Zarządzenie nr 55/2023
Wójta Gminy Rakszawa
z dnia 31 marca 2023 r.

w sprawie zmiany zarządzenia nr 100/2019 Wójta Gminy Rakszawa z dnia 18 czerwca 2019 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych, Polityki Bezpieczeństwa Systemów Teleinformatycznych oraz Regulaminu Użytkowania Systemów Teleinformatycznych i Regulaminu Monitoringu.

Na podstawie art. 33 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tekst jednolity Dz.U. z 2022 r., poz. 559 z późn. zm.) oraz art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE 9 Dz. U. UE L 119),

Zarządzam, co następuje:

§ 1

Do Polityki Bezpieczeństwa wskazanej w pkt. 1 § 1 zarządzenia nr 100/2019 Wójta Gminy Rakszawa z dnia 18 czerwca 2019 r.

Dodaje się załączniki:

1. Procedura stosowania zasad Privacy by design i Prywacy by default (zał. nr 1 do zarządzenia);

2. Procedura tworzenia kopii zapasowych plików z danymi osobowymi

obowiązująca w Urzędzie Gminy Rakszawa (zał. nr 2 do zarządzenia).

§ 2

Dodaje się ust. 7 w brzmieniu:

„ 7. Plan ciągłości działania w Urzędzie Gminy Rakszawa" (zał. nr 3 do zarządzenia)

§ 3

Pozostałe części zarządzenia pozostają bez zmian.

§ 4

Zobowiązuję się wszystkich pracowników Urzędu Gminy przetwarzających dane osobowe do przestrzegania zasad zawartych w dokumentach wymienionych w § 1, § 2 oraz w pierwotnym zarządzeniu nr 100/2019 Wójta Gminy Rakszawa z dnia 18 czerwca 2019 r.

§ 5

Nadzór nad realizacją zarządzenia powierza się Sekretarzowi Gminy.

§ 6

Zarządzenie wchodzi w życie z dniem 01.06.2023 roku.

WÓJT GMINY
RAKSZAWA
Jacek Szubart

Zał. nr 1 do zarządzenia nr 55/2023 z dnia 31.03.2023 r.
Wójta Gminy Rakszawa

WÓJT GMINY
RAKSZAWA
Jacek Seubart

.....
Zatwierdzam

Procedura stosowania zasad Privacy by design i Privacy by default

obowiązująca w Urzędzie Gminy Rakszawa

Rozdział 1
Zagadnienia ogólne

1. Niniejsza Procedura ma na celu wdrożenie do Polityki Bezpieczeństwa Danych Osobowych zasadę privacy by design, stosownie do art. 25 ust. 1 Rozporządzenia oraz zasadę privacy by default, stosownie do art. 25 ust. 2 Rozporządzenia.
2. Użyte zwroty i definicje są tożsame ze wskazanymi w Systemie Zarządzania Bezpieczeństwem Informacji obowiązującym w Urzędzie Gminy Rakszawa.
3. Niniejszy dokument dotyczy zarówno procesów już wdrożonych, jak i tych dopiero wdrażanych. Bez znaczenia pozostaje również fakt, czy zmiany wynikają z decyzji Administratora, podpisanej umowy, czy spowodowane są nowelizacją przepisów.
4. Nadrzędnym celem niniejszego dokumentu jest zapobieżenie wystąpienia naruszenia przetwarzania danych osobowych oraz należyta realizacja praw osób fizycznych.
5. Procedura ma zastosowanie do:
   1) zadań własnych
   2) zleconych - o ile zlecający zadanie nie dostarcza oprogramowania, sprzętu.
6. Analizy wykonywane w związku z realizacją niniejszej Procedury są dokumentowane w formie pisemnej.
7. Zmiany w procesie przetwarzania danych osobowych są okolicznością szczególnie obarczającą administratora odpowiedzialnością za zmaterializowanie się zagrożeń związanych z niedopełnieniem powyższych obowiązków.
8. Względy natury organizacyjno - finansowej nie powinny być traktowane jako podstawy do sprzecznego z prawem przetwarzania danych osobowych.
9. Procedura ma na celu zapewnienie, że dane osobowe będą chronione przez cały cykl istnienia określonego procesu, poprzez jego etapy: projektowania, wdrażania, sprawdzania i korekt.
10. Niniejsza procedura powinna być uwzględniona, gdy Administrator dokonuje zmiany w funkcjonującym procesie przetwarzania, która wiąże się ze zmianą zasad lub sposobów przetwarzania danych osobowych, w szczególności związanych z działaniami:
    1) rekrutacyjnymi, działaniami kadrowymi, a zwłaszcza monitorowaniem działalności pracowników.
    2) organizacją urzędu,
    3) promocyjnymi, w szczególności poprzez:
    a) publikowanie na portalach społecznościowych
    b) wykorzystanie wizerunku na banerach i innych akcesoriach reklamowych.
    4) księgowymi,
    5) monitoringiem
    6) procesem uchwałodawczym, który związany jest z potrzebą przetwarzania danych mieszkańców.
    7) wprowadza nową czynność przetwarzania, które wiążą się z przetwarzaniem danych osobowych.

d) ASI stara się usunąć wychwycone słabości i luki w oprogramowaniu również w sytuacji gdy jest to oprogramowanie zewnętrzne.

5) w sytuacji, gdy zakupiony program posiada dodatkowe funkcjonalności, które mogą stanowić niebezpieczeństwo dla prywatności, stara się wyłączyć te funkcje.

38. Wdrożony proces przetwarzana podlega sprawdzaniu przez wyznaczonych pracowników.
39. Po rozpoczęciu czynności przetwarzania IOD sprawdza, czy wymagane jest ponowne przeprowadzenie ocen zagrożeń bezpieczeństwa i wpływu na ochronę danych, które zostały ukończone w fazie wymagań. IOD dokumentuje przeprowadzoną analizę.
40. ASI monitoruje bezpieczeństwo serwerów, punktów końcowych i sieci w celu wykrycia podejrzanej aktywność, która może wykorzystać luki w oprogramowaniu, skutkujące incydentami związanymi z ochroną i bezpieczeństwem danych.
41. W przypadku incydentów teleinformatycznych ASI analizuje, przegląda logi, uzyskuje przegląd tego, co się stało, oraz określa zakres incydentu.
42. W przypadku skargi, która wpłynęła od podmiotu danych, IOD kontaktuje się z ASI (jeśli naruszenie jest związane z działaniem systemów teleinformatycznych) oraz pracownikiem merytorycznym.
43. W pełni wdrożona czynność przetwarzana powinna przechodzić korekty.
44. O wykrytych incydentach mających związek z naruszeniem przetwarzanych danych ASI informuje IOD. Incydentom związanym z bezpieczeństwem należy nadać wysoki priorytet.
45. ASI sprawdza, czy zagrożenia stanowią rzeczywiste naruszenia bezpieczeństwa, czy są fałszywymi alarmami.
46. W przypadku incydentów należy stosować procedury związane z planem ciągłości działania i odtwarzania systemów po awarii.
47. W przypadku stale powtarzających się incydentów, które kwalifikowane są jako naruszenie danych osobowych należy rozważyć zmianę czynności przetwarzania - w zakresie niezbędnym (zmianę oprogramowania, uprawnień, etc.)
48. W ramach cyklicznych szkoleń IOD oraz ASI przeprowadza szkolenie w zakresie reagowania na incydenty obejmujące incydenty teleinformatyczne.

Rozdział 4
Szczególne obowiązki związane z poszczególnymi czynnościami przetwarzania danych

I. Upublicznianie danych w BIP związanych z nowym procesem

1. W sytuacji zamieszczenia danych w BIP administrator uwzględnia przepisy Polityki Retencji jeżeli jest opracowana.
2. Danych osobowych nie zamieszcza się, a upublicznione uchyla, jeżeli nie jest to niezbędne do celów ich przetwarzania oraz jeżeli nie istnieje inny zgodny cel i podstawa prawna zgodna z art. 6 bądź art. 9 RODO.
3. Każde upubliczniane danych poprzez BIP powinno być w razie potrzeby obiektywnie uzasadnione przez administratora danych zgodnie z zasadą rozliczalności.
4. Brak jednak określonych przepisami prawa okresów przetwarzania udostępnionych informacji (zawierających dane osobowe) nie powoduje, że informacje takie można przetwarzać bezterminowo.

II. Podpisanie umowy cywilnoprawnej

1. Jeżeli administrator korzysta z oprogramowania osób trzecich lub oprogramowania dostępnego na rynku, powinien przeprowadzić ocenę ryzyka związanego z produktem

i upewnić się, że jego funkcje, które nie mają podstawy prawnej lub nie są zgodne z zamierzonymi celami przetwarzania, zostaną wyłączone.

2. W sytuacji gdy realizacja czynności przetwarzania związana jest podpisywanie umów cywilnoprawnych, w których zachodzić będzie powierzenie przetwarzania danych osobowych wyznaczony pracownik przed podpisaniem umowy zwraca się do:
   1) IOD w celu uzyskania opinii na temat danych, które są niezbędne dla zrealizowania zadania i wymagają powierzenia przetwarzania.
   2) ASI w celu uzyskania opinii o wymaganych funkcjonalnościach- informuje o kosztach.
3. W sytuacji gdy zachodzi powierzenie przetwarzania danych osobowych administrator określa:
   1) wdrożenie odpowiednich środków technicznych i organizacyjnych, takich jak np. pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych.
   2) w momencie podpisywania umowy głównej - administrator wskaże podstawowe warunki dotyczące zabezpieczania danych osobowych, które następnie zostaną doprecyzowane w umowie powierzenia. Powyższe dotyczy w szczególności zagadnień przekazywania danych poza obszar EOG.
   3) W przypadku migracji danych osobowych należy włączyć podmiot przetwarzający w proces. Administrator zwraca uwagę na dostarczenie podmiotowi przetwarzającemu pełnych informacji o podejmowanych czynnościach i oczekiwanych rezultatach, administrator wymaga od podmiotu przetwarzającego zachowania wszelkich zasad dot. ODO

III. Udostępnianie danych

1. Pracownicy są zobligowania do sprawdzania, a w razie wątpliwości konsultowania z IOD udostępniania danych innym podmiotom. W szczególności dotyczy to innych organów administracji, komorników, poczt polskiej, pod względem legalizmu.

WÓJT GMINY
RAKSZAWA
Jacek Szubart

.....

Zatwierdzam

Zał. nr 2 do Zarządzenia nr 55/2023
z dnia 31.03.2023 r. Wójta Gminy Rakszawa

WÓJT GMINY
RAKSZAWA
Jacek Szubart

.....

Zatwierdzam

Procedura tworzenia kopii zapasowych plików z danymi osobowymi

Obowiązująca w Urzędzie Gminy Rakszawa

I. Zasady ogólne

1. W celu zapewnienia zgodności z przepisami o ochronie danych osobowych, w tym zapewnienia należytej staranności przy zapewnieniu ochrony danych osobowych, wprowadza się niniejszą Procedurę tworzenia kopii zapasowych plików z danymi osobowymi.
2. Procedura obowiązuje każdego użytkownika upoważnionego do przetwarzania danych osobowych w formie elektronicznej.
3. Zasady określone poniżej odnoszą się do plików elektronicznych tworzonych przez użytkownika na jego urządzeniu komputerowym.
4. Wsparcia technicznego związanego z tworzeniem kopii plików udziela informatyk.

II. Zasady tworzenia kopii zapasowych plików

1. Kopia zapasowa plików powinna być wykonywana raz na tydzień.
2. Dla plików z istotnymi danymi należy tworzyć kopię przy każdej istotnej zmianie zawartości.
3. Wykonanie kopii zapasowej wybranych plików użytkownik realizuje poprzez skopiowanie plików do wyznaczonego przez administratora zasobu sieciowego lub na zaszyfrowany udostępniony przez administratora zewnętrzny nośnik informacji .
4. Po wykonaniu kopii użytkownik jest zobowiązany sprawdzić, czy pliki skopiowały się prawidłowo, np. czy nie skopiowały się jedynie ich skróty albo pliki nie są uszkodzone.
5. Jeśli zewnętrzny nośnik informacji nie jest zabezpieczony kryptograficznie, należy zamiast kopiowania wskazanego w punkcie 3 zaznaczone pliki dodać do skompresowanego archiwum (np. Programem 7-zip), które zostanie zabezpieczone ustalonym przez użytkownika, silnym hasłem dostępu. Dopiero zabezpieczone hasłem archiwum należy przekopiować.
6. Po skopiowaniu na udostępniony przez administratora zasób sieciowy lub dysk zewnętrzny skompresowanego archiwum, użytkownik upewnia się, czy plik skopiował się prawidłowo oraz czy jego otwarcie wymaga podania ustalonego hasła.
7. Należy przechowywać dwie starsze kopie zapasowe plików. Jeżeli użytkownik dodał trzecią z kolei kopię zapasową do zewnętrznego miejsca przechowywania, to po upewnieniu się, że jest ona poprawna, usuwa bezpowrotnie najstarszą kopię zapasową.

8. Utworzenie kopii zapasowej można zrealizować także globalnie dla wszystkich plików teleelektronicznych na urządzeniu użytkownika z wykorzystaniem narzędzi systemowych lub udostępnionych przez administratora innych narzędzi. Zasady tworzenia i przechowywania kopii zapasowych pozostają takie same w przypadku skorzystania przez użytkownika z tej funkcji.

9. Użytkownik jest zobligowany do przestrzegania niniejszej procedury.

10. Nieprzestrzeganie niniejszej procedury stanowi ryzyko dla rozliczalności przetwarzanych przez użytkownika danych osobowych i może zostać uznane za naruszenie obowiązków pracowniczych lub postanowień umowy ze zleceniobiorcą.

WÓJT GMINY
RAKSZAWA
Jacek Szubart

.....

Zatwierdzam

Zał. nr 3 do Zarządzenia nr 55/2023
z dnia 31.03.2023 r. Wójta Gminy Rakszawa

URZĄD GMINY RAKSZAWA

PLAN CIĄGŁOŚCI DZIAŁANIA

DO UŻYTKU SŁUŻBOWEGO

ZATWIERDZAM

WÓJT GMINY RAKSZAWA

JACEK SZUBART

PLAN CIĄGŁOŚCI DZIAŁANIA W URZĘDZIE GMINY RAKSZAWA

Spis treści

ROZDZIAŁ I

POSTANOWIENIA OGÓLNE

1. Wstęp

Niniejszy dokument określa wymagania w zakresie wdrażania i realizacji działań, zapewniających ciągłość przetwarzania informacji, w szczególności danych osobowych, przetwarzanych przez Administratora.

Działania określone w niniejszej Polityce są adekwatne do konsekwencji przerwania ciągłości przetwarzania informacji, w tym danych osobowych oraz kosztów wdrożenia i utrzymania właściwych mechanizmów zabezpieczających, z uwzględnieniem mechanizmów o charakterze organizacyjnym i technicznym. Plan ciągłości działania jest integralną częścią SZBI (Systemu Zarządzania Bezpieczeństwem Informacji obowiązującym w Urzędzie Gminy Rakszawa). Ma za zadanie zabezpieczenia pracy podczas normalnej działalności Urzędu oraz umożliwienie funkcjonowania w przypadku wystąpienia zagrożenia lub awarii (sytuacja kryzysowa) , na wszystkich poziomach organizacyjnych.

2. Cel i zakres

a. U Administratora podejmowane są działania umożliwiające zapewnienie dostępności informacji w zakresie niezbędnym do efektywnej realizacji jego zadań.

b. Podejmowane działania mają na celu:

- zminimalizowanie ryzyka wystąpienia sytuacji, w której nastąpi utrata dostępności informacji;
- umożliwienie realizacji zadań w przypadku utraty dostępności infrastruktury niezbędnej do przetwarzania informacji, w szczególności infrastruktury teleinformatycznej.

c. Szczegółowe działania, gwarantujące osiągnięcie celu, o którym mowa w punkcie 2, b, zostały opisane w Rozdziale II niniejszej Polityki.

d. Podstawą do podjęcia działań zapewniających ciągłość przetwarzania informacji przez Administratora jest proces szacowania ryzyka utraty poufności, dostępności i integralności przetwarzanych informacji. Proces szacowania ryzyka realizowany jest zgodnie z zasadami opisanymi w dokumencie „Analiza Ryzyka". Podejmowane działania są adekwatne do wyników szacowania ryzyka i są ekonomicznie uzasadnione.

e. W celu przygotowania pracowników Administratora do reagowania na zdarzenia powodujące utratę dostępności informacji, w tym danych osobowych przeprowadzane są okresowe testy oraz przeglądy prawidłowej realizacji zadań związanych z zapewnieniem ciągłości działania.

f. Częstotliwość przeprowadzania testów została wskazana w Rozdziale III niniejszego dokumentu. Na podstawie wyników testów i przeglądów podejmowane są niezbędne działania korygujące.

g. Wszelkie działania podejmowane w celu zapewnienia ciągłości przetwarzania informacji są zgodne z wymaganiami zawartymi w przepisach Ogólnego Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, RODO), w szczególności z art. 32 ust. 1 tego rozporządzenia.

3. Słownik pojęć

Termin	Znaczenie
Administrator	Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych, który na podstawie art. 28 – Ogólnego Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, powierzył do Administratora przetwarzanie danych w drodze umowy zawartej na piśmie, w zakresie i celu przewidzianym w umowie;
Informatyk/ ASI	Osoba odpowiedzialna za prawidłowe funkcjonowanie powierzonego jej do administrowania fragmentu systemu informatycznego, określenie to obejmuje zarówno administratorów systemów operacyjnych jak i aplikacji użytkowych. Osoba upoważniona do ustalania identyfikatorów użytkowników i pierwszych haseł do dostępu do systemach informatycznych, które obsługują oraz do nadzoru i kontroli przetwarzania danych w zakresie określonym przepisami o ochronie danych osobowych oraz regulacjami wewnętrznymi Administratora
Informacje	Wszelkie informacje, w szczególności dane osobowe, w formie elektronicznej - w postaci plików lub ustrukturyzowanej bazy danych, przetwarzane przez pracowników Administratora przy użyciu urządzeń i systemów informatycznych, aplikacji, programów i desktopowych narzędzi programowych.

Infrastruktura teleinformatyczna	Systemy teleinformatyczne wraz z aktywnymi i pasywnymi elementami sieci teleinformatycznej.
Pracownik	Osoba fizyczna realizująca zadania na rzecz Administratora na podstawie umowy o pracę lub umowy cywilnoprawnej, osoba odbywająca staż lub praktyki u Administratora.
Procedura awaryjna	Procedura opisująca schemat postępowania w sytuacji wystąpienia awarii, która może mieć wpływ na zachowanie ciągłości działania Administrator, spowodowane brakiem możliwości dostępu do informacji i ich przetwarzania.
Inspektor Ochrony Danych	osoba wyznaczona przez Administratora odpowiedziaina za bezpieczeństwo informacji, w szczególności danych osobowych przetwarzanych przez Administratora. Upoważniona do kontroli przetwarzania danych w zakresie określonym przepisami o ochronie danych osobowych oraz regulacjami wewnętrznymi Administratora
Symulacja	Test polegający na realizacji przez pracowników zadań w sposób taki jak w sytuacji awaryjnej, przy czym rzeczywista awaria nie miała miejsca.
System informatyczny	Zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych, w stosunku do których Administratorem lub Podmiotem przetwarzającym jest Administrator.
Środowisko produkcyjne	Sieć, urządzenia i systemy teleinformatyczne wykorzystywane przez pracowników Administratora do realizacji obowiązków służbowych.
Środowisko testowe	Sieć, urządzenia i systemy teleinformatyczne wykorzystywane do przeprowadzania testów. Środowisko testowe umożliwia uniknięcie przeprowadzania testów bezpośrednio w środowisku produkcyjnym. Ze względu na wiarygodność testów powinno technicznie odpowiadać środowisku produkcyjnemu.

ROZDZIAŁ II

ZAPEWNIENIE CIĄGŁOŚCI PRZETWARZANIA INFORMACJI

1. **Działania podejmowane w celu zapewnienia ciągłości przetwarzania informacji**
   a. Działania mające na celu minimalizację ryzyka przerwy w dostępności infrastruktury teleinformatycznej oraz minimalizację czasu przywrócenia dostępności infrastruktury obejmują w szczególności:
   - ✓ zapewnienie zapasowych komponentów technicznych umożliwiających ciągłość przetwarzania informacji w przypadku awarii komponentów podstawowych;
   - ✓ wykonywanie kopii zapasowych informacji, umożliwiających ich odtworzenie w przypadku awarii technicznej lub nieautoryzowanego usunięcia danych;
   - ✓ zawarcie umów serwisowych umożliwiających przywrócenie funkcjonowania komponentów technicznych uszkodzonych w wyniku awarii;
   - ✓ zapewnienie zabezpieczeń środowiskowych obejmujących:
     - systemy zasilania awaryjnego;
     - systemy przeciwprzepięciowe;
     - systemy przeciwpożarowe i gaśnicze;

   b. Dla systemów teleinformatycznych stosuje się procedury awaryjne, które obejmują w szczególności:
   - ✓ procedurę postępowania w przypadku niedostępności systemów informatycznych;
   - ✓ procedurę odtwarzania zasobów z kopii zapasowych.

   c. Za podjęcie działań w zakresie zapewnienia ciągłości funkcjonowania infrastruktury teleinformatycznej oraz zapewnienia zabezpieczeń środowiskowych i ich poprawnych działaniem odpowiada Informatyk.

   d. Administrator sprawuje nadzór w zakresie podejmowanych działań przez Informatyka.

2. Organizacja zarządzania ciągłością przetwarzania informacji

1. Działania mające na celu minimalizację ryzyka utraty dostępności pracowników niezbędnych do realizacji zadań obejmują w szczególności:
    - zapewnienie zastępstw;
    - unikanie sytuacji, w której kompetencje do wykonania danego zadania posiada wyłącznie jeden pracownik Administratora.;
    - unikanie ryzyka związanego z niedostępnością wszystkich pracowników Administratora posiadających kompetencje niezbędne do realizacji zadań w ramach bieżącej pracy, w szczególności poprzez planowanie urlopów, szkoleń, wyjazdów służbowych, w sposób zapewniający dostępność wystarczającej liczby pracowników do realizacji tych zadań;
    - zarządzanie uprawnieniami do dostępu do systemów teleinformatycznych w sposób umożliwiający realizację zastępstw;
    - zapewnienie możliwości zastąpienia podmiotu świadczącego usługi na rzecz Administratora innym podmiotem, w sytuacji braku możliwości świadczenia wymaganych usług lub świadczenia usług na poziomie nieakceptowalnym przez Administratora.
2. Działania zapewniające przywrócenie zdolności realizacji działalności statutowej

	Funkcja	Opis działań	Potrzebne zasoby / odpowiedzialni
1)	Zweryfikować zasadność zgłoszenia od użytkownika	Sprawdzić, czy zgłoszenie dotyczy zdarzenia spowodowanego awarią systemu informatycznego.	Zapewnić: - dostęp do infrastruktury informatycznej na stanowisku, skąd pochodzi zgłoszenie. Odpowiedzialny: IOD
2)	Ustalić źródła awarii	Ustalić, co jest przyczyną awarii: - przerwa w zasilaniu prądem, - brak połączenia z siecią Internet, - wadliwe działanie sprzętu, - wadliwe działanie aplikacji, - wadliwe działanie systemu, na którym uruchomiona jest aplikacja.	Zapewnić: - dostęp do serwerowni oraz do sprzętu, który uległ awarii, - kontakt z osobą, która może w porze nocnej pobrać klucze od Urzędu, - w przypadku zablokowania zamka wezwać ślusarza, - w przypadku awarii zasilania elektrycznego wezwać elektryka. Odpowiedzialny: Administrator
3)	Określić skalę awarii	Ustalić, czy awaria powoduje zatrzymanie pracy: -jednego	Zapewnić: - kontakt z kluczowymi pracownikami referatów, lista z numerami telefonów.

		pomieszczenia pracy lub referatu (od 1 do 6 osób) - kilku referatów (od 7 do 25 osób) - całego budynku urzędu - wszystkich budynków urzędu	Odpowiedzialny: IOD
4)	Ustalić czy wznawianie usługi może odbywać się w dotychczasowej lokalizacji	Działanie ma na celu zweryfikowanie, czy wznawiane usługi uruchamiane będą w dotychczasowej lokalizacji, czy w lokalizacjach alternatywnych.	Zapewnić: - możliwość uruchomienia dowolnych usług w lokalizacji: - infrastrukturę sieciową, zasilanie prądem Odpowiedzialny: Informatyk
5)	Zakupić niezbędne elementy wyposażenia, dokonać naprawy (wymiany) urządzeń uruchomić aplikację	W przypadku braku możliwości zakupu należy znaleźć rozwiązanie alternatywne (np. zdecydować o przeniesieniu aplikacji na stałe na inny serwer)	- zgłosić zapotrzebowanie do Skarbnika UG na środki na zakup elementów niezbędnych do ponownego uruchomienia systemu. Odpowiedzialny: Informatyk
6)	Zweryfikować możliwość przeniesienia aplikacji na inny serwer	Sprawdzić, czy aplikacja może być uruchomiona na którymś z działających poprawnie serwerów.	Odpowiedzialny: Informatyk
7)	Przygotować serwer zastępczy,	Jako serwer zastępczy można wykorzystać np. Komputer typu desktop, który należy odpowiednio skonfigurować. Po uruchomieniu aplikacji na serwerze zastępczym należy przetestować jej działanie.	Zapewnić: - maszynę dowolnego typu, która w podstawowym zakresie pozwoli na uruchomienie podstawowych usług. Odpowiedzialny: Informatyk
8)	Podjąć decyzję o terminie odtworzenia maszyny	W razie konieczności należy skontaktować się z właściwymi kierownikami komórek organizacyjnych.	Zapewnić: - kontakt z kluczowymi pracownikami referatów, lista z numerami telefonów. Odpowiedzialny: IOD
9)	Przywrócić funkcjonowanie aplikacji / systemu	Spróbować usunąć przyczynę nieprawidłowego działania. W razie konieczności należy odtworzyć aplikację korzystając z kopii zapasowych.	Zapewnić: - dostęp do najbardziej aktualnej wersji aplikacji, - dostęp do aktualnej bazy danych. Odpowiedzialny: Informatyk
10)	Sprawdzenie aplikacji / systemu	Po przeniesieniu / uruchomieniu należy zweryfikować prawidłowe funkcjonowanie **aplikacji / systemów** zainstalowanych na serwerze.	Odpowiedzialny: Informatyk
11)	Uruchomienie usługi w systemie informatycznym Urzędu	Po uruchomieniu usługi należy powiadomić właściwych kierowników o tym fakcie.	Zapewnić: - kontakt z kluczowymi pracownikami referatów, lista z numerami telefonów. Odpowiedzialny: IOD lub Informatyk

ROZDZIAŁ III

TESTOWANIE

a. Testowanie skuteczności procedur awaryjnych

- W celu zapewnienia skuteczności działań podejmowanych w sytuacjach awaryjnych, zgodnie z wdrożonymi procedurami awaryjnymi, o których mowa w Rozdziale II, pkt 1, b, muszą one podlegać testowaniu.
- Testy przeprowadzane są okresowo, nie rzadziej niż raz na dwa lata dla każdej procedury, zgodnie z założonym harmonogramem.
- Testy mają na celu:

✓ sprawdzenie technicznych możliwości przywrócenia poprawnego działania systemów teleinformatycznych po awarii;

✓ przygotowanie pracowników Administratora odpowiedzialnych z realizację procedur awaryjnych do praktycznej ich realizacji.

- Testy przeprowadzane są w środowisku testowym, w sposób i w terminach minimalizujących ryzyko negatywnego wpływu na działanie i realizację zadań przez innych pracowników Administratora.
- Testy przeprowadzane są w oparciu o symulację sytuacji awaryjnych.
- Zakres testów obejmuje w szczególności:

1) procedury awaryjne podlegające testom,
2) urządzenia techniczne podlegające testom,
3) sposób przeprowadzenia testu,
4) termin przeprowadzenia testu,
5) osoby biorące udział w testach,
6) zasoby niezbędne do przeprowadzenia testów.

- Za określenie szczegółowego zakresu oraz harmonogramu przeprowadzenie testów, a także dokonanie oceny ich efektywności odpowiada Informatyk.
- W ramach przeprowadzania testów weryfikuje się następujące parametry:

1) czas odtwarzania zasobów z kopii zapasowych;
2) poprawność działania zabezpieczeń środowiskowych,
3) czasy reakcji służb serwisowych i innych podmiotów zewnętrznych.

- Wyniki testów podlegają dokumentowaniu i analizie. Dokumentacja zawiera opis realizowanych zadań, czas potrzebny na ich realizację, osoby realizujące zadania, wynik realizacji zadań oraz uwagi.
- Wyniki testów stanowią podstawę do:
  i. aktualizacji procedur awaryjnych;
  ii. podjęcia działań w celu przygotowania pracowników do realizacji procedur awaryjnych, w szczególności poprzez działania szkoleniowe;
  iii. optymalizacji infrastruktury teleinformatycznej, w celu umożliwienia efektywnej realizacji działań w wypadku sytuacji awaryjnej.

ROZDZIAŁ IV

PRZEGLĄDY, AKTUALIZACJA I DYSTRYBUCJA DOKUMENTACJI

a. Przeglądy i aktualizacja

- Polityka Ciągłości Działania i towarzyszące jej procedury podlegają przeglądom i aktualizacji.
- Za dokonywanie przeglądów i aktualizację niniejszego dokumentu odpowiedzialni są Inspektor Ochrony Danych i Informatyk.
- Przeglądy przeprowadzane są:
  i. okresowo, nie rzadziej niż raz w roku;
  ii. w przypadku wystąpienia zdarzeń, które mogą wpłynąć na aktualność procedury.
- Przegląd procedur awaryjnych jest inicjowany w szczególności w przypadku wystąpienia następujących zdarzeń:
  i. zmiany struktury organizacyjnej lub zmiany kompetencji komórki odpowiedzialnej za realizację procedury awaryjnej;
  ii. zmiany regulacji prawnych określających sposób zabezpieczenia informacji;
  iii. zmiany sposobu wykonywania zadań przez komórkę organizacyjną, mających wpływ na realizację procedury awaryjnej;
  iv. wprowadzenia nowych lub modyfikacja istniejących systemów teleinformatycznych w zakresie wpływającym na możliwości przywrócenia systemu po awarii;
  v. zmiany w zakresie wsparcia systemów teleinformatycznych przez producentów lub podmioty świadczące usługi serwisowe, objęte procedurami awaryjnymi;
  vi. wdrożenia nowych lub zmiana istniejących zabezpieczeń technicznych, w tym środowiskowych, mających wpływ na realizację procedur awaryjnych.
- Podczas oceny poprawności procedury w ramach przeprowadzanego przeglądu brane są w szczególności pod uwagę:
  i. wymagania prawne określające postępowanie z informacjami;
  ii. struktura organizacyjna Administratora i zakres kompetencji;

iii. zmiany dotyczące infrastruktury teleinformatycznej objętej procedurami awaryjnymi,

iv. zmiany dotyczące zabezpieczeń technicznych, w tym środowiskowych, mających wpływ na realizację procedur awaryjnych.

- W wyniku przeprowadzonego przeglądu podejmowana jest decyzja, wskazująca na:

i. brak konieczności wprowadzenia zmian w procedurach awaryjnych;

ii. konieczność monitorowania procedur awaryjnych, z uwagi na możliwość wystąpienia potrzeby wprowadzenia zmian;

iii. konieczność modyfikacji procedury awaryjnej;

iv. konieczność wprowadzenia nowej procedury awaryjnej.

b. Dystrybucja dokumentacji

- Polityka Ciągłości Działania powinna być udostępniona wszystkim pracownikom odpowiedzialnym za realizację określonych w niej zadań.
- Pracownicy Administratora realizujący czynności określone w procedurach awaryjnych, są zobowiązani do zapoznania się z ich treścią.
- Procedury awaryjne powinny być stale dostępne pracownikom realizującym określone w nich zadania.

ROZDZIAŁ V

POSTĘPOWANIE W PRZYPADKU NARUSZENIA I PODEJRZENIA NARUSZENIA ZABEZPIECZENIA SYSTEMU OCHRONY DANYCH OSOBOWYCH

5.1. **Naruszenie ochrony danych może być skutkiem:**

a) Szkodliwego wpływu środowiska na system przetwarzania danych;

b) Zewnętrznym zdarzeń losowych;

c) Zamierzonych lub niezamierzonych czynności użytkowników systemów przetwarzania danych;

d) Nieuprawnionych działań osób nieupoważnionych do dostępu do danych.

5.2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane:

a) Niewłaściwe parametry środowiska takie jak temperatura, wilgotność dla pomieszczeń, w którym przetwarzane są dane;

b) Sytuacja klęski żywiołowej (pożar, powódź, huragan);

c) Naruszenie lub próby naruszenia integralności systemu do przetwarzania danych (np. stan urządzenia wchodzącego w skład systemu wskazuje na zakłócenie jego pracy – brak dostępu do sieci czy awaria komputera, stan aplikacji wskazuje na obecność wirusa komputerowego);

d) Naruszenie lub próby naruszenia integralności danych rozumiane jako wszelkie modyfikacje (dodanie, zmiana, usunięcie), zniszczenia lub próby ich dokonania przez osoby nieuprawnione lub uprawnione działające w złej wierze lub jako błąd osoby uprawnionej (np. zmianę zawartości danych, utratę całości lub części danych);

e) Wykorzystanie nielegalnych aplikacji lub elementów nielegalnego oprogramowania;

f) Istotne zakłócenie toku pracy procedur zapewniających ochronę przetwarzania danych (np. brak wprowadzenia wymaganego dokumentu lub potwierdzenia takiej operacji), pojawienie się odpowiedniego komunikatu alarmowego z tych procedur (np. utrata dostępu do danych) ;

g) Otrzymanie informacji o naruszeniu danych osobowych (np. sygn. o nieautoryzowanym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu, stan przeglądanych danych wskazuje na ingerencję w strukturę zbioru);

h) Niedopełnienie obowiązku ochrony danych przez umożliwienie dostępu do danych (np. pozostawienie kopii danych, nie zablokowanie dostępu do systemu, brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi przebywającymi w pomieszczeniach gdzie przetwarza się dane);

i) Nieuprawniony dostęp lub próba dostępu do pomieszczeń gdzie przetwarza się dane;

j) Nieuprawniony dostęp lub próba dostępu do systemu przetwarzania danych (np. nieuprawniona praca na koncie użytkownika, istnienie nieautoryzowanych kont dostępu do danych- pojawienie się nowych lub nie zablokowanie czy usunięcie starych);

k) Ujawnienie indywidulanych haseł dostępu do danych;

l) Wykonanie nieuprawnionych kopii danych;

m) Zmiana lub usunięcie zapisanych danych na kopiach bezpieczeństwa lub archiwalnych;

n) Brak nośnika zawierającego dane (np. zaginięcie wydruku, kopii bezpieczeństwa, dysku itp.)

o) Niewłaściwe niszczenie nośników z danymi pozwalające na ich odczyt;

p) Inne sytuacje wskazujące lub potwierdzające naruszenia bezpieczeństwa danych.

5.3. W przypadku stwierdzenia naruszenia danych lub zaistnienia okoliczności wskazujących na naruszenie systemu ochrony danych osobowych, osoba zatrudniona przy ich przetwarzaniu bezzwłocznie powiadamia o tym fakcie Administratora lub upoważnioną przez niego osobę (Informatyka lub/oraz IOD)

5.4. Określony obowiązek dotyczy również Procesora oraz jego pracowników pracujących na określonym zbiorze danych.

5.5. Postanowienia pkt. 5.1 i 5.2 mają odpowiednie zastosowanie w przypadku naruszenia bądź podejrzenia naruszenia ochrony danych osobowych.

5.6. W przypadku awarii systemu informatycznego spowodowanej błędem programu lub użytkownika odpowiednie zastosowanie mają postanowienia Rozdziału VI niniejszej polityki.

5.7. W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób stosuje się zasady postepowania określone w Instrukcji Bezpieczeństwa Pożarowego, obowiązującej u Administratora budynku.

5.8. Do czasu przybycia Administratora lub upoważnionej przez niego osoby, użytkownik systemu:

- Powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcia śladów bądź dowodów;
- Zabezpiecza elementy systemu informatycznego przed dostępem osób trzecich;
- Podejmuje, stosownie do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

5.9. Administrator lub osoba przez niego upoważniona, po przybyciu na miejsce:

- Ocenia zaistniałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane, stan urządzeń i zbioru danych oraz identyfikuje wielkość negatywnych następstw incydentu,
- Wysłuchuje relacji osoby zatrudnionej przy przetwarzaniu danych, która dokonała powiadomienia,
- Podejmuje decyzję o toku dalszego postepowania, stosownie do zakresu naruszenia lub podejrzenia naruszenia ochrony danych osobowych (skalę incydentu oraz dokładne postepowanie w sytuacji zagrożenia utraty danych określa „ Procedura zarzadzania incydentami" obowiązująca w Urzędzie Gminy Rakszawa").
- Sporządza z przebiegu zdarzenia raport, w którym zamieszcza w szczególności informacje o :

I. Godzinie pojawiania się w pomieszczeniach, w którym przetwarzane są dane,
II. Sytuacji, jaką zastał,
III. Dacie i godzinie powiadomienia,
IV. Podjętych działaniach i ich uzasadnieniu,
V. Kopia raportu przekazana jest bezzwłocznie Administratorowi w przypadku, gdy raport sporządzony został przez osobę upoważnioną przez Administratora.

- Administrator lub osoby przez niego upoważnione podejmują kroki zmierzające do likwidacji naruszeń zabezpieczeń systemu i zapobieżenia wystąpieniu ich w przyszłości w tym celu:

- w miarę możliwości przywraca stan zgodny zasadami zabezpieczenia systemu,
- o ile taka potrzeba zachodzi, postuluje wprowadzenie nowych form zabezpieczenia sytemu,

a w razie ich wprowadzenia zaznajamia z nimi osoby zatrudnione przy przetwarzaniu danych.

- W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej u Administratora/ Procesora dyscypliny pracy, dokonuje wyjaśnienia wszystkich okoliczności incydentu i o podjęcie stosownych działań wobec sprawcy/ sprawców.
- Użytkownik, w sytuacji, o której mowa, może kontynuować pracę dopiero po otrzymaniu pozwolenia od Administratora.
- W przypadku zaginięcia komputera przenośnego lub nośników magnetycznych, na których zgromadzone były dane osobowe, użytkownik posługujący się komputerem przenośnym niezwłocznie powiadamia Administratora lub upoważnioną przez niego osobę, a ponadto w przypadku kradzieży najbliższą jednostkę policji.
- W sytuacji, o której mowa powyżej Administrator lub upoważniona przez niego osoba podejmuje niezbędne kroki do wyjaśnienia okoliczności zdarzenia, sporządza protokół z zajścia, który powinna podpisać także osoba, której skradziono lub, której zaginął sprzęt.
- W przypadku kradzieży komputera przenośnego razem z nośnikiem magnetycznym Administrator lub upoważniona przez niego osoba podejmuje działania zmierzające do odzyskania utraconych danych oraz nadzoruje proces przebiegu wyjaśniania sprawy.
- Osoba zatrudniona przy przetwarzaniu danych osobowych za naruszenie obowiązków wynikających z niniejszego Planu i przepisów o ochronie danych osobowych ponosi odpowiedzialność przewidziana w Kodeksie Pracy oraz wynikającą z Rozporządzenia.

ROZDZIAŁ VI

PROCES POSTĘPOWANIA W PRZYPADKU USZKODZENIA ZBIORU DANYCH

6.1 Odtworzeniem danych zajmuje się Administrator we współpracy z Administratorem Systemu Informatycznego.

6.2 Pierwszym podejmowanym krokiem jest zawieszenie uprawnień użytkowników i zakomunikowanie o czasowym zablokowaniu dostępu do zbioru danych.

6.3 Później ustalane jest źródło awarii i obszar uszkodzeń.

6.4 Następnie podejmowane są działania w celu usunięcia awarii i próby naprawy zbioru danych.

6.5 Kolejnym krokiem jest sprawdzenie poprawności i spójności zbioru danych.

6.6 Finalnie system poddawany jest procedurze testowania i dopiero po stwierdzeniu poprawności jego działania następuje przywrócenie uprawnień dla użytkowników i poinformowanie ich o możliwości bezpiecznego przetwarzania danych.

6.7 W przypadku stwierdzenia niespójności bądź utraty danych następuje ich odzysk z kopii bezpieczeństwa /zapasowych/.

6.8 Administrator Systemu Informatycznego sporządza raport z przebiegu i wyniku odtworzenia danych, który przekazuje Administratorowi.

ROZDZIAŁ VII

PROCES POSTĘPOWANIA W PRZYPADKU AWARII SERWERA (PROCEDURA AWARYJNA)

7.1 W przypadku awarii serwera powoływany jest komitet kryzysowy w składzie

a. Administrator Systemu Informatycznego

b. Administrator

7.2 Pierwszym podejmowanym krokiem jest zawieszenie uprawnień użytkowników i zakomunikowanie o czasowym zablokowaniu dostępu do serwera/systemu.

7.3 Później ustalane jest źródło awarii i obszar uszkodzeń.

7.4 Następnie podejmowane są działania w celu usunięcia awarii i próby naprawy serwera/systemu.

7.5 Kolejnym krokiem jest sprawdzanie poprawności i spójności systemów i zbiorów danych.

7.6 Finalnie serwer/system oraz zbiory danych poddawane są procedurze testowania i dopiero po stwierdzeniu poprawności jego działania następuje przywrócenie uprawnień dla użytkowników i poinformowanie ich o możliwości bezpiecznego przetwarzania danych.

7.7 W przypadku nieudanej próby naprawy serwera następuje bezzwłoczne przejście na serwer zapasowy.

7.8 Uszkodzony serwer podlega bezzwłocznej naprawie w siedzibie Administratora.

7.9 Administrator Systemu Informatycznego sporządza raport, który przekazuje Administratorowi.

7.10 Zasady postępowania w stosunku do osób, które dopuściły się zaniedbań związanych z zapewnieniem bezpieczeństwa przetwarzania danych.

7.11 W sytuacji gdy zagrożenie bezpieczeństwa zaistniało w wyniku działań osoby zatrudnionej przy przetwarzaniu danych, Administrator występuje o pozbawienie praw dostępu do danych osobowych dla tej osoby.

7.12 Identyfikator osoby, która utraciła uprawnienia dostępu do danych jest niezwłocznie wyrejestrowany z systemu informatycznego. Hasło takiej osoby jest unieważniane, jak również podejmowane są wszelkie czynności, których celem jest zapobieżenie dalszemu dostępowi tej osoby do danych.

7.13 Jeżeli zachodzi podejrzenie, że naruszenie lub powstałe niebezpieczeństwo naruszenia ochrony danych jest wynikiem czynu karalnego, Administrator zawiadamia o powyższych okolicznościach właściwy organ ścigania.

7.14 Jeżeli okoliczności faktycznie wskazują na konieczność natychmiastowej interwencji organów ścigania, zawiadomienia takiego dokonać może osoba zatrudniona przy przetwarzaniu danych (operator danych), o czym niezwłocznie powiadomi Administratora.

7.15 Serwery chronione są przed awarią zasilania poprzez zasilacze awaryjne, które zapewniają bieżącą kontrolę i korektę parametrów zasilania, jak również w wypadku całkowitego zaniku napięcia zapewniają utrzymanie jego poziomu do czasu bezpiecznego wyłączenia serwerów.

7.16 Sprzęt komputerowy podłączony jest do wydzielonego obwodu instalacji elektrycznej. Niedopuszczalne jest podłączanie do tego obwodu żadnych innych urządzeń.

ROZDZIAŁ VIII

POSTANOWIENIA KOŃCOWE

8.1 Osoba zatrudniona przy przetwarzaniu danych osobowych podlega obowiązkowemu szkoleniu z zakresu przepisów o ochronie danych osobowych.

8.2 Okresowym szkoleniom – stosownie do potrzeb wynikających ze zmian w systemie zabezpieczenia danych osobowych /zastosowanie nowych sposobów, środków i form ochrony danych osobowych /oraz w związku ze zmianą przepisów o ochronie danych osobowych – podlegają wszyscy użytkownicy.

8.3 Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych każda osoba powinna być zapoznana z Politykami Ochrony Danych.

8.4 Pracownik składa stosowne pisemne oświadczenie o zapoznaniu się z obowiązującymi Politykami Ochrony Danych, którego wzór zawiera do Polityki Ochrony Danych Osobowych. Oświadczenia przechowywane są w aktach osobowych pracowniczych oraz u Inspektora Danych Osobowych.

8.5 Polityka ciągłości działania, jako integralna część Polityki Ochrony Danych Osobowych jest dokumentem wewnętrznym Administratora i nie może być udostępniana osobom postronnym w żadnej formie.

8.6 W sprawach nieuregulowanych w Politykach mają zastosowanie w/w przepisy o ochronie danych osobowych oraz przepisów wykonawczych wydanych na ich podstawie.