości:

1. Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych.
2. Jeżeli przyczyną zdarzenia była infekcja wirusem należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.
3. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika systemu należy wyciągnąć konsekwencje dyscyplinarne.

CHARAKTERYSTYKA MOŻLIWYCH „UCHYBIEŃ I ZAGROŻEŃ"

1. Uchybienia i zagrożenia niecelowe wewnętrzne i zewnętrzne.

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

a. Niewłaściwe zabezpieczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe;
b. Niewłaściwe zabezpieczenie sprzętu komputerowego;
c. Dopuszczenie do przetwarzania danych przez osoby nieposiadające upoważnienia;
d. Kradzież danych;
e. Kradzież sprzętu komputerowego;
f. Działanie wirusów i innego szkodliwego oprogramowania oraz działania, wskutek którego dojdzie do utraty danych osobowych lub uszkodzenia nośników danych.

2. Uchybienia i zagrożenia celowe wewnętrzne i zewnętrzne.

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

a. Celowe zniszczenie danych osobowych lub nośników danych;
b. Kradzież danych osobowych;
c. Dopuszczenie do przetwarzania danych osoby nieposiadającej stosownych uprawnień;
d. Kradzież sprzętu informatycznego;
e. Działanie wirusów i innego szkodliwego oprogramowania oraz działania, wskutek którego dojdzie do utraty danych osobowych lub uszkodzenia nośników danych.

3. 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:

a. Klęski żywiołowe;
b. Przerwy w zasilaniu;
c. Awaria serwera, komputera;
d. Pożar;
e. Zalanie wodą.

Administrator Danych poprzez IOD w przypadku stwierdzenia uchybienia:

a. Odnotowuje każde uchybienie w „Dzienniku Uchybień i Zagrożeń",
b. Sporządza „Protokół Uchybienia",
c. Wprowadza procedury uniemożliwiające ponowne powstanie uchybienia.

AD/ IOD w przypadku stwierdzenia zagrożenia:

a. Zabezpiecza dowody, powiadamia policję (w przypadku włamania);
b. Zabezpiecza dane osobowe oraz nośniki danych;
c. Odnotowuje każde zagrożenie w „DZIENNIKU UCHYBIEŃ I ZAGROŻEŃ";
d. Sporządza „PROTOKÓŁ ZAGROŻENIA";
e. Wprowadza procedury uniemożliwiające ponowne powstanie zagrożenia;
f. Podejmuje próbę przywrócenia stanu sprzed zaistnienia zagrożenia;
g. Wyciąga konsekwencje dyscyplinarne wobec osób odpowiedzialnych za zagrożenie a także inne przewidziane prawem.

REJESTR UCHYBIEŃ I ZAGROŻEŃ ORAZ POSTĘPOWANIE OSÓB FUNKCYJNYCH.

Kod uchybienia lub zagrożenia	Uchybienia i zagrożenia nieświadome 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 IOD. IOD sporządza protokół uchybienia.
2	Komputer nie jest zabezpieczony hasłem.	Należy zabezpieczyć dane osobowe oraz powiadomić IOD. IOD sporządza protokół uchybienia.
3	Dostęp do danych osobowych mają osoby nieposiadające upoważnienia.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić IOD. IOD sporządza protokół uchybienia.
4	Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym.	Należy powiadomić IOD, który sprawdza za pośrednictwem ASI system uwierzytelniania oraz sprawdza, czy nie doszło do kradzieży lub zniszczenia danych. IOD sporządza protokół uchybienia.
5	Próba kradzieży danych osobowych poprzez zewnętrzny nośnik danych.	Należy nie dopuścić do kradzieży danych i powiadomić IOD. IOD za pośrednictwem ASI zabezpiecza nośnik danych. IOD sporządza protokół zagrożenia. Należy powiadomić Policję.
6	Próba kradzieży danych osobowych w formie papierowej.	Należy nie dopuścić do kradzieży danych i powiadomić IOD. IOD lub osoba które otrzymała o powyższym informacje zabezpiecza dane. IOD sporządza protokół zagrożenia. Należy powiadomić Policję.
7	Nieuprawniony dostęp do danych osobowych w formie papierowej.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić IOD. IOD sporządza protokół uchybienia.
8	Dane osobowe przechowywane są w niezabezpieczonym pomieszczeniu.	Należy powiadomić IOD. Osoba odpowiedzialna zabezpiecza pomieszczenie. IOD sporządza protokół uchybienia.
9	Próba włamania do pomieszczenia/budynku.	Należy zabezpieczyć dowody i powiadomić IOD. IOD lub osoba upoważniona sprawdza stan uszkodzeń, zabezpiecza dowody i wzywa policję. IOD sporządza protokół zagrożenia. Należy powiadomić Policję.
10	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania.	Należy zrobić audyt systemów zabezpieczeń, a w szczególności systemów antywirusowych, firewall. IOD za pośrednictwem ASI ocenia, czy nie doszło do utraty danych osobowych i sporządza protokół uchybienia lub zagrożenia.
11	Brak aktywnego oprogramowania antywirusowego.	Należy powiadomić ASI. ASI aktualizuje lub nabywa oprogramowanie antywirusowe. IOD sporządza protokół uchybienia.
12	Zniszczenie lub modyfikacja danych osobowych w formie papierowej.	Należy zabezpieczyć dowody i powiadomić IOD. IOD lub osoba upoważniona sprawdza stan uszkodzeń, zabezpiecza dowody. IOD sporządza protokół zagrożenia.
13	Zniszczenie lub modyfikacja danych osobowych w systemie informatycznym.	Należy zabezpieczyć dowody i powiadomić ASI. ASI sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia IOD. IOD sporządza protokół zagrożenia.
14	Uszkodzenie komputerów, nośników danych.	Należy powiadomić ASI. ASI ocenia w wyniku czego doszło do zniszczenia i przywraca dane z kopii zapasowej. ASI powiadamia IOD, który sporządza protokół zagrożenia.
15	Próba nieuprawnionej interwencji przy sprzęcie komputerowym.	Należy uniemożliwić dostęp osób do sprzętu komputerowego oraz powiadomić ASI. IOD sporządza protokół uchybienia.
16	Zdarzenia losowe.	Należy oszacować powstałe starty i sporządzić protokół zagrożenia lub uchybienia.
17	Inne	Należy dokonać identyfikacji zagrożenia oraz wdrożyć adekwatne środki zapobiegawcze

Administrator Systemu Informatycznego w obszarze swojej odpowiedzialności przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia i **w terminie nieprzekraczającym 48 godzin** od daty jego zaistnienia i przekazuje go IOD. Inspektor Ochrony Danych sporządza protokół oraz kolejno wdraża procedury:

1. Procedura działań korygujących i zapobiegawczych;
2. Procedura bieżącego szacowania ryzyka i wdrożenie wypracowanych wniosków;
3. Zawiadomienie UODO oraz osoby, której dane dotyczą – o ile incydent wymaga takiej czynności.

ZAWIADAMIANIE OSOBY, KTÓREJ DANE DOTYCZĄ, O NARUSZENIU OCHRONY DANYCH OSOBOWYCH.

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator Danych bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie musi być przekazane, jasnym i prostym językiem
   i opisywać charakter naruszenia ochrony danych osobowych.
2. Zawiadomienie, nie jest wymagane, w następujących przypadkach:
   a. Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
   b. Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
   c. Wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.
3. **Jeżeli naruszenie dotyczy danych osobowych szczególnej kategorii należy uznać, że zachodzi wysokie prawdopodobieństwo naruszenia praw i wolności osoby fizycznej.**

Załącznik nr 1

DZIENNIK UCHYBIEŃ I ZAGROŻEŃ

Kod	Data i godzina zdarzenia	Rodzaj zdarzenia (uchybienie/ zagrożenie)	Opis zdarzenia	Skutki zdarzenia	Działania korygujące	Podpis IOD

Załącznik nr 2

REJESTR NARUSZEŃ

zasad ochrony danych osobowych

Numer (kolejny) incydentu	..... nr/rok
zgłaszający	..... imię i nazwisko
data i godzina zgłoszenia	.....

opis naruszenia/incydentu	.....
jakich danych dotyczy naruszenia [zbiór danych lub ich kategoria]	.....
naruszenie przepisów prawa	TAK / NIE
Zidentyfikowana przyczyna wystąpienia naruszenia [jeśli została zidentyfikowana]	.....
Podjęte działania naprawcze	.....
Konieczność podjęcia działań korygujących w ramach zasad przetwarzania danych osobowych	TAK / NIE
Proponowane działania korygujące	.....
Czy wymagane jest powiadomienie:	Organu nadzorczego: □ NIE Podmiotu danych: □ NIE

Przyjmuję do wiadomości:	
..... data i podpis IOD	..... data i podpis AD

Załącznik nr 3

Analiza zdarzenia pod kontem znamion naruszenia praw lub wolności osób fizycznych.

1. **Wypełnia AD, IOD lub ASI:**

1. Czy zdarzenie wpłynęło na niżej wymienione prawa i wolności osób których danych dotyczyło (wpisać tak lub nie).

z zakresu praw i wolności osobistych:

- prawo do życia:
- nietykalność i wolność osobista:
- prawo do sprawiedliwego procesu:
- prawo do nieujawniania informacji o osobie bez podstawy prawnej:
- prawo do żądania sprostowania oraz usunięcia informacji: (nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny zustawą)
- prawo dostępu do dokumentów urzędowych dotyczących osoby:
- prawo do ochrony prawnej życia prywatnego:
- prawo rodziców do wychowania dzieci w zgodzie z własnymi przekonaniami:
- prawo do wolności oraz ochrony tajemnicy komunikowania się:
- prawo do nienaruszalności mieszkania:
- wolność poruszania się po terytorium RP:
- wolność sumienia i religii:
- prawo do wolności poglądów oraz do rozpowszechniania informacji:

z zakresu praw i wolności politycznych:

- prawo do organizowania pokojowych zgromadzeń oraz uczestnictwa w nich:
- wolność zrzeszania się:
- wolność zrzeszania się w związkach zawodowych:
- wolność zrzeszania się w organizacjach społeczno-politycznych:
- prawo do uczestnictwa w referendum czy prawo wyboru: (prezydenta, posłów, senatorów oraz przedstawicieli do organów władzy samorządowej)
- prawo do składania wniosków, petycji oraz skarg:

z zakresu wolności i praw ekonomicznych, socjalnych i kulturalnych:

- prawo do posiadania własności oraz prawo do dziedziczenia:
- wolność wyboru miejsca pracy i wykonywania zawodu:
- prawo do bezpiecznych i higienicznych warunków pracy:
- prawo do zabezpieczenia społecznego w razie niezdolności do pracy: (spowodowanej chorobą, inwalidztwem czy podeszłym wiekiem)
- prawo do ochrony zdrowia:
- prawo do nauki:
- ochrona praw dziecka:
- wolność twórczości artystycznej i badań naukowych:

2. **Charakter naruszenia danych osobowych (elektroniczne, fizyczne, wielokrotne, jednokrotne):**

   .....

3. **Kategorie osób i liczba osób których dane naruszono (np. osoby fizyczne – wnioskodawcy, pracownicy, itp.):**

   .....

4. **Kategoria i liczba wpisów danych osobowych których dane naruszono (np. wpisy z systemu jakiego lub strony z prowadzonych akt itp.):**

   .....

5. **Dane Inspektora Ochrony Danych osobowych na dzień zgłoszenia (jeżeli wyznaczono):**

   .....

6. **Możliwe konsekwencje naruszenia danych osobowych (np. brak możliwości wglądu w dokumenty lub system, zagrożenie kradzieży tożsamości, sprzedaż danych osobowych, nielegalne uzyskanie kredytu, nielegalny wynajem mieszkania, samochodu, użycie danych do zastawu itp.):**

   .....

7. **Czy wymaga zgłoszenia do organu nadzorczego, jeżeli nie to uzasadnić, dlaczego:**

   .....

.....
(data, podpis czytelny AD)

Przyjęto zgłoszenie i odnotowano w rejestrze incydentów/naruszeń danych osobowych.

.....
(data i podpis)

03 INSTRUKCJA AUDYTÓW WEWNĘTRZNYCH TESTU BEZPIECZEŃSTWA SYSTEMU PRZETWARZAJĄCEGO DANE OSOBOWE.

Audyt bezpieczeństwa – to proces zbierania i oceniania dowodów w celu określenia czy system ochrony danych osobowych oraz system informatyczny i związane z nim zasoby właściwie chronią majątek, utrzymują integralność danych i dostarczają odpowiednich i rzetelnych informacji, osiągają efektywnie cele organizacji, oszczędnie wykorzystują zasoby i stosują mechanizmy kontroli wewnętrznej, tak aby dostarczyć rozsądnego zapewnienia, że osiągane są cele operacyjne i kontrolne, oraz że chroni się przed niepożądanymi zdarzeniami lub są one na czas wykrywane a ich skutki na czas korygowanej.
Audyt jest prowadzony w celu stwierdzenia stopnia zgodności ocenianego systemu z określonym standardem lub normą wybraną jako punkt odniesienia.

Zakres i częstotliwość audytu wewnętrznego.

1. Przyjęto zasadę, że audyty wewnętrzne mogą być okresowe – nie rzadziej niż raz w roku lub doraźne (w przypadku istotnej zmiany w konfiguracji, wystąpienia incydentu w obszarze danych osobowych lub wystąpienia incydentu związanego z bezpieczeństwem fizycznym stref przetwarzania). W skład zespołu audytowego wchodzą: Inspektor Ochrony Danych, ASI w razie potrzeby specjaliści w danej dziedzinie (np. księgowości).
2. Po przeprowadzeniu okresowego audytu bezpieczeństwa Inspektor Ochrony Danych tworzy protokół z przebiegu audytu uwzględniający wszystkie zagadnienia zgodnie z Załącznikiem nr 1 „Kwestionariusz audytu wewnętrznego systemu do przetwarzania danych osobowych".
3. Na spotkaniu zamykającym audyt omawiany jest zatwierdzony przez AD protokół oraz wypełniony kwestionariusz audytu wewnętrznego oraz odbywa się analiza zagrożeń dla wszystkich obszarów, w których może wystąpić ryzyko zagrożeń dla bezpieczeństwa danych osobowych i zasobów systemu teleinformatycznego.
4. W przypadku audytu doraźnego audytowana i wyjaśniana jest sytuacja związana z incydentem, jego zagrożeniami i skutkami. W trakcie audytu prowadzone są wyjaśnienia i rozmowy z użytkownikami na okoliczność incydentu.
5. Po audycie doraźnym Inspektor Ochrony Danych sporządza protokół z audytu oraz dokonuje się ponownego szacowania ryzyka w audytowanym obszarze dla przetwarzanych danych osobowych w systemie teleinformatycznym (wraz z ASI), ocenę zagrożeń i ewentualne środki, które należałoby podjąć dla podniesienia poziomu bezpieczeństwa i wyeliminowania incydentów.

Test bezpieczeństwa systemu teleinformatycznego przetwarzającego dane osobowe.

1. Za przygotowanie i opracowanie planu testów bezpieczeństwa odpowiada ASI. W realizacji omawianego przedsięwzięcia może uczestniczyć Inspektor Ochrony Danych.
2. Testy bezpieczeństwa będą prowadzone raz w roku, z którego ASI zobowiązany jest sporządzić stosowny raport i przedstawić go AD oraz IOD.
3. W ramach testu bezpieczeństwa systemu teleinformatycznego przeprowadzona zostanie analiza procedur zawartych w „Polityce Bezpieczeństwa", założenia i prowadzenia wymaganej dokumentacji, rejestrów, oświadczeń.

4. Ponadto kontroli będą podlegać zdarzenia generowane przez logi systemowe, analiza i raportowanie dzienników zdarzeń. Jednocześnie skontrolowana zostanie wiedza użytkowników systemu teleinformatycznego przetwarzającego dane osobowe.
5. Zakres testowanych zabezpieczeń systemu teleinformatycznego będzie obejmował wybrane zagadnienia ujęte w kwestionariuszu audytu wewnętrznego.
6. Raport z przeprowadzonego testu bezpieczeństwa opracowuje ASI i przedstawia do zapoznania Inspektorowi Ochrony Danych i AD.
7. Test bezpieczeństwa systemu teleinformatycznego może być prowadzony okresowo lub doraźnie na polecenie AD lub IOD.

Załącznik nr 1

KWESTIONARIUSZ AUDYTU WEWNĘTRZNEGO SYSTEMU TELEINFORMATYCZNEGO PRZETWARZAJĄCEGO DANE OSOBOWE.

LP	ZAGADNIENIE	TAK	NIE	UWAGI
	Bezpieczeństwo osobowe, uprawnienia do dostępu do danych osobowych przetwarzanych w systemie			
1.	Czy w jednostce organizacyjnej wyznaczone zostały osoby formalnie odpowiedzialne za zapewnienie funkcjonowania i bezpieczeństwa systemu (ASI)?			
2.	Czy osoby odpowiedzialne w jednostce organizacyjnej za ochronę danych osobowych przetwarzanych w systemie mają określone zakresy zadań i odpowiedzialności?			
3.	Czy użytkownicy systemu posiadają uprawnienia do dostępu do danych osobowych przetwarzanych w systemie?			
4.	Czy wszyscy użytkownicy systemu posiadają zaświadczenia o odbyciu szkolenia w zakresie ochrony danych osobowych?			
5.	Czy przed dopuszczeniem do pracy w systemie użytkownicy odbyli szkolenie w zakresie zasad bezpiecznego funkcjonowania systemu oraz praktycznego stosowania procedur?			
6.	Czy użytkownicy systemu potwierdzili fakt zapoznania się i zrozumienia PB i procedur po przez podpisanie oświadczenia o zachowaniu poufności?			
7.	Czy w przypadku zwolnienia z pracy użytkownika systemu blokowana jest skutecznie możliwość dostępu do systemu? Jak wygląda procedura, gdzie jest ujęta?			
8.	Czy w przypadku zwolnienia z pracy stosowana jest zasada całkowitego rozliczenia użytkownika systemu z posiadanych zasobów? *Uwaga: wymaganie dotyczy przykładowo rozliczenia z posiadanych sprzętowych tokenów uwierzytelniających, kluczy, kart identyfikacyjnych, przepustek, itp.*			
9.	Czy określone zostały zasady podejmowania decyzji w sprawie dalszego wykorzystywania zasobów informacyjnych będących w posiadaniu zwalnianych lub przenoszonych na inne stanowiska pracowników lub ich usunięcia z systemu? Gdzie została ujęta?			

LP	ZAGADNIENIE	TAK	NIE	UWAGI
	Bezpieczeństwo fizyczne systemu			
1.	Czy określono strefy przetwarzania i ich lokalizacje dla poszczególnych elementów systemu?			
2.	Czy prawidłowo eksploatowany jest system zabezpieczający strefy przetwarzania (zarządzanie kluczami, monitoring)?			
3.	Czy prowadzona jest weryfikacja osób wchodzących do stref przetwarzania? W jaki sposób?			
4.	Czy przyznawanie /odbieranie środków kontroli dostępu fizycznego (klucze, karty, kody, hasła itp.) do stref przetwarzania prowadzone jest zgodnie z zapisami polityki bezpieczeństwa?			
	Ciągłości działania, kopie zapasowe, alternatywne łącza, Urządzenia, zasilanie awaryjne			
1.	Czy prowadzony jest wykaz osób odpowiedzialnych w jednostce za ciągłość działania systemu i czy aktualne są ich dane kontaktowe?			
2.	Czy osoby odpowiedzialne za realizację planu ciągłości działania zostały przeszkolone w zakresie ich zadań zgodnie z zaplanowaną częstotliwością?			
3.	Czy kopie zapasowe danych systemu są tworzone i przechowywane zgodnie z zasadami opisanymi w PB?			
4.	Czy tworzone i właściwie przechowywane są kopie zapasowe systemów operacyjnych, oprogramowania krytycznego dla systemu? Co jaki okres czasu, gdzie są przechowywane?			
	Utrzymanie systemu, przeglądy diagnostyczne, naprawy			
1.	Czy prowadzona jest dokumentacja dotyczącą napraw i przeglądów diagnostycznych systemu TI zgodnie z zapisami zawartymi w dokumentacji bezpieczeństwa systemu?			
2.	Czy w systemie TI kontrolowane jest wykorzystanie urządzeń i narzędzi diagnostycznych? W jaki sposób?			
3.	Czy dokonywanie napraw elementów systemu TI poza lokalizacjami organizacji jest przeprowadzane i dokumentowane zgodnie z dokumentacją bezpieczeństwa systemu TI?			
4.	Czy prace naprawcze i przeglądy prowadzone przez serwis zewnętrzny są nadzorowane i dokumentowane przez administratora systemu lub uprawnionych pracowników? Gdzie są odnotowane?			
5.	Czy warunki realizacji umów serwisowych przez dostawców zewnętrznych są zgodne z zapisami zawartymi w PB?			

LP	ZAGADNIENIE	TAK	NIE	UWAGI
6.	Czy wyznaczono osoby odpowiedzialne w jednostce za nadzór nad pracami naprawczymi i przeglądami prowadzonymi przez serwisy zewnętrzne?			
Zapobieganie i reagowanie na incydenty bezpieczeństwa, ochrona przed oprogramowaniem złośliwym				
1.	Czy wprowadzone zostały zasady i procedury wykonywania bieżącej analizy i oceny bezpieczeństwa systemu?			
2.	Czy wprowadzone zostały zasady i procedury związane z przygotowywaniem planu działań naprawczych lub korekcyjnych w celu usunięcia nieprawidłowości stwierdzonych w czasie weryfikacji poprawności działania zabezpieczeń (np. okresowe testy bezpieczeństwa), a także w sytuacji związanej z koniecznością lub potrzebą wprowadzenia zmian w systemie (np. w wyniku wystąpienia incydentu bezpieczeństwa lub na podstawie wyników okresowo przeprowadzonego procesu szacowania ryzyka)?			
3.	Czy prowadzone są okresowe szkolenia w zakresie problematyki reagowania na incydenty bezpieczeństwa?			
4.	Czy w systemie zastosowano mechanizmy lub procedury zapobiegające incydentom bezpieczeństwa w systemie, w tym zabezpieczające przed działaniem oprogramowania złośliwego, a także umożliwiające jak najszybsze wykrywanie incydentów bezpieczeństwa systemu oraz zapewniające niezwłoczne informowanie odpowiednich osób o wykrytym incydencie?			
5.	Czy dla systemu przeprowadzany jest ponowny proces szacowania ryzyka w przypadku zaistnienia istotnego incydentu bezpieczeństwa?			
6.	Czy w systemie wdrożone zostały metody postępowania z incydentami bezpieczeństwa?			
7.	Czy w systemie dokumentuje się przypadki wystąpienia incydentów bezpieczeństwa oraz sposób wyjaśnienia przyczyn powstania incydentów i ich skutków?			
8.	Czy system chroniony jest przed złośliwym oprogramowaniem?			
9.	Czy mechanizmy ochrony przed kodem złośliwym są skonfigurowane tak, aby uruchamiać oprogramowanie wykrywające kod złośliwy po uruchomieniu systemu na stacjach roboczych i w takiej konfiguracji, aby wykrywać i usuwać kod złośliwy przynajmniej: (i) przesłany za pośrednictwem poczty elektronicznej, w tym, jako załącznik do poczty elektronicznej, (ii) wprowadzany			

LP	ZAGADNIENIE	TAK	NIE	UWAGI
	w wyniku dostępu do stron WWW oraz (iii) wprowadzany za pośrednictwem nośników przenośnych?			
10.	Czy monitorowane są zdarzenia mające wpływ na bezpieczeństwo danych osobowych przetwarzanych w systemie?			
	Zasady wprowadzania poprawek, aktualizacja oprogramowania			
1.	Czy poprawki/uaktualnienia do oprogramowania i systemu operacyjnego wprowadzane są na bieżąco, odpowiednio testowane i dokumentowane?			
2.	Czy system wykrywa nieautoryzowane zmiany w oprogramowaniu i konfiguracji?			
	Ochrona informatycznych nośników danych			
1.	Czy istnieje wykaz rodzajów informatycznych nośników danych dopuszczonych do wykorzystania w systemie. Czy nośniki te są zabezpieczone (np. szyfrowane)?			
2.	Czy nośniki zawierające dane osobowe są właściwie ewidencjonowane i przechowywane?			
3.	Czy właściwie realizowane są zasady przydzielania uprawnień użytkownikom do korzystania z nośnika i rozliczania użytkowników z posiadanych nośników?			
4.	Czy wdrożono środki umożliwiające realizację procedur niszczenia nośników danych?			
	Identyfikacja i uwierzytelnianie użytkowników i Urządzeń			
1.	Czy wprowadzono mechanizmy uwierzytelniania użytkowników podczas dostępu do urządzeń i usług systemu?			
2.	Czy hasła użytkowników systemu mają odpowiednią długość i stopień złożoności oraz czy są zmieniane zgodnie z PB?			

LP	ZAGADNIENIE	TAK	NIE	UWAGI
	Kontrola dostępu do systemu			
1.	Czy prowadzony jest rejestr użytkowników uprawnionych do pracy w systemie z wyszczególnieniem informacji o posiadanych przez nich uprawnieniach?			
2.	Czy ewidencja użytkowników jest uaktualniana na bieżąco?			
3.	Czy zarządzanie kontami użytkowników systemu (zakładanie, przyznawanie uprawnień, modyfikowanie uprawnień, blokowanie, usunięcie itp.) jest zgodne z zapisami zawartymi w dokumentacji bezpieczeństwa?			
4.	Czy przegląd działań użytkowników dokonywany jest zgodnie z opisanym w polityce okresem czasowym i zakresem objętym przeglądem?			
5.	Czy w systemie stosuje się zasadę przyznawania ,,minimum uprawnień" wymaganych do pracy w systemie?			
6.	Czy w systemie zastosowano automatyczną blokadę dostępu do zasobów, po wyczerpaniu nieudanych prób logowań?			
7.	Czy system blokuje dostęp użytkownika po braku jego aktywności?			
	Audyt wewnętrzny, testy bezpieczeństwa systemu			
1.	Czy audyty wewnętrzne przeprowadzane są zgodnie z zaplanowaną częstotliwością?			
2.	Czy ustalono osoby odpowiedzialne za przeprowadzanie okresowych audytów wewnętrznych i czy zostały im przydzielone zadania w tym zakresie?			
3.	Czy były przeprowadzane dodatkowe, nieplanowane audyty wewnętrzne spowodowane wystąpieniem incydentu bezpieczeństwa?			

LP	ZAGADNIENIE	TAK	NIE	UWAGI
4.	Czy audyty wewnętrzne są odpowiednio dokumentowane?			
5.	Czy zalecenia po audytach zostały zrealizowane?			
6.	Czy w systemie określone zostały zdarzenia, które podlegają procedurom audytu bezpieczeństwa systemu z powodu ich istotności dla bezpieczeństwa systemu?			
7.	Czy w systemie występują elementy, które generują zapisy audytowe (np. mechanizmy systemowe - zasady inspekcji)?			
8.	Czy lista audytowanych w systemie zdarzeń jest okresowo przeglądana i aktualizowana?			
9.	Czy system tworzy zapisy audytowe dotyczące rodzaju zdarzenia, daty, miejsca i czasu zdarzenia, źródła zdarzenia, skutku zdarzenia (sukces/porażka), tożsamości użytkownika związanego ze zdarzeniami?			
10.	Czy w systemie wprowadzono taką pojemność baz danych zawierających informacje o audytowanych zdarzeniach, aby zapobiec możliwości utraty informacji w skutek przepełnienia w założonym czasie (np. wielkość plików zawierających dzienniki zdarzeń)?			
11.	Czy system zapewnia ochronę danych osobowych i narzędzi audytowych przed nieautoryzowanym dostępem, modyfikacją oraz usunięciem?			
	Zarządzanie ryzykiem			
1.	Czy formalnie została powołana struktura organizacyjna odpowiedzialna za zarządzanie ryzykiem w systemie?			
2.	Czy przeprowadzane były szacowania ryzyka po wykryciu nowych zagrożeń lub zidentyfikowaniu nowych podatności, które nie były rozpatrywane podczas wcześniejszego szacowania ryzyka dla bezpieczeństwa danych osobowych?			

LP	ZAGADNIENIE	TAK	NIE	UWAGI
3.	Czy monitorowane są czynniki ryzyka bezpieczeństwa systemu oraz czy odpowiednio raportowane są wszelkie naruszenia bezpieczeństwa?			
4.	Czy okresowo przeglądane są rejestry zdarzeń systemów ochrony fizycznej, czy są właściwe przechowywane?			
5.	Czy są aktualne wyznaczone ryzyka szczątkowe i czy zostały zaakceptowane przez AD?			

04	INSTRUKCJA CIĄGŁOŚCI DZIAŁANIA.

Celem instrukcji jest zapewnienie ciągłości działania systemów przetwarzających dane osobowe oraz zabezpieczenie danych osobowych przed ich nieuprawnionym udostępnieniem.
Podstawowymi elementami instrukcji jest: struktura zarządzania kryzysowego, zasady postępowania w sytuacjach kryzysowych i awaryjnych.
Strategia zachowania ciągłości działania jest opracowywana na podstawie zebranych podczas analizy ryzyka i wpływu na działanie wymagań dotyczących parametrów odtworzenia z uwzględnieniem celów i dostępnych zasobów.

I. WPROWADZENIE I UTRZYMANIE SYSTEMU CIĄGŁOŚCI DZIAŁANIA

1) Efektywność systemu ciągłości działania realizuje się poprzez następujące działania:

- Testowanie: cykliczne sprawdzanie skuteczności planu ciągłości działania. Testy są także efektywną metodą szkolenia i budowania świadomości na wszystkich szczeblach organizacji.
- Aktualizację: regularne sprawdzanie i dostosowanie do zmieniających się warunków wewnętrznych o zewnętrznych umożliwia utrzymanie efektywnego planu działania na wypadek sytuacji kryzysowej.
  Odpowiedzialny: Administrator Systemu Informatycznego

- Audyt: pozwala na stwierdzenie czy spełnia on wymogi zgodności z przyjętą polityką ochrony danych – instrukcją ciągłości działania, przepisami prawa oraz normami i rekomendacjami regulatorów.
  Odpowiedzialni: Inspektor Ochrony Danych, Administratora Systemu Informatycznego

- Szkolenia i akcje informacyjne: system powinien realizować zadania szkoleniowe, ogólne dla wszystkich pracowników oraz specjalistyczne dla członków struktury zarządzania kryzysowego. Szkolenia ogólne powinny być wspierane okresowymi akcjami informacyjnymi, których głównym celem jest budowanie świadomości pracowników.
  Odpowiedzialni: Inspektor Ochrony Danych, Administrator systemu Informatycznego, Pracownik wskazany przez AD odpowiedzialny za sprawy organizacyjno – administracyjne

II. BIEŻĄCE DZIAŁANIA ZAPEWNIAJĄCE CIĄGŁOŚĆ DZIAŁANIA

1) Aktualizacje oprogramowania

a) ASI nadzoruje aktualizację oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki).
b) AD odpowiada za zapewnienie licencjonowanego oprogramowania do przetwarzania danych osobowych.

2) Zabezpieczenie oprogramowania.

a) Oprogramowanie używane w systemie informatycznym jednostki musi być chronione przed niekontrolowaną modyfikacją, nieautoryzowanym usunięciem oraz dostępem osób nieupoważnionych.

b) Przed zainstalowaniem nowego oprogramowania należy sprawdzić jego działanie pod kątem bezpieczeństwa systemu informatycznego jednostki i zainstalowanych urządzeń, przy czym sprawdzenia dokonuje ASI lub osoba upoważniona przez AD.

3) Wykonywanie kopii systemów informatycznych.

a) Na potrzeby zachowania ciągłości działania systemów informatycznych i utrzymania integralności danych, wykonuje się następujące kopie zapasowe:
   - Bazy danych;
   - Pliki i katalogi na stacjach roboczych / serwerach;
   - Systemy operacyjne stacji roboczych / serwerów.

b) Zaleca się, aby wykonywanie kopii zapasowych realizowane były zgodnie z przyjętym harmonogramem.

c) Kopie tworzone są całościowo, następnie przyrostowo, tzn. kopiowane są pliki nowe i te których zawartość uległa zmianie.

d) Wyniki tworzenia kopii zapasowych są rejestrowane automatycznie.

e) Kopie zapasowe sporządza się również w następujących przypadkach:
   - przed dokonaniem istotnej zmiany konfiguracyjnej (np. aktualizacji oprogramowania, ustawień systemowych);
   - po przeprowadzeniu zmiany konfiguracyjnej (np. aktualizacji oprogramowania, ustawień systemowych, zmianie praw dostępu).

f) Kopie zapasowe, wykonane w danym dniu przechowywane są przez okres 2 miesięcy.

g) Po ustaniu użyteczności kopii zapasowej jest ona niezwłocznie usuwana.

h) Kopie zapasowe konfiguracji systemów operacyjnych serwerów wykowywane są za pomocą dedykowanego oprogramowania.

i) Miejscem przechowywania kopii zapasowych jest wydzielona macierz lub nośnik zewnętrzny, zlokalizowane w innym miejscu (budynku) niż są wykonywane.

j) Za prawidłowość tworzenia kopii zapasowych odpowiada Administrator Systemu Informatycznego.

4) Profilaktyka antywirusowa.

a) Osobą prowadzącą działania profilaktyczne mające na celu ochronę zasobów sieci komputerowej przed atakami wirusów komputerowych jest Administrator Systemu Informatycznego.

b) Ochrona antywirusowa zasobów informatycznych jest realizowana przez system antywirusowy:

c) Aktualizacja baz sygnatur wirusów:
   - Bazy sygnatur wirusów dla serwera są aktualizowane bezpośrednio z serwera producenta systemu antywirusowego;
   - Bazy sygnatur wirusów dla stanowisk roboczych są aktualizowane bezpośrednio

z serwera producenta systemu antywirusowego;

- Aktualizacja baz sygnatur wirusów odbywa się nie rzadziej niż jeden raz każdego dnia roboczego.

5) Kontrola antywirusowa.

a) Zasoby informatyczne są skanowane na bieżąco za pomocą modułu rezydentnego;

b) Kontroli podlegają wszystkie pliki (odczytywane i zapisywane) w tym poczta elektroniczna;

c) System antywirusowy jest zaprogramowany do wykonywania okresowych kontroli antywirusowych całego systemu plików;

d) Kontrole te są wykonywane przez program automatycznie nie rzadziej niż jeden raz w tygodniu;

e) Zabrania się korzystania ze stanowiska bez aktywnego programu antywirusowego.

6) System zasilania awaryjnego

a) Funkcją układów zasilania awaryjnego jest zapewnienie zasilania systemom informatycznym podczas zaniku napięcia w podstawowym źródle zasilania.

b) Zaleca się stosowanie:

- indywidualny zasilacz UPS – przeznaczony do podtrzymania zasilania komputerów osobistych;
- zasilacze UPS centralne – zabezpieczają np. urządzenia w serwerowni lub cały budynek;
- akumulatory – stosowane w laptopach (urządzeniach mobilnych).

III. POSTĘPOWANIE W PRZYPADKU AWARII

W przypadku awarii systemu, Administrator Systemu Informatycznego, po usunięciu przyczyny zaistniałej awarii, dokonuje przywrócenia systemu operacyjnego oraz zainstalowanego oprogramowania, jeśli zajdzie taka konieczność. Korzysta przy tym z posiadanego licencjonowanego oprogramowania oraz danych wcześniej zarchiwizowanych. W przypadku wykrycia wirusów, po ich usunięciu, za pomocą oprogramowania antywirusowego, dokonuje sprawdzenia poprawności zainstalowanego oprogramowania i dopiero wtedy dopuszcza innych użytkowników do pracy. W sytuacji utraty danych użytkownicy mogą odzyskać dane ze swoich indywidualnych nośników informacji z kopią zapasową.

W sytuacjach kryzysowych, mogących wystąpić na terenie jednostki użytkownicy, Administrator Systemu Informatycznego oraz Inspektor Ochrony Danych postępują zgodnie z przyjętymi procedurami. Ponadto biorą oni udział w szkoleniach organizowanych w jednostce organizacyjnej.