ZARZĄDZENIE Nr 26/2019
Wójta Gminy Szczytniki
z dnia 31 lipca 2019 r.

w sprawie: ochrony danych osobowych w Urzędzie Gminy w Szczytnikach.

Na podstawie art. 31 i art. 33 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tj. Dz. U. z 2018 r. poz. 994) oraz art. 24 ust. 2 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1), **z a r z ą d z a m, co następuje:**

§ 1. 1. Na użytek niniejszego zarządzenia:

1) **„RODO"** oznacza Rozporządzenie 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1);
2) **„Urząd"** oznacza Urząd Gminy w Szczytnikach;
3) **„Administrator Danych Osobowych"** oznacza Wójta Gminy Szczytniki z siedzibą 62-865 Szczytniki 139;
4) **„Zarządzenie ODO"** oznacza niniejsze zarządzenie Wójta Gminy Szczytniki;
5) Zastosowano definicje pojęć zgodnie z definicjami w art. 4 RODO;
6) **„Kierownicy komórek organizacyjnych Urzędu"** oznaczają odpowiednio kierowników referatów oraz samodzielne stanowiska pracy.
7) **„System Informatyczny Urzędu Gminy w Szczytnikach"** oznacza system informatyczny funkcjonujący w Urzędzie, na który składają się: systemy operacyjne, oprogramowanie, sprzęt komputerowy oraz teleinformatyczny (w tym sieciowy), wszelkie nośniki cyfrowe, systemy poczty elektronicznej, strony internetowe (w tym Biuletyn Informacji Publicznej), przetwarzane dane oraz procedury i polityki bezpieczeństwa dotyczące ich funkcjonowania.

§ 2. 1. Wszyscy pracownicy Urzędu zobligowani są do ochrony danych osobowych zgodnie z obowiązującym prawem Unii Europejskiej, prawem krajowym oraz przepisami wewnętrznymi określonymi w zarządzeniach Wójta Gminy Szczytniki.

2. Zgodnie z art. 29 oraz art. 32 ust. 4 RODO każdy pracownik Urzędu ma posiadać upoważnienie do przetwarzania danych osobowych.

3. Wzór upoważnienia, o którym mowa w ust. 2 stanowi załącznik nr 1 do Zarządzenia ODO.

4. Kierownicy komórek organizacyjnych Urzędu odpowiadają za terminowe przygotowanie oraz przedłożenie do podpisu projektów upoważnień do przetwarzania danych osobowych dla podległych

pracowników.

5. Sekretarz Gminy odpowiada za terminowe przygotowanie oraz przedłożenie do podpisu projektów upoważnień do przetwarzania danych osobowych dla Kierowników komórek organizacyjnych Urzędu.

6. Osoby, które zostały upoważnione do przetwarzania danych osobowych są obowiązane zachować je w tajemnicy, a także sposoby ich zabezpieczania, w trakcie oraz po ustaniu zatrudnienia.

7. Kierownicy komórek organizacyjnych Urzędu określają, w indywidualnych zakresach czynności pracowników, zakres odpowiedzialności za ochronę danych osobowych znajdujących się w zbiorze danych, przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem danych.

§ 3. 1. Administrator powołuje Inspektora ochrony danych osobowych zarządzeniem w sprawie wyznaczenia Inspektora ochrony danych, który jest odpowiedzialny za nadzór nad stosowaniem środków organizacyjnych i technicznych, zapewniających ochronę przetwarzanych danych, w szczególności przed ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem ustawy, kradzieżą, uszkodzeniem lub zniszczeniem. Status i obowiązki Inspektora określa załącznik nr 2 do Zarządzenia ODO.

2. Inspektor Ochrony Danych powinien:
   1) posiadać pełną zdolność do czynności prawnych oraz korzystać z pełni praw publicznych,
   2) posiadać fachową wiedzę na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełniania zadań, o których mowa w art. 39 RODO, ustawie i aktach prawa wewnętrznego,
   3) wykonywać zadania niezależnie i bez konfliktu interesów,
   4) mieć wiedzę w zakresie europejskiego i krajowego prawa ochrony danych oraz praktyk ochrony danych, a także szczegółową wiedzę na temat RODO,
   5) posiadać wiedzę na temat systemów informatycznych służących do przetwarzania, a także potrzeb i sposobów zabezpieczania danych osobowych przetwarzanych i nie może być karany za przestępstwo popełnione z winy umyślnej.

3. Administrator danych może powierzyć IOD wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań, o których mowa w niniejszym Zarządzeniu ODO.

4. W przypadku powołania IOD Administrator jest zobowiązany dokonać stosownego zgłoszenia zgodnie z wymogami prawa powszechnie obowiązującego. Jego wykreślenie z Rejestru następuje po powiadomieniu Prezesa Urzędu Ochrony Danych Osobowych o jego odwołaniu przez Administratora albo w przypadku jego śmierci.

5. Dane Inspektora ochrony danych publikowane są na stronie Biuletynu Informacji Publicznej oraz stronie internetowej Gminy.

6. Za publikację aktualnych danych, w tym danych teleadresowych Inspektora ochrony danych

odpowiada Kierownik Referatu Administracyjno-Organizacyjnego Urzędu.

7. Inspektor ochrony danych odpowiada za prowadzenie dokumentacji ochrony danych osobowych zgodnie z załącznikiem nr 6 do Zarządzenia ODO.

8. Kierownicy komórek organizacyjnych Urzędu odpowiadają za terminowe aktualizowanie dokumentacji ochrony danych osobowych, o której mowa w ust. 4 w zakresie merytorycznym funkcjonowania komórki.

9. Kierownicy komórek organizacyjnych Urzędu mogą wyznaczyć do realizacji zadań wynikających z ust. 5 oraz bezpośredniej współpracy z Inspektorem ochrony danych pracownika zarządzanej przez siebie komórki organizacyjnej, nie jest jednak możliwe delegowanie odpowiedzialności, o której mowa w ust. 5, za wyjątkiem przypadków wskazanych przez Administratora.

§ 4. 1. Administrator może powołać Administratora Systemów Informatycznych osobnym zarządzeniem.

2. ASI odpowiada za zapewnienie przestrzegania zasad ochrony danych osobowych przetwarzanych za pomocą systemów informatycznych określonych w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

3. ASI podczas wykonywania obowiązków z zakresu ochrony danych osobowych podlega bezpośrednio kierownikowi jednostki organizacyjnej, który reprezentuje Administratora.

4. W przypadku nie powołania ASI bezpieczeństwo przetwarzania danych osobowych w systemie informatycznym spoczywa na Administratorze.

4. Szczegółowy zakres obowiązków ASI określa załącznik nr 5 do Zarządzenia ODO.

§ 5. 1. Znajdujące się z zasobach Urzędu Gminy w Szczytnikach wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej przetwarzane zarówno w formie tradycyjnej (papierowej), jak i elektronicznej stanowią dane osobowe i podlegają ochronie stosownie do przepisów RODO oraz przepisów krajowych regulujących ochronę danych osobowych.

2. Dane osobowe przetwarzane w Urzędzie winny być przetwarzane wyłącznie w przypadkach o których mowa w art. 6, art. 9 oraz art. 10 RODO.

3. Przetwarzanie danych osobowych w Urzędzie dopuszcza się tylko w obszarze przetwarzania danych osobowych, określonym w załączniku nr 13 do Zarządzenia ODO.

4. Za aktualność określenia obszaru przetwarzania danych osobowych odpowiadają Kierownicy komórek organizacyjnych.

5. Wprowadza się do stosowania Instrukcję Zarządzania Systemem Informatycznym Urzędu Gminy w Szczytnikach, stanowiącą załącznik nr 11 do Zarządzenia ODO.

§ 6. 1. Zgodnie z art. 32 ust.1 lit. a) oraz art. 25 RODO wdraża się w Urzędzie Gminy

w Szczytnikach System Zarządzania Ryzykiem Ochrony Danych Osobowych, który pozwala (przy uwzględnieniu stanu wiedzy technicznej, kosztu wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia) wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

2. Sposób wdrożenia Systemu Zarządzania Ryzykiem Ochrony Danych Osobowych w tym metodykę przeprowadzania analizy ryzyka reguluje odrębne zarządzenie Wójta Gminy w Szczytnikach.

3. Ocena skutków dla ochrony danych oraz gdy przetwarzanie powoduje wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą odbywa się zgodnie z art. 35 i 36 RODO z zastosowaniem procedur opisanych w zarządzeniu Wójta Gminy Szczytniki, o którym mowa w ust. 2.

4. Analiza oceny ryzyka jest podstawą podejmowania działań zapobiegawczych i ich priorytetyzacji, a jej posiadanie pozwala szerzej spojrzeć na własną organizację. Aby dobrze podejść do analizy, należy pamiętać o kilku bardzo ważnych aspektach:

1) należy zidentyfikować zagrożenia, z którymi można spotkać się podczas przetwarzania danych,
2) należy zidentyfikować aktywa, które mogą być zagrożone,
3) należy określić prawdopodobieństwo wystąpienia ryzyka, a także ewentualny wpływ zdarzenia na aktywa,
4) na tej podstawie należy podjąć odpowiednie kroki zaradcze,
5) konieczne są okresowe przeglądy i zmiany w analizie, w miarę pojawiania się nowych zagrożeń.

5. Jako podstawowe środki techniczne i organizacyjne zapewniające ochronę danych osobowych mają być zastosowane środki określone w załączniku nr 10 do Zarządzenia ODO.

§ 7. 1. Mając na uwadze, że przetwarzane dane mają być adekwatne, stosowne oraz ograniczone do tego co niezbędne do celów w których są przetwarzane, pracownicy Urzędu są zobligowani do przetwarzania tylko tych danych, które są niezbędne do wykonywania powierzonych zadań i są przetwarzane na podstawie art. 6 ust.1 lit. b), c), d) lub e) RODO z zastrzeżeniem ust. 2.

2. W przypadku jeśli przetwarzanie danych osobowych odbywa się na podstawie art. 6 ust. 1 lit. a) RODO (czyli na podstawie zgody osoby, której dane dotyczą) pracownicy Urzędu są zobligowani do uzyskania (przed przystąpieniem do przetwarzania) zgody osoby której dane dotyczą zgodnie z przepisami prawa w szczególności z art. 7 i 8 RODO, dopełnienia obowiązku informacyjnego zgodnie z art. 12 - 14 RODO oraz respektowania i ułatwiania osobie, której dane dotyczą wykonania praw przysługujących na mocy art. 15 – 22 oraz art. 34 RODO.

§ 8. 1. Udostępnianie danych osobowych odbiorcom oraz organom publicznym, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem krajowym, następuje wyłącznie na mocy przepisów prawa.

2. Przetwarzanie danych osobowych dokonywane w imieniu Administratora przez podmiot przetwarzający jest dopuszczalne wyłącznie po uprzednim pisemnym powierzeniu przetwarzania danych osobowych zgodnym z RODO.

3. Za powierzenie przetwarzania danych osobowych odpowiadają Kierownicy komórek organizacyjnych Urzędu w zakresie realizacji zadań merytorycznych w podległej im komórce. Przed powierzeniem przetwarzania danych osobowych Kierownicy komórek organizacyjnych Urzędu zobligowani są do przedłożenia projektu umowy powierzenia przetwarzania danych osobowych do konsultacji Inspektorowi ochrony danych i uwzględnienia jego wytycznych.

§ 9. 1. Wprowadza się Instrukcję postępowania w sytuacji naruszenia zasad ochrony danych osobowych, stanowiącą załącznik nr 14 do Zarządzenia ODO.

2. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu oraz zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych odbywa się zgodnie z art. 33 oraz art. 34 RODO z zastosowaniem procedury opisanej w instrukcji postępowania w sytuacji naruszenia zasad ochrony danych osobowych, o której mowa w ust. 1.

§ 10. 1. Upoważnienia do przetwarzania danych osobowych wydane przed 25 maja 2018 r., które są zgodne z RODO i przepisami krajowymi obowiązującymi na dzień 25 maja 2018 r., podpisane przez osobę do tego upoważnioną, zachowują ważność.

2. Dostosowanie Polityki Ochrony Danych Osobowych do Zarządzenia ODO ma nastąpić w terminie do dnia 31 października 2018 r. Do tego czasu obowiązuje Polityka bezpieczeństwa przetwarzania danych osobowych oraz Instrukcja zarządzania systemem informatycznym w Urzędzie Gminy w Szczytnikach (Zarządzenie Nr 42 Wójta Gminy Szczytniki z dnia 30 grudnia 2016 r.) wg stanu na dzień 24.05.2018 r. z bieżącymi zmianami.

§ 11. Wykonanie Zarządzenia ODO powierza się wszystkim pracownikom Urzędu Gminy w Szczytnikach.

§ 12. Nadzór nad wykonaniem Zarządzenia ODO powierza się Sekretarzowi Gminy.

§ 13. Traci moc zarządzenie:

1) Zarządzenie Nr 14/2018 Wojta Gminy Szczytniki z dnia 22 maja 2018 r. w sprawie wprowadzenia Polityki bezpieczeństwa przetwarzania danych osobowych oraz Instrukcji zarządzania systemem informatycznym w Urzędzie Gminy w Szczytnikach.

§ 14. Zarządzenie ODO wchodzi w życie z dniem 01 sierpień 2019 r.

WÓJT
Marek Albrecht

Załącznik nr 1
do Zarządzenia Nr 26/2019
Wójta Gminy Szczytniki
z dnia 31 lipca 2019 r.

.....
(pieczęć Urzędu)

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Nr ..... / .....

Na podstawie art. 268a ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2017 r. poz. 1257 z późn. zm.), art. 31 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2018 r. poz. 994) oraz art. 29 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 (Dz.U.UE.L. z 2016 r. Nr 119, str. 1), niniejszym upoważniam do przetwarzania danych osobowych *Panią /Pana*[1]

.....
(imię i nazwisko pracownika)

zatrudnioną/zatrudnionego[1] na stanowisku .....
(nazwa stanowiska)

w .....
(nazwa komórki organizacyjnej Urzędu)

w Urzędzie Gminy w Szczytnikach do przetwarzania danych osobowych na stanowisku pracy ds. ..... oraz danych osobowych zawartych w niżej wymienionych zbiorach danych osobowych:

Lp.	Nazwa zbioru danych osobowych[2]	Zakres przetwarzania[3]

używając następujących identyfikatorów:
- w zakresie dostępu do oprogramowania Windows - .....
- do pracy w systemie informatycznym, obsługi tego systemu i urządzeń wchodzących w jego skład w zakresie:
  1) ..... (nazwa identyfikatora)

/w formie tradycyjnej[1]

Miejscem przetwarzania danych osobowych są pomieszczenia Urzędu Gminy w Szczytnikach pod adresem: 62-865 Szczytniki 139, o numerach pomieszczeń: .....

Okres ważności upoważnienia: od ..... na czas *nieokreślony/określony do* .....[1]

Traci moc upoważnienie numer: ..... z dnia .....[1]
(wpisać anulowane upoważnienie)

Wniosek przełożonego o nadanie upoważnienia	Data	Podpis
Akceptacja Inspektora Danych Osobowych	Data	Podpis
Nadanie upoważnienia Administrator Danych Osobowych	Data	Podpis

Oświadczam, iż:

1) zapoznałam/zapoznałem się z przepisami 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 (Dz.U.UE.L. z 2016 r. Nr 119, str. 1), obowiązującymi przepisami krajowymi z zakresu ochrony danych osobowych oraz z Zarządzeniem Nr 14/2018 Wójta Gminy Szczytniki z dnia 22 maja 2018 r. w sprawie ochrony danych osobowych w Urzędzie Gminy w Szczytnikach i zobowiązuję się do ich przestrzegania;
2) zobowiązuję się zachować w tajemnicy te dane oraz sposoby ich zabezpieczenia;
3) znana jest mi odpowiedzialność karna za naruszenie ww. przepisów.

.....
(data i podpis osoby upoważnionej)

Otrzymują:
1) Osoba upoważniona,
2) Inspektor ochrony danych
3) Referat Administracyjno-Organizacyjny – kadry
4) Referat merytoryczny

---

[1] Niewłaściwe należy skreślić lub usunąć,
[2] Należy podać nazwę zbioru danych osobowych zgodną z Rejestrem czynności przetwarzania,
[3] Zakres przetwarzania ma zawierać informację czy przetwarzanie jest:
- w pełnym zakresie,
- w zakresie ograniczonym do ..... (tu należy wybrać rodzaj operacji przetwarzania do jakich osoba jest upoważniona z następującego katalogu: zbieranie, utrwalanie, organizowanie, porządkowanie, wprowadzanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Data nadania uprawnień do systemów informatycznych	Data	Podpis
Data odebrania uprawnień do systemów informatycznych	Data	Podpis

Załącznik nr 2
do Zarządzenia Nr 26/2019
Wójta Gminy Szczytniki
z dnia 31 lipca 2019 r.

RAMOWY ZAKRES ZADAŃ
INSPEKTORA OCHRONY DANYCH
w URZĘDZIE GMINY w SZCZYTNIKACH

1. Inspektor Ochrony Danych realizuje obowiązki zgodnie z wymaganiami obowiązującego prawa przy uwzględnieniu ryzyka i oceny skutków związanych z czynnościami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania;
2. Osoby, których dane są gromadzone i przetwarzane, mogą kontaktować się z Inspektorem Ochrony Danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy przepisów prawa powszechnie obowiązującego i aktów prawa wewnętrznego;
3. Inspektor Ochrony Danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z przepisami prawa powszechnie obowiązującego i regulacjami wewnętrznymi;
4. Inspektor Ochrony Danych zobowiązany jest w szczególności do:
   1) informowania Administratora oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich na mocy powszechnie obowiązujących przepisów prawa oraz aktów prawa wewnętrznego w zakresie ochrony danych osobowych i doradzanie im w tej sprawie,
   2) nadzorowania i monitorowania przestrzegania przepisów prawa o ochronie danych oraz aktów prawa wewnętrznego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu Administratora i podmiotów trzecich uczestniczącego w operacjach przetwarzania oraz powiązanych z tym audytów,
   3) udziału w ocenie skutków dla ochrony danych zgodnie z art. 35 RODO oraz monitorowanie wykonania zaleceń opracowanych w wyniku wykonania oceny,
   4) współpracy z organem nadzorczym, pełnienia funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
   5) weryfikacji zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie, minimum raz w roku sprawozdania dla Administratora,
   6) przygotowywania do końca grudnia każdego roku Planu sprawdzeń (audytów) na następny rok i przedstawienie go Administratorowi, a po akceptacji jego realizację; plan sprawdzeń jest

określeniem harmonogramu weryfikacji systemu ochrony danych osobowych i w okresie pięciu lat sprawdzenia powinny łącznie objąć:

a) zabezpieczenia: organizacyjne i techniczne zbiorów danych osobowych,
b) system informatyczny służący do przetwarzania danych osobowych,
c) kompletność zidentyfikowanych zbiorów danych osobowych,
d) przesłanki legalności przetwarzania danych osobowych,
e) przesłanki legalności przetwarzania danych szczególnie chronionych,
f) zakres i cel przetwarzania danych,
g) merytoryczną poprawność danych i ich adekwatność do celu przetwarzania,
h) obowiązek informacyjny,
i) profilowanie,
j) przekazywanie danych do państwa trzeciego, w tym do krajów spoza Unii Europejskiej,
k) powierzenie przetwarzania danych osobowych (w tym zakres i poprawność konstruowania umów powierzenia przetwarzania danych),
l) zgodność dokumentacji przetwarzania danych osobowych z obowiązującymi przepisami prawa powszechnie obowiązującego i stosowanymi w Urzędzie zabezpieczeniami, technologiami, systemami, itp,

7) opracowania i aktualizowania Zarządzenia ODO w sprawie ochrony danych osobowych oraz dokumentów związanych z przetwarzaniem danych osobowych;
8) wspieranie administratora w realizacji przygotowywania odpowiedzi na żądania osób, których dane dotyczą, uzyskania od administratora potwierdzenia, czy przetwarzane dane osobowe jej dotyczące, a jeżeli ma to miejsce, uzyskanie dostępu do nich wraz z zakresem właściwych informacji o danych osobowych,
9) informowania o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania osób, które wystąpiły z takim żądaniem;
10) prowadzenia i aktualizacji rejestru czynności przetwarzania;
11) prowadzenia i aktualizacji rejestru naruszeń bezpieczeństwa, zgodnie ze wzorem oraz instrukcją określoną w załączniku nr 3 do Zarządzenia ODO;
12) przygotowania i przekazywania do podpisu do Administratora zgłaszania o naruszeniu ochrony danych osobowych do organu nadzorczego oraz zawiadamiania osoby, której dane dotyczą o naruszeniu ochrony danych osobowych – zgodnie z postanowieniami art. 33 i 34 RODO;
13) prowadzenia i aktualizacji rejestru umów powierzenia przetwarzania danych, jako element dokumentacji ochrony danych osobowych, stanowiącej załącznik nr 4 do Zarządzenia ODO;
14) nadzorowania i monitorowania procesu profilowania (o ile taki ma miejsce);
15) opiniowania umów zawieranych z podmiotami trzecimi w zakresie ich zgodności z przepisami prawa powszechnie obowiązującego i wewnętrznego w zakresie ochrony danych osobowych;

16) nadzorowania i monitorowania realizacji obowiązku informacyjnego, zgodnie z wymogami RODO;
17) prowadzenia Rejestru zgłoszonych sprzeciwów dotyczących przetwarzania danych osobowych i wniosków o zaprzestanie lub ograniczenie przetwarzania danych;
18) informowanie Administratora o wystąpieniu incydentu;
19) przygotowania wzorów klauzul informacyjnych i umów powierzenia przetwarzania danych;
20) gromadzenia potwierdzenia (dotyczy formy papierowej) wywiązania się z obowiązku informacyjnego oraz weryfikacji prawidłowości gromadzenia potwierdzeń w systemach informatycznych;
21) prowadzenia ewidencji upoważnień do przetwarzania danych osobowych oraz dokumentacji związanej z udzieleniem upoważnień, zgodnie ze wzorem zawartym w załączniku nr 4 do zarządzenia ODO;
22) przygotowywania upoważnień do przetwarzania danych osobowych zgodnie ze wzorem zawartym w załączniku nr 1 do Zarządzenia ODO;
23) wykonania szacowania ryzyka i oceny skutków przed wprowadzeniem nowej technologii (np. nowego systemu informatycznego, w którym przetwarzane będą dane osobowe wraz z administratorem systemu i właścicielem zasobu;

5. Inspektor Ochrony Danych jest uprawniony w szczególności do:
   1) wstępu do pomieszczeń, w których przetwarzane są dane osobowe,
   2) odbierania wyjaśnień od osób przetwarzających dane osobowe,
   3) dokumentowania ustaleń i dokonywania innych czynności niezbędnych do wykonania jego zadań wynikających z RODO, Ustawy, aktów prawa wewnętrznego i zakresu jego obowiązków/zakresu umowy o świadczenie usług;

Szczegółowy zakres uprawnień Inspektora Ochrony Danych określa RODO i Ustawa.

Załącznik nr 3
do Zarządzenia Nr 26/2019
Wójta Gminy Szczytniki
z dnia 31 lipca 2019 r.

REJESTR NARUSZEŃ BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Rodzaj naruszenia	Obowiązek zgłoszenia organowi nadzorczemu	Obowiązek zawiadomienia osoby, której dane dotyczą	Okoliczności naruszenia	Skutki naruszenia	Podjęte działania zaradcze

Załącznik nr 4
do Zarządzenia Nr 26/2019
Wójta Gminy Szczytniki
z dnia 31 lipca 2019 r.

REJESTR UMÓW
POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH
W URZĘDZIE GMINY SZCZYTNIKI

Lp.	Nr umowy i data zawarcia	Nazwa kontrahenta	Przedmiot umowy	Komórka organizacyjna nadzorująca wykonanie umowy	Uwagi
1					
2					

Załącznik nr 5
do Zarządzenia Nr 26/2019
Wójta Gminy Szczytniki
z dnia 31 lipca 2019 r.

ZADANIA ADMNISTRATORA SYSTEMÓW INFORMATYCZNYCH

1. Obowiązki ASI pełni wyznaczona przez Administratora osoba fizyczna lub osoba prawna.
2. Do najważniejszych obowiązków ASI należy:
   1) operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę danych osobowych w nich przetwarzanych;
   2) przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa;
   3) udział w przeprowadzanych przez Administratora kontrolach ochrony przetwarzanych danych osobowych;
   4) kontrola przepływu informacji pomiędzy systemem informatycznym, a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a system informatycznym;
   5) zarządzanie stosowanymi w systemach informatycznych środkami uwierzytelnienia; w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień na podstawie zaakceptowanych wniosków przez osobę do tego upoważnioną;
   6) utrzymanie systemów informatycznych Urzędu w należytej sprawności technicznej;
   7) bieżąca współpraca z IOD i Administratorem;
   8) zabezpieczenie systemów przetwarzania danych osobowych zgłoszonych ASI, w zależności od kategorii przetwarzanych w tym systemie danych;
   9) zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych;
   10) bieżący nadzór oraz zapewnianiem optymalnej ciągłości działania systemu informatycznego w tym opracowanie procedur określających zarządzanie systemem informatycznym przetwarzającym dane osobowe;
   11) w przypadku powstania zagrożenia ochrony danych osobowych bezzwłoczne podjęcie stosowanych działań;
   12) przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych;
   13) analiza raportów wszelkich zdarzeń w tym incydentów związanych z bezpieczeństwem systemów przetwarzania danych;
   14) zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z RODO, ustawą i innymi politykami i instrukcjami w zakresie ochrony danych osobowych;
   15) instalacja i konfiguracja oprogramowania i sprzętu używanego do przetwarzania danych osobowych;

16) konfiguracja i administracja oprogramowaniem systemowym i sieciowym zabezpieczającym dane osobowe przed nieupoważnionym dostępem;
17) nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności szkodliwego oprogramowania;
18) nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji;
19) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
20) przyznawanie na wniosek IOD, za zgodą Administratora informacji ściśle określonych praw dostępu do danych osobowych w danym systemie;
21) udzielanie pomocy w ramach realizacji serwisu dla potrzeb Urzędu Gminy w Szczytnikach;
22) diagnozowanie i usuwanie awarii sprzętu komputerowego oraz realizacja umów z firmami świadczącymi usługi pogwarancyjnego sprzętu komputerowego;
23) wykonywanie i zarządzanie kopiami awaryjnymi oprogramowania systemowego (w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie) i sieciowego;
24) wykonywanie i przechowywanie dokumentacji należącej do kompetencji ASI;
25) nadzór nad wdrożeniem i zarządzaniem aplikacjami (przeglądanie, nadawanie i odbieranie uprawnień użytkownikom, itp.), w których przetwarza się dane osobowe;
26) wspólnie z ADO współdziałanie w wypełnianiu wniosków zgłoszeń do rejestracji zbiorów danych osobowych w części E i F;
27) współpraca w trakcie kontroli UODO w zakresie dotyczącym systemu informatycznego.

Załącznik nr 6
do Zarządzenia Nr 26/2019
Wójta Gminy Szczytniki
z dnia 31 lipca 2019 r.

DOKUMENTACJA OCHRONY DANYCH OSOBOWYCH

1. Dokumentacja ochrony danych osobowych, o której mowa w § 3 ust. 7 Zarządzenia ODO składa się z:
   1) Rejestru czynności przetwarzania danych osobowych, wg wzoru określonego w załączniku nr 7 do Zarządzenia ODO;
   2) Polityki Bezpieczeństwa Danych Osobowych, na którą składają się elementy określone w ust. 5;
   3) Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy w Szczytnikach, stanowiącej załącznik nr 11 do Zarządzenia ODO;
   4) Rejestr wydanych upoważnień do przetwarzania danych osobowych wg wzoru określonego w załączniku nr 12 do Zarządzenia ODO;
   5) Procedura szacowania ryzyka określona w załączniku nr 15 do Zarządzenia ODO;

2. Rejestr czynności przetwarzania danych osobowych jest to dokument, który ma pokazywać w szczególności w jakich procesach w Urzędzie są przetwarzane dane osobowe, w jakim celu, kogo dotyczą oraz jak są zabezpieczone.

3. Celem prowadzenia rejestru jest możliwość zorientowania się przez organ nadzorczy jak faktycznie przebiegają procesy przetwarzania danych gdyż w tych kategoriach podmiotów może być to skomplikowane lub szczególnie istotne ze względu na prawo do prywatności osób, których dane dotyczą. Zakres informacji objętych rejestrem czynności przetwarzania danych osobowych nie wskazuje szczegółów tych procesów, a jedynie wskazuje podstawowe informacje, które mają pozwolić organowi nadzorczemu skierowanie szczegółowych pytań lub czynności kontrolnych wobec właściwych podmiotów. Innymi słowy celem prowadzenia rejestru jest przyspieszenie działania organu nadzorczego sytuacji, gdy czas reakcji jest kluczowy dla skuteczności nadzoru.

4. Rejestr czynności przetwarzania prowadzony jest:
   1) **w formie elektronicznej** w postaci tabeli w arkuszu kalkulacyjnym lub w dedykowanym oprogramowaniu i zawiera dla każdego zbioru danych osobowych minimalnie informacje:
      - Nazwę i dane kontaktowe administratora danych oraz dane kontaktowe IOD jeżeli został powołany;
      - Liczba porządkowa;
      - Nazwa zbioru danych osobowych lub nazwa czynności przetwarzania wynikająca ze zbioru danych osobowych;
      - Komórka organizacyjna Urzędu;

- Cel przetwarzania danych osobowych;
- Opis kategorii osób, których dane dotyczą;
- Kategorie danych osobowych (wrażliwe lub zwykłe);
- Podstawa prawna przetwarzania danych osobowych;
- Planowany termin usunięcia poszczególnych kategorii danych (jeżeli jest to możliwe);
- Nazwa współadministratora i dane kontaktowe;
- Nazwa podmiotu przetwarzającego i dane kontaktowe;
- Kategorie odbiorców, którym dane osobowe zostały lub zostaną udostępnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
- Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust.1 RODO;
- Informację o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej (nazwa państwa lub organizacji), a przypadku transferu (art. 49 ust. 1 akapit drugi RODO) wraz z dokumentacją opisującą zastosowane zabezpieczenia w tym procesie;
- Źródło danych, sposób zbierania danych do zbioru, w szczególności informacja czy dane ze zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą.

2) w formie papierowej – wydruk rejestru dokonywany z postaci elektronicznej oraz zatwierdzany przez Inspektora ochrony danych, wykonywany na żądanie uprawnionych osób oraz minimalnie co pół roku w przypadku zmian w rejestrze.

5. Polityka Bezpieczeństwa Danych Osobowych jest określeniem kierunków działań dla zapewnienia bezpieczeństwa zbiorów danych osobowych przetwarzanych w Urzędzie Gminy w Szczytnikach, podlega zatwierdzeniu przez Administratora i zawiera w szczególności:

1) Wykaz zbiorów danych osobowych prowadzony według wzoru określonego w załączniku nr 8 do Zarządzenia ODO ze wskazaniem dla każdego zbioru;
   - wykazu budynków i pomieszczeń lub części pomieszczeń tworzących obszar, w których przetwarzane są dane w zbiorze z uwzględnieniem przetwarzania w Systemie Informatycznym Urzędu Gminy w Szczytnikach;
   - wykazu opiekunów zbiorów danych osobowych;
   - wykazu programów i systemów informatycznych zastosowanych do przetwarzania danych osobowych ze wskazaniem zbiorów danych osobowych
   2) Opis sposobu przepływu danych pomiędzy poszczególnymi systemami według wzoru określonego w załącznik nr 9 do Zarządzenia ODO ;
3) Określenie środków technicznych (w tym informatycznych) oraz organizacyjnych (w tym ochrony fizycznej danych) niezbędnych oraz zastosowanych dla zapewnienia poufności,

integralności i rozliczalności przetwarzanych danych osobowych według załącznika nr 10 do Zarządzenia ODO.

6. Rejestr wydanych upoważnień do przetwarzania danych osobowych minimalnie zawiera informacje:

- Liczbę porządkową;
- Numer upoważnienia nadany w gminnym rejestrze upoważnień Wójta;
- Datę nadania upoważnienia
- Imię i nazwisko pracownika;
- Nazwa komórki organizacyjnej;
- Stanowisko;
- Nazwy zbiorów danych osobowych wraz z określeniem dla każdego zbioru zakresu przetwarzania;
- Datę początku obowiązywania upoważnienia;
- Datę końca obowiązywania upoważnienia;
- Wyrejestrowanie (w przypadku zakończenia obowiązywania upoważnienia w tym miejscu odnotowywane są przyczyny).
- Identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

7. Z uwagi na zabezpieczenie danych przed nieuprawnionym dostępem oraz ich utratą dostęp do dokumentacji, o której mowa w ust. 1 mają wyłącznie osoby upoważnione przez Wójta Gminy Szczytniki oraz podmioty uprawnione na podstawie obowiązującego prawa.

Załącznik nr 7
do Zarządzenia Nr 26/2019
Wójta Gminy Szczytniki
z dnia 31 lipcaec 2019 r.

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

LP.	Nazwa i nr zbioru danych osobowych lub nazwa czynności przetwarzania wynikająca ze zbioru danych osobowych, komórka organizacyjna	Cel przetwarzania danych osobowych	Opis kategorii osób, których dane dotyczą	Kategorie danych osobowych (wrażliwe lub zwykłe)	Podstawa prawna przetwarzania danych osobowych	Planowany termin usunięcia poszczególnych kategorii danych *(jeżeli jest to możliwe)*	Nazwa współadministratora i dane kontaktowe *(jeśli dotyczy)*	Nazwa podmiotu przetwarzającego i dane kontakowe *(jeśli dotyczy)*	Kategorie odbiorców, którym dane osobowe zostały lub zostaną udostępnione *(innych niż podmiot przetwarzający)*	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO *(jeżeli jest to możliwe)*	Transfer do kraju trzeciego lub org. międzynarodowej		Źródło danych, sposób zbierania danych do zbioru
											Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń	
		Art. 30 ust. 1 pkt b	Art. 30 ust. 1 pkt c	Art. 30 ust. 1 pkt c		Art. 30 ust. 1 pkt f	Art. 30 ust. 1 pkt a	Art. 30 ust. 1 pkt d	Art. 30 ust. 1 pkt d	Art. 30 ust. 1 pkt g	Art. 30 ust. 1 pkt e	Art. 30 ust. 1 pkt e	

Załącznik nr 8
do Zarządzenia Nr 26/2019
Wójta Gminy Szczytniki
z dnia 31 lipca 2019 r.

WYKAZ ZBIORÓW DANYCH OSOBOWYCH PRZETWARZANYCH ELETRONICZNIE LUB W INNY SPOSÓB ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA DANYCH OSOBOWYCH I WYKAZEM PRACOWNIKÓW PRZETWARZAJACYCH.

Numer zbioru	Nazwa zbioru nr i rok zgłoszenia zbioru do GIODO przez gminę nr nadany przez GIODO – księga rejestrowa zgłoszenie do IOD	Sposób przetwarzania	Nazwa programu 1) forma danych 2) zabezpieczenie informatyczne 3) bazę danych chroni UPS (TAK/NIE)	Pracownicy przetwarzający dany zbiór	Lokalizacja bazy danych/ nr pomieszczenia przetwarzania danych osobowych	Zabezpieczenie fizyczne

Załącznik nr 9
do Zarządzenia Nr 26/2019
Wójta Gminy Szczytniki
z dnia 31 lipca 2019 r.

OPIS STRUKTURY ZBIORÓW DANYCH OSOBOWYCH PRZECHOWYWANYCH W SYSTEMACH INFORMATYCZNYCH ORAZ SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY SYSTEMAMI INFORMATYCZNYMI.

L.p.	Nazwa i nr zbioru/nazwa programu/ rodzaj urządzenia /docelowy system informatyczny/obszar tworzenia danych	Opis zbioru – pola danych wskazujące zawartość poszczególnych pól informacyjnych – zakres przesyłanych danych osobowych	Pole powiązania – przepływu danych między poszczególnymi systemami – sposób transmisji

Załącznik nr 10
do Zarządzenia Nr 26/2019
Wójta Gminy Szczytniki
z dnia 31 lipca 2019 r.

PODSTAWOWE ŚRODKI TECHNICZNE I ORGANIZACYJNE ZAPEWNIAJĄCE OCHRONĘ DANYCH OSOBOWYCH

1. **Środki techniczne zapewniające ochronę danych osobowych** stanowią:

   1) środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej:

   - ☐☐ komputer służący do przetwarzania danych osobowych jest połączony z lokalną siecią komputerową;
   - ☐☐ zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące System informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania;
   - ☐☐ dane osobowe, które są przetwarzane na wydzielonej stacji komputerowej/ komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła uruchomionego sprzętu;
   - ☐☐ dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła lub z wykorzystaniem karty procesorowej oraz kodu PIN;
   - ☐☐ zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu Systemu informatycznego;
   - ☐☐ zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł;
   - ☐☐ zastosowano system rejestracji dostępu do Systemu informatycznego/zbioru danych osobowych;
   - ☐☐ zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji;
   - ☐☐ dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia;
   - ☐☐ zastosowano procedurę oddzwonienia (callback) przy transmisji realizowanej za pośrednictwem modemu;
   - ☐☐ zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej;
   - ☐☐ zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity – zastosowano ochronę antywirusową;
   - użyto system Firewall do ochrony dostępu do sieci komputerowej;
   - użyto system IDS/IPS do ochrony dostępu do sieci komputerowej;
   - w miarę możliwości – zastosowanie pseudonimizacji danych osobowych;

- w miarę możliwości – zastosowanie szyfrowania danych osobowych.

2) środki ochrony w ramach systemowych narzędzi programowych i baz danych:

☐ wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych;

☐☐ zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych;

☐☐ dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła lub przy użyciu karty procesorowej oraz kodu PIN;

☐☐ zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników Systemu informatycznego;

☐☐ zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych;

☐☐ zastosowano kryptograficzne środki ochrony danych osobowych;

☐☐ zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe;

☐☐ zastosowano mechanizm automatycznej blokady dostępu do Systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

2. Środki organizacyjne zapewniające ochronę danych osobowych stanowią:

1) środki ochrony fizycznej danych do których należą:

☐☐ zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi) lub o podwyższonej odporności ogniowej >= 30 min lub/i o podwyższonej odporności na włamanie - drzwi klasy C;

☐☐ zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą szyb antywłamaniowych;

☐☐ pomieszczenia, w którym przetwarzany jest zbiór danych osobowych nie są wyposażone w system alarmowy przeciwwłamaniowy;

☐☐ dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych nie są objęte systemem kontroli dostępu;

☐☐ dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych nie jest kontrolowany przez system monitoringu z zastosowaniem kamer przemysłowych lub dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych nie jest w czasie nieobecności zatrudnionych tam pracowników, nadzorowany przez służbę ochrony i dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych przez całą dobę nie jest nadzorowany przez służbę ochrony;

□□ zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie lub w zamkniętej metalowej szafie lub w zamkniętym sejfie lub kasie pancernej;

□□ kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie lub w zamkniętej metalowej szafie lub w zamkniętym sejfie lub kasie pancernej;

□□ pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą wolnostojącej gaśnicy;

- dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

2) środki organizacyjne do których należą:

□ sporządzono i wdrożono Politykę Bezpieczeństwa Danych Osobowych;

- sporządzono i wdrożono Instrukcję Zarządzania Systemem Informatycznym w Urzędzie Gminy w Szczytnikach;
- osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych;
- przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego;
- osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
- stworzono procedurę postepowania w sytuacji naruszenia ochrony danych osobowych;
- prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;
- informacji telefonicznych nie udziela się, względnie udziela się po zidentyfikowaniu rozmówcy i stwierdzeniu jego upoważnienia do uzyskania danych;
- przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności pracownika Urzędu Gminy w Szczytnikach upoważnionego do przetwarzania tych danych oraz w warunkach zapewniających bezpieczeństwo danych;
- monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane;
- kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

2. Środki techniczne i organizacyjne zapewniające ochronę danych osobowych wymienione w ust. 1 oraz ust. 2 należy stosować adekwatnie do ryzyka naruszenia zasad ochrony danych osobowych oraz celem zapewnienia, w miarę możliwości, jak najwyższej ochrony danych osobowych.

Załącznik nr 11
do Zarządzenia Nr 26/2019
Wójta Gminy Szczytniki
z dnia 31 lipca 2019 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W URZĘDZIE GMINY W SZCZYTNIKACH

1. Niniejszy dokument opisuje reguły Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych u Urzędzie Gminy w Szczytnikach.
2. Zastosowane w instrukcji określenia zostały zdefiniowane w § 1 Zarządzenia ODO ponadto na użytek niniejszej instrukcji:
   1) **„Administrator systemu informatycznego"** oznacza osobę wyznaczoną przez Administratora odpowiedzialną za opiekę techniczną i zabezpieczenia Systemu Informatycznego Urzędu Gminy w Szczytnikach;
   2) **„Użytkownik"** oznacza każdą osobę zatrudnioną w Urzędzie Gminy w Szczytnikach upoważnioną do przetwarzania danych osobowych oraz korzystającą lub mającą dostęp do Systemu Informatycznego Urzędu Gminy w Szczytnikach;
   3) **„Instrukcja"** oznacza niniejszą Instrukcję Zarządzania Systemem Informatycznym Urzędu Gminy w Szczytnikach;
   4) **„System informatyczny"** oznacza System Informatyczny Urzędu Gminy w Szczytnikach;
   5) **„identyfikator użytkownika"** oznacza ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
   6) **„stacja robocza"** oznacza każdy komputer lub inne urządzenie komputerowe przeznaczone do bezpośredniej pracy (w odróżnieniu od serwera, który tylko udostępnia zdalnie jakieś usługi.

3. Instrukcja określa zasady i tryb wykonywania czynności w Systemie Informatycznym Urzędu Gminy w Szczytnikach związanych z ochroną danych osobowych i składa się z procedur:
   1) Procedura nadawania i cofania uprawnień w Systemie Informatycznym Urzedu Gminy w Szczytnikach zamieszczona w ust. 4 Instrukcji.
   2) Procedura określająca wymogi oraz sposób użytkowania haseł w Systemie informatycznym zamieszczona w ust. 5 Instrukcji.
   3) Procedura rozpoczęcia, zawieszenia i zakończenia pracy dla użytkowników Systemu informatycznego zamieszczona w ust. 6 Instrukcji.
   4) Procedura tworzenia kopii zapasowych danych oraz programów i narzędzi programowych służących do przetwarzania danych osobowych w Systemie informatycznym zamieszczona w ust. 7 Instrukcji.

5) Procedura likwidacji nośników cyfrowych w tym kart elektronicznych zamieszczona w ust. 8 Instrukcji.
6) Procedura określająca metody i częstotliwość sprawdzania obecności szkodliwego/złośliwego oprogramowania służącego do uszkodzenia, przejęcia danych lub kontroli nad Systemem informatycznym przez osobę nieupoważnioną zamieszczona w ust. 9 Instrukcji.
7) Procedura wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych zamieszczona w ust. 10 Instrukcji.
8) Procedura Zarządzania Systemem informatycznym w przypadkach awaryjnych zamieszczona w ust. 11 Instrukcji.

4. Procedura nadawania i cofania uprawnień w Systemie Informatycznym Urzędu Gminy w Szczytnikach.

1) Użytkownik przedkłada niezwłocznie upoważnienie Inspektorowi ochrony danych, który dokonuje wpisu danych w Ewidencji wydanych upoważnień do przetwarzania danych osobowych i ustala dla niego odrębny identyfikator użytkownika.
2) Jeden użytkownik może mieć kilka identyfikatorów użytkownika.
3) Identyfikatory użytkownika muszą być unikalne w Systemie informatycznym również w zakresie identyfikatorów użytkowanych uprzednio przez niepracujących już użytkowników, co oznacza, że identyfikator użytkownika używany przez osobę już niezatrudnioną w Urzędzie nie może być użyty ponownie dla innego użytkownika.
4) Uprawnienia w systemie informatycznym nadawane są przez Administratora systemu informatycznego oraz inne upoważnione do tego osoby na podstawie Upoważnienia do przetwarzania danych osobowych oraz Upoważnienia do pracy w Systemie Informatycznym Urzędu Gminy w Szczytnikach, z zastosowaniem identyfikatorów nadanych przez Inspektora ochrony danych osobowych.
5) Dostęp do Systemu informatycznego ma być możliwy wyłącznie po wprowadzeniu identyfikatora użytkownika i dokonaniu uwierzytelnienia.
6) Jako identyfikatora użytkownika możliwe jest zastosowanie certyfikatu umieszczonego na karcie elektronicznej (karta kryptograficzna, chipowa, zbliżeniowa).
7) W przypadku cofnięcia upoważnienia do korzystania z Systemu informatycznego (w tym cofnięcia upoważnienia do przetwarzania danych osobowych):

   - Kierownik komórki organizacyjnej Urzędu zobowiązany jest powiadomić o tym Inspektora ochrony danych;

   - Inspektor ochrony danych wyrejestrowuje niezwłocznie użytkownika i poleca Administratorowi systemu informatycznego unieważnienie bądź zablokowanie identyfikatora i hasła wyrejestrowanego użytkownika oraz podejmuje inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

5. Procedura określająca wymogi oraz sposób użytkowania haseł w Systemie informatycznym.

1) Pierwsze hasło użytkownika do Systemu informatycznego jest zakładane przez Administratora Systemu Informatycznego oraz inne upoważnione do tego osoby podczas zakładania identyfikatora użytkownika w Systemie informatycznym. Następnie użytkownik musi zmienić hasło wg zasad określonych w punkcie 2.
2) Ustala się następujące zasady tworzenia i funkcjonowania haseł:
   a) hasło jest obowiązkowe dla każdego użytkownika posiadającego identyfikator użytkownika w Systemie informatycznym;
   b) po założeniu lub zmianie hasła przez Administratora systemu informatycznego lub innej upoważnionej do tego osoby, użytkownik ma obowiązek zarejestrować się do Systemu informatycznego i zmienić hasło;
   c) hasło składa się minimalnie z 8 znaków, które nie powinny być łatwe do zidentyfikowania (nie należy używać jako hasła np.: imion, nazwisk, daty urodzenia, identyfikatora w systemie informatycznym, wyrazów lub cyfr będących danymi osobowymi użytkownika lub dotyczących zbioru danych);
   d) hasło powinno się składać z małych i wielkich liter, cyfr oraz co najmniej jednego znaku nie będącego literą, ani cyfrą;
   e) hasła nie należy nigdzie zapisywać;
   f) w przypadku ujawnienia hasła musi ono zostać niezwłocznie zmienione, a niniejszy incydent zgłoszony Inspektorowi ochrony danych zgodnie z instrukcją postępowania w sytuacji naruszenia zasad ochrony danych osobowych określoną **w załączniku nr 14 do Zarządzania ODO;**
   g) hasło zmienia się przynajmniej raz z miesiącu;
   h) hasła użytkowników muszą być zapisywane w Systemie informatycznym w postaci zaszyfrowanej;
   i) hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności;
   j) użytkownik, który utracił hasło, klucz prywatny, nie może za pomocą przyznanego identyfikatora uzyskać dostępu do Systemu informatycznego, zobowiązany jest zgłosić bezzwłocznie ten fakt Administratorowi systemu informatycznego, który jest udostępniany przez Informatyka.
3) Zmiana hasła, o którym mowa w punkcie 2 stanowi podstawowy obowiązek pracownika.

6. Procedura rozpoczęcia, zawieszenia i zakończenia pracy dla użytkowników Systemu informatycznego.

1) Każde zakłócenie w pracy Systemu informatycznego zauważone przez użytkownika wymaga zgłoszenia Administratorowi systemu informatycznego.

2) Rozpoczęcie pracy w Systemie informatycznym na stacji roboczej wymaga wykonania następujących czynności:
   a) włączenie zasilania stacji roboczej (najczęściej poprzez włączenie listwy zasilającej);
   b) włączenie stacji roboczej;
   c) po załadowaniu się systemu operacyjnego – zarejestrowanie się w Systemie informatycznym przy użyciu identyfikatora użytkownika i hasła;
   d) po pozytywnym przejściu procedury uwierzytelnienia – uzyskanie dostępu do Systemu informatycznego.
3) Podczas zawieszenia pracy z wykorzystaniem Systemu informatycznego połączonego z jednoczesnym odejściem od stacji roboczej, użytkownik powinien zabezpieczyć stację roboczą przed dostępem osoby nieupoważnionej poprzez zastosowanie wygaszaczy ekranu zabezpieczonych hasłem (min. po 2 minutach), wyciągnięcie karty elektronicznej, kluczy z podpisem elektronicznym, zablokowanie stanowiska hasłem lub wyłączenie stacji roboczej.
4) Po zakończeniu pracy na stacji roboczej użytkownik zobowiązany jest:
   a) poprawnie zamknąć wszystkie działające programy i aplikacje;
   b) poprawnie zamknąć systemy operacyjne;
   c) w przypadku gdy stacja robocza nie jest przeznaczona do pracy ciągłej wyłączyć zasilanie (najczęściej poprzez wyłączenie listwy zasilającej).

7. Procedura tworzenia kopii zapasowych danych oraz programów i narzędzi programowych służących do przetwarzania danych osobowych w Systemie informatycznym.

1) Użytkownicy zabezpieczają dane osobowe przetwarzane w Systemie informatycznym przez wykonywanie kopii zapasowych danych oraz programów i narzędzi programowych służących do przetwarzania danych.
2) W Systemie informatycznym stosuje się zintegrowany i automatyczny system wykonywania kopii zapasowych (zwanego dalej systemem kopii zapasowych) na który składa się oprogramowanie oraz skrypty zarządzające wykonywaniem i odtwarzaniem kopii zapasowych oraz sprzęt komputerowy na którym dokonywane jest sporządzanie i przechowywanie kopii zapasowych.
3) Administrator systemu informatycznego jest odpowiedzialny za funkcjonowanie systemu kopii zapasowych oraz objęcie tym systemem wszystkich danych przetwarzanych w Systemie informatycznym jeśli tylko pozwalają na to możliwości techniczne.
4) W przypadku braku możliwości technicznych objęcia części danych systemem kopii zapasowych Administrator systemu informatycznego ustala z Inspektorem ochrony danych i użytkownikami sposób, częstotliwość oraz osobę odpowiedzialną za ręczne sporządzanie kopii zapasowej tych danych.
5) Tworzenie kopii zapasowych danych oraz programów i narzędzi programowych służących do

ich przetwarzania należy dokonywać z częstotliwością umożliwiającą odtworzenie danych po awarii Systemu informatycznego. Szczegółowy harmonogram tworzenia kopii zapasowych winien by zamieszczony w Polityce Bezpieczeństwa Danych Osobowych.

6) Opis i konfiguracja systemu kopii zapasowych oraz ustaleń, o których mowa w punkcie 4 Administrator system informatycznego odnotowuje w Polityce Bezpieczeństwa Danych Osobowych.
7) Użytkownicy winni przetwarzać dane osobowe w Systemie informatycznym w miejscach zabezpieczonych systemem kopii zapasowych, w innym przypadku zobligowani są do sporządzania osobiście ręcznych kopii zapasowych danych z uwzględnieniem następujących zasad:
   a) Kopie zapasowe należy sporządzać, w zależności od urządzeń obecnych na stanowisku, na następujących nośnikach: płytach CD-R, DVD, Blu-ray, kasetach streamera, zapasowych dyskach twardych, pamięciach przenośnych i innych dostępnych nośnikach cyfrowych będących własnością Urzędu Gminy w Szczytnikach, z których będzie możliwe poprawne odtworzenie danych w razie awarii systemu informatycznego.
   b) Wszystkie wykonane kopie zapasowe Systemu informatycznego powinny być opisane w sposób jednoznacznie określający zawartość kopii, datę i godzinę sporządzenia.
   c) Kopie zapasowe należy przechowywać w miejscu wskazanym przez Administratora systemu informatycznego, który jest zobligowany do konsultacji w tym zakresie z Inspektorem ochrony danych oraz Kierownikiem komórki organizacyjnej Urzędu. Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym wglądem, przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
9) Kopii zapasowych nie przechowuje się w tych samych pomieszczeniach, w których są przetwarzane lub przechowywane zbiory danych osobowych.
10) Kopie zapasowe przechowuje się w zamykanych szafach.
11) Za sporządzanie kopii zapasowych systemów i danych znajdujących się na serwerach odpowiedzialny jest Administrator.
12) W przypadku przekazywania nośników informacji zawierających kopie zapasowe danych osobowych podmiotom zewnętrznym na podstawie zawartych umów celem bezpiecznego ich przechowywania, stosownie wcześniej musi zostać określona procedura przekazywania oraz metody zabezpieczania przekazywania nośników informacji przed dostępem osób nieupoważnionych zarówno podczas transportu, jak i podczas późniejszego przechowywania z zastosowaniem środków ochrony kryptograficznej.
13) Kopie zapasowe należy:
   a) okresowo sprawdzać pod kątem dalszej przydatności do odtwarzania danych w przypadku awarii systemu;
   b) bezzwłocznie usuwać po ustaniu ich użyteczności.

14) Kopie zapasowe zapisane na nośnikach jednorazowego zapisu, a także na zepsutych nośnikach wielokrotnego zapisu przeznaczonych do likwidacji należy pozbawić zapisu danych w sposób uniemożliwiający ich odtworzenie, to znaczy zniszczyć w odpowiedniej niszczarce lub uszkodzić w trwały sposób zgodnie z procedurą likwidacji nośników cyfrowych określoną w ust. 8 Instrukcji.

8. Procedura likwidacji nośników cyfrowych w tym kart elektronicznych oraz zasady kasacji i utylizacji sprzętu komputerowego

Głównym celem jest zapewnienie bezpiecznej likwidacji sprzętu komputerowego, elementów eksploatacyjnych tegoż sprzętu oraz nośników danych. Procedurę stosuje się w następujący sposób:

1) Nośniki cyfrowe, w tym karty elektroniczne przeznaczone do likwidacji pozbawia się wcześniej zapisu danych na nich zapisanych, a przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
2) Użytkownicy mogą niszczyć niepotrzebne lub uszkodzone nośniki cyfrowe (z wyłączeniem kart elektronicznych) samodzielnie wyłącznie z użyciem specjalnie do tego przeznaczonych niszczarek, w przeciwnym razie są zobligowani do przekazania nośnika cyfrowego do Administratora systemu informatycznego celem likwidacji.
3) Karty elektroniczne po ustaniu ważności należy niezwłocznie przekazywać do Informatyka/ASI celem likwidacji.
4) Likwidacja dysków twardych oraz kart elektronicznych w Urzędzie winna odbywać się w obecności Inspektora ochrony danych i zostać potwierdzona w postaci wewnętrznego protokołu likwidacji.
5) Sprzęt wycofany z eksploatacji, trwale uszkodzony lub wyeksploatowany mogący zawierać dane osobowe zgłasza się niezwłocznie ASI i IOD.
6) Kasację należy poprzedzić zgromadzeniem w jednym miejscu sprzętu do kasacji przez osobę upoważnioną przez Administratora.
7) Należy także pamiętać o obowiązku zgłoszenia listy sprzętu komputerowego i eksploatacyjnego, a także nośników danych pozbawionych wcześniej w sposób trwały możliwości odczytu, do pracownika odpowiedzialnego za prowadzenie ewidencji rzeczowych składników majątku w Urzędzie (środków trwałych, wartości niematerialnych i prawnych, pozostałych środków trwałych, wyposażenia);
8) Sprzęt w wypadku gdy jest wpisany do ewidencji środków trwałych zostaje zdjęty z ewidencji środków trwałych i przekazany firmie zajmującej się utylizacją na podstawie karty przekazania odpadu, której 1 egzemplarz trafia do osoby upoważnionej przez Administratora Danych.

9. Procedura określająca metody i częstotliwość sprawdzania obecności szkodliwego/złośliwego oprogramowania służącego do uszkodzenia, przejęcia danych lub kontroli nad Systemem informatycznym przez osobę nieupoważnioną.

1) Nadzór nad sprawdzaniem systemu pod kątem obecności szkodliwego/złośliwego oprogramowania prowadzi Administrator systemu informatycznego.
2) Każdy użytkownik Systemu informatycznego zobowiązany jest do używania w pracy wyłącznie cyfrowych nośników informacji będących własnością Urzędu i przechowywania na nich tylko danych związanych z charakterem pracy.
3) Nośniki cyfrowe przekazywane Urzędowi mogą być użytkowane w Systemie informatycznym wyłącznie po sprawdzeniu ich programem antywirusowym.
4) Na komputerach stacjonarnych, serwerach i urządzeniach mobilnych należy:
   a) stosować programy antywirusowe monitorujące w czasie rzeczywistym System informatyczny podczas jego pracy oraz skanujące wyżej wymienione maszyny nie rzadziej niż raz na tydzień;
   b) stosować programy przeciwdziałające oprogramowaniu służącemu do przejęcia danych lub kontroli nad systemem informatycznym przez osobę nieuprawnioną.
5) Programy antywirusowe należy uaktualniać zgodnie z zaleceniami dostawcy programu. Za nadzór nad aktualizacją programów antywirusowych odpowiada Administrator systemu informatycznego.
6) Procedurę usuwania występujących wirusów komputerowych należy wykonać przy użyciu tylko dopuszczonych do użytkowania programów narzędziowych i antywirusowych zgodnie z obowiązującymi przepisami prawa w zakresie czynności kancelaryjnych *lub Instrukcją Kancelaryjną (Zarządzeniem w sprawie ustalenia procedury wykonywania czynności kancelaryjnych z wykorzystaniem informatyki i oprogramowania oraz procedury zarządzania oprogramowaniem.- wprowadzić takie zasady – jeśli będzie taka możliwość)*
7) W celu zabezpieczenia Systemu informatycznego przed atakami szkodliwego/złośliwego oprogramowania Administrator systemu informatycznego wdraża:
   a) identyfikację i uwierzytelnianie użytkowników uzyskujących dostęp do systemu poprzez kontrolę praw dostępu do zasobów systemu informatycznego;
   b) rejestrację informacji o dostępach lub próbach dostępu do zasobów i usług systemu;
   c) rejestrację i śledzenie komunikatów o błędach w pracy systemów informatycznych.

10. Procedura wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1) Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   a) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się

wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie,

b) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawiane są przez podmiot przetwarzający z którym zawarto umowę powierzenia przetwarzania danych osobowych.

2) Przeglądy i konserwacje Systemu informatycznego służącego do przetwarzania danych osobowych dokonywanego przez osoby i podmioty zewnętrzne są możliwe tylko pod warunkiem zawarcia z nim umowy powierzenia przetwarzania danych osobowych oraz przy obecności Administratora systemu informatycznego, Inspektora ochrony danych lub innej osoby upoważnionej przez Administratora.

11. Procedura Zarządzania Systemem informatycznym w przypadkach awaryjnych.

1) Poprzez przypadek awaryjny należy rozumieć awarię systemu informatycznego służącego do przetwarzania danych osobowych pod nieobecność Administratora systemu informatycznego lub konieczność dokonania czynności administracyjnych przez firmy serwisujące sprzęt i oprogramowanie na podstawie umów z użyciem identyfikatorów i haseł użytkowników systemu.

2) W przypadkach awaryjnych możliwe jest udostępnienie za zgodą Administratora lub osoby przez niego wyznaczonej identyfikatorów i haseł użytkowników uprzywilejowanych (którymi są użytkownicy posiadający uprawnienia na poziomie administratora systemów informatycznych).

3) W przypadku zaistnienia okoliczności określonych w punkcie 2 udostępnienie identyfikatorów i haseł musi odbywać się przy obecności osoby upoważnionej, a po usunięciu awarii hasło musi zostać natychmiast zmienione, lub identyfikator i hasło zablokowane do czasu zmiany hasła.

4) Przypadek awaryjny musi zostać niezwłocznie odnotowany w Systemie informatycznym w postaci notatki służbowej przekazanej Inspektorowi ochrony danych oraz Administratorowi systemu informatycznego.

5) Identyfikatory i hasła administracyjne do Systemu informatycznego wraz z instrukcją ich użycia w przypadku awaryjnym przechowywane są w zamykanej szafie przez Administratora systemu informatycznego lub Inspektora ochrony danych.

6) Miejsce przechowywania kodów alarmów i kluczy do szaf oraz pomieszczeń, w których przechowuje się identyfikatory i hasła administracyjne do Systemu informatycznego Administrator systemu informatycznego wskazuje Inspektorowi ochrony danych.

12. Pozostałe zasady funkcjonowania Systemu informatycznego:

1) Korzystanie z Systemu informatycznego odbywa się za pośrednictwem stanowisk pracy (w szczególności stacji roboczych), do których dostęp jest możliwy wyłącznie pod warunkiem

posiadania przez użytkownika identyfikatora użytkownika i hasła do systemu informatycznego.

2) Podczas przekazywania danych osobowych za pomocą urządzeń teletransmisji danych użytkownik powinien:
   a) zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych przed ich udostępnieniem osobom nieupoważnionym w postaci np. identyfikatora i hasła, szyfrowania przesyłanych danych, używania podpisu elektronicznego,
   b) zapewnić kontrolę nad tym jakie dane, kiedy i przez kogo zostały wprowadzone oraz komu są przekazywane.
3) Za nadzór nad bezpieczeństwem przesyłanych danych odpowiedzialny jest Administrator systemu informatycznego lub firma zewnętrzna, z którą Urząd podpisał umowę na przesył informacji. W przypadku wykrycia naruszenia zabezpieczeń tych danych Administrator systemu informatycznego zastosuje się do instrukcji postępowania w sytuacji naruszenia zasad ochrony danych osobowych określonej w załączniku nr 14 do Zarządzania ODO.
4) Komputery, serwery oraz urządzenia, na których jest przetwarzana baza danych oraz serwery służące do przetwarzania danych osobowych muszą posiadać urządzenia podtrzymujące zasilanie wyposażone w oprogramowanie umożliwiające bezpieczne zamknięcie pracujących aplikacji i wyłączenie systemu.
5) Zasoby w sieci komputerowej zawierające dane osobowe mogą być udostępniane jedynie w ramach funkcjonujących domen intranetowych tylko i wyłącznie z wyznaczonym dostępem dla określonych (uwierzytelnionych i uprawnionych) użytkowników.
6) Udostępnianie zasobów może odbywać się tylko i wyłącznie w sieciach zabezpieczonych sprzętową lub programową zaporą ogniową (firewall) przed dostępem do publicznej sieci telekomunikacyjnej.
7) W przypadku zdalnego dostępu do systemu i danych lub przesyłania tych danych w publicznej sieci telekomunikacyjnej, należy stosować kryptograficzne środki ochrony wobec danych wykorzystywanych do uwierzytelnienia.
8) Użytkownik komputera przenośnego zawierającego dane osobowe zobowiązany jest zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania określonym w załączniku nr 13 do Zarządzenia ODO, w tym zobowiązany jest stosować kryptograficzne środki ochrony wobec wszystkich przetwarzanych danych osobowych.
9) Udostępnianie danych osobowych odbiorcom w Systemie informatycznym jest możliwe tylko, jeśli system informatyczny w sposób jednoznaczny i trwały zachowuje informacje o odbiorcy, czasie udostępnienia danych osobowych i zakresie udostępnienia danych osobowych, chyba, że System informatyczny używany jest do przetwarzania danych zawartych w zbiorach

jawnych.

10) Kierownicy komórek organizacyjnych Urzędu są zobowiązani do kontrolowania przestrzegania innych instrukcji i procedur, które Inspektor ochrony danych podał im do wiadomości.

13. Wszystkie procedury, wytyczne i niezbędne instrukcje dotyczące bezpieczeństwa systemu informatycznego zawarte w Polityce Bezpieczeństwa Danych Osobowych, Inspektor ochrony danych przekazuje użytkownikom do wiadomości w zakresie niezbędnym do bezpiecznej pracy w Systemie informatycznym.

Załącznik nr 12
do Zarządzenia Nr 26/2019
Wójta Gminy Szczytniki
z dnia 31 lipca 2019 r.

REJESTR WYDANYCH UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY W SZCZYTNIKACH

Lp	Nr upoważn. z gminnego rejestru upoważnień	Data nadania upoważnienia	Imię i nazwisko pracownika	Nazwa komórki organizacyjnej Stanowisko	Nazwy zbiorów danych osobowych zakres przetwarzania danych w zbiorze	Data początku obowiązywania upoważn.	Data końca obowiązywania upoważn.	Przyczyny wyrejestrowania	Identyfikator do przetwarzania danych w systemie informatycznym

Załącznik nr 13
do Zarządzenia Nr 26/2019
Wójta Gminy Szczytniki
z dnia 31 lipca 2019 r.

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

1. Administrator przetwarza dane wyłącznie w pomieszczeniach do tego przeznaczonych w sposób uniemożliwiający dostęp do danych osobom nieuprawnionym.

2. Dane osobowe przetwarzane są w budynku siedziby Urzędu Gminy w Szczytnikach, w sposób tradycyjny i za pomocą systemów informatycznych.

3. Obszar przetwarzania danych osobowych stanowią:

   1) pomieszczenia biurowe, pomieszczenia archiwalne, pomieszczenia w których funkcjonuje System Informatyczny w następujących komórkach organizacyjnych Urzędu, zamieszczony w poniższej tabeli:

Lp.	Nazwa jednostki organizacyjnej – adres - budynek	Nazwa Referatu/ samodzielnego stanowiska Nr pomieszczenia przetwarzania danych osobowych	Przydział kluczy do pomieszczenia
1.	Urząd Gminy w Szczytnikach 62-865 Szczytniki 139	➢ Budynek urzędu gminy – Szczytniki 139	1) Wójt Gminy 2) Pracownik obsługi sekretariatu
		➢ Referat Finansów – Podatki – Nr 1/a	1) St. ds. wymiaru podatków i opłat lokalnych
		➢ Referat Administracyjno-Organizacyjny – Obrona cywilna i zarządzanie kryzysowe/ Biuro Rady Gminy – Nr 1/b	1) St. ds. zarządzania kryzysowego, obrony cywilnej, obsługi Rady Gminy i kontroli procesu windykacji
		➢ Referat Infrastruktury i Ochrony Środowiska, Stanowisko ds. profilaktyki i rozwiązywania problemów alkoholowych – Nr 2/a	1) Kierownik RIOŚ
		➢ Referat Spraw Obywatelskich – Nr 2/b	1) Kierownik RSO
		➢ Referat Infrastruktury i Ochrony Środowiska – Nr 2/c	
		➢ Referat Infrastruktury i Ochrony Środowiska – Nr 2/d	
		➢ Referat Infrastruktury i Ochrony Środowiska – Nr 2/e	
		➢ Referat Finansów – Nr 3/a	1) St.ds. księgowości budżetowej
		➢ Skarbnik Gminy – Nr 3/b	1) Skarbnik gminy
		➢ Sekretariat Urzędu Nr 4/b	1) Pracownik obsługi

			sekretariatu
		➢ Wójt Gminy Nr 4/a	1) Wójt Gminy
		➢ Sekretarz Gminy - Nr 4/c	1) Sekretarz Gminy
		➢ Pomieszczenie służbowe - socjalne / kserokopiarka – Nr 4/d	1) Pracownik obsługi sekretariatu
		➢ Sala konferencyjna – Nr 4/e	1) Pracownik obsługi sekretariatu
		➢ Referat Administracyjno-Organizacyjny / Obsługa prawna Urzędu – Nr 5	1) Kierownik RAO
		➢ Pomieszczenie służbowe/serwerownia – Nr 6	1) Pracownik obsługi sekretariatu
		➢ Referat Spraw Obywatelskich – Nr 7	1) Kierownik RSO
		➢ Referat Finansów – Nr 8	1) St.ds. księgowości jednostek podległych
2	Zespół Szkół w Szczytnikach Popów 54	Archiwum Zakładowe	Pracownik obsługi sekretariatu

4. Szczegółowy wykaz pomieszczeń dla obszarów, w których przetwarzane są dane osobowe prowadzi Inspektor ochrony danych w ramach dokumentacji, o której mowa w załączniku nr 4 do Zarządzenia ODO.
5. O każdej zmianie miejsca przetwarzania danych osobowych Kierownicy komórek organizacyjnych Urzędu mają obowiązek informować Inspektora ochrony danych przed rozpoczęciem przetwarzania w nowym miejscu.
6. Osoby upoważnione do przechowywania kluczy pomieszczeń składają oświadczenie o miejscu ich przechowywania.
7. W przypadku nieobecności osób wskazanych w przydziale kluczy, klucze ewidencyjnie przekazywane są wskazanym przez nich osobom.
8. Każde pomieszczenie posiada trzy egzemplarze klucza, każda szafa, w której przechowywane są dokumenty związane z przetwarzaniem danych osobowych posiada dwa egzemplarze klucza. Egzemplarze niewykorzystywane w ilości min 1szt. przechowywane są w depozycie u Wójta Gminy w zamkniętej kopercie otwieranej komisyjnie w sytuacjach nieprzewidywalnej nieobecności osób upoważnionych.
9. Klucze do wszystkich pomieszczeń posiada osoba sprzątająca, która składa oświadczenie o miejscu ich przechowywania.

Załącznik nr 14
do Zarządzenia Nr 26/2019
Wójta Gminy Szczytniki
z dnia 31 lipca 2019 r.

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH

1. Zastosowane w instrukcji określenia zostały zdefiniowane w § 1 Zarządzenia ODO oraz w załączniku nr 11 do Zarządzenia ODO.
2. Naruszeniem zasad organizacyjnej ochrony danych osobowych jest naruszenie środków, o których mowa w ust. 2 załącznika nr 10 do Zarządzenia ODO, w szczególności:
   1) nieuprawniony dostęp lub próba dostępu do pomieszczeń, w których odbywa się przetwarzanie danych osobowych;
   2) praca przy przetwarzaniu danych osobowych osoby nieprzeszkolonej lub nieposiadającej upoważnienia do przetwarzania danych osobowych wydanego przez Administratora;
   3) udzielenie informacji telefonicznych nieuprawnionej osobie do uzyskania tych informacji;
   4) celowe lub nieświadome przekazanie danych osobowych osobie nieuprawnionej do ich otrzymania;
   5) nienależytym zabezpieczeniu danych w tym niechowaniu dokumentów do zamykanych szaf i pozostawianie w miejscu ogólnie dostępnym, przechowywaniu dokumentów i nośników cyfrowych zawierających dane osobowe w szafach z niesprawnymi zamkami;
   6) wyrzucaniu dokumentów zawierających dane osobowe bez uprzedniego ich zniszczenia w stopniu uniemożliwiającym odczytanie danych;
   7) przebywaniu pracowników obsługi informatycznej lub technicznej firm zewnętrznych w budynku bez nadzoru uprawnionych pracowników Urzędu;
   8) kradzież dokumentów lub nośników cyfrowych zawierających dane osobowe.
3. Naruszeniem zasad technicznej ochrony danych osobowych jest naruszenie środków, o których mowa w ust. 1 załącznika nr 10 do Zarządzenia ODO, w szczególności:
   1) naruszenie lub próby naruszenia integralności Systemu informatycznego przez osoby nieuprawnione do dostępu do systemu informatycznego;
   2) nieautoryzowane logowanie do Systemu informatycznego;
   3) nieuprawnione prace na koncie użytkownika dopuszczonego do przetwarzania danych osobowych przez osobę do tego nieuprawnioną;
   4) ujawnienia hasła funkcjonującego w Systemie informatycznym osobie nieuprawnionej;
   5) istnienie nieautoryzowanych kont dostępu do Systemu informatycznego, w tym nie blokowanie kont osób z cofniętym upoważnieniem do przetwarzania danych osobowych lub/i z cofniętym upoważnieniem do pracy w Systemie informatycznym;
   6) włamanie lub próba włamania z zewnątrz sieci;

7) nieautoryzowane zmiany danych w Systemie informatycznym;

8) nieautoryzowana zmiana lub usunięcie danych zapisanych na kopiach bezpieczeństwa lub kopiach archiwalnych;

9) brak lub niepełna ochrona antywirusowa elementów systemu informatycznego;

10) niewykonywanie kopii zapasowych w przewidzianym terminie;

11) wykonywanie uszkodzonych kopii zapasowych;

12) niewłaściwe lub nieuprawnione uszkadzanie, niszczenie nośników zawierających dane osobowe;

4. W przypadku wystąpienia okoliczności wskazujących na możliwość naruszenia zasad ochrony danych, o którym mowa w ust. 2 i ust. 3 pracownicy Urzędu zobowiązani są do natychmiastowego reagowania w sposób określony w ust. 5 do ust. 7.

5. W sytuacji wskazującej na naruszenie ochrony danych osobowych należy:

1) w miarę możliwości zabezpieczyć dane osobowe przed dalszą podatnością na naruszenie;

2) natychmiast poinformować Inspektora ochrony danych oraz swojego bezpośredniego przełożonego;

3) w przypadku naruszenia zasad ochrony organizacyjnej fizycznej zgłosić ten fakt Administratorowi;

4) w przypadku naruszenia zasad ochrony technicznej zgłosić ten fakt Administratorowi systemu informatycznego oraz Inspektorowi ochrony danych.

6. Po pierwszej reakcji na potencjalne naruszenie zasad ochrony danych osobowych, osoba stwierdzająca naruszenie wraz z Inspektorem ochrony danych zobowiązane są do:

1) podjęcia czynności zmierzających do zabezpieczenia miejsca zdarzenia, zabezpieczenia ewentualnych dowodów naruszenia i minimalizacji zaistniałych szkód, w szczególności poprzez:

□□ wstrzymanie przekazywania i udostępniania danych osobowych;

□□ usunięcie uchybień;

□□ zastosowanie dodatkowych środków technicznych i organizacyjnych zabezpieczających dane osobowe;

□□ zwiększenie kontroli podczas przetwarzania danych osobowych;

2) umożliwie pełnego udokumentowania zdarzenia celem precyzyjnego określenia przyczyn i ewentualnych skutków naruszenia obowiązujących zasad.

7. W sytuacji naruszenia zasad ochrony danych osobowych, niezwłocznie, po wcześniejszym wykonaniu czynności opisanych w ust. 5 i ust. 6, dokonuje się oceny, czy naruszenie skutkuje lub może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, w szczególności:

1) Oceny, czy naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych dokonuje zespół składający się z:

□□ Inspektora ochrony danych;

□□ Kierowników komórek organizacyjnych Urzędu merytorycznie odpowiedzialnych za dane osobowe, których naruszenie dotyczy;

□□ Administratora systemu informatycznego jeśli naruszenie dotyczy danych osobowych przetwarzanych w Systemie informatycznym.

2) Dokonuje się oceny prawdopodobieństwa ryzyka naruszenia praw lub wolności osób fizycznych;

3) Zespół, o którym mowa w punkcie 1 winien oceny dokonać bez zbędnej zwłoki, w miarę możliwości, nie później niż w terminie 24 godzin od stwierdzenia naruszenia i przekazuje niniejszą ocenę Administratorowi.

8. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki (w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia) zgłasza je (zgodnie z art. 33 RODO) organowi nadzorczemu właściwemu zgodnie z art. 55 RODO, chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych – prawdopodobieństwo określone jest zgodnie z ust. 7.

9. Jeśli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator, bez zbędnej zwłoki, zawiadamiania osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych zgodnie z art. 34 RODO.

Załącznik nr 15
do Zarządzenia Nr 26/2019
Wójta Gminy Szczytniki
z dnia 31 lipca 2019 r.

Procedura szacowania ryzyka w Urzędzie Gminy w Szczytnikach

Podmiot - Urząd Gminy w Szczytnikach
Aktywa – zasoby wykorzystywane przez organizację, związane z przetwarzaniem danych osobowych; aktywa można podzielić na:
a) aktywa podstawowe:
- zbiory danych osobowych lub czynności przetwarzania danych wynikające ze zbiorów danych osobowych ,

b) aktywa wspierające:
- sprzęt (np. laptop),
- oprogramowanie (np. aplikacja wykorzystywana do wykonywania usług),
- sieć (np. wewnętrzna sieć administratora),
- personel (np. wykwalifikowani pracownicy),
- siedziba (np. budynki)
- struktura organizacyjna (np. ustanowienie inspektora ochrony danych)

Dostępność – zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, kiedy jest to potrzebne,
Integralność – zapewnienie dokładności i kompletności informacji oraz metod przetwarzania danych,
Poufność – zapewnienie, że informacja jest dostępna jedynie dla osób upoważnionych,
Podatność - „słaby punkt", właściwość danego aktywu, które mogą być wykorzystywane przez zagrożenie (np. brak systematycznego aktualizowania jest podatnością oprogramowania, która może spowodować realne powstanie zagrożenia w postaci zainstalowania wirusa w komputerze),
Właściciel ryzyka – osoba (osoby) odpowiedzialna za dany aktyw i ryzyko z nim związane (np. kierownik działu),
Zabezpieczenie – środek, który modyfikuje ryzyko naruszenia bezpieczeństwa (np. szyfrowanie, kontrola dostępu, czujniki dymu, szafy ogniotrwałe),
Zagrożenie – potencjalne zdarzenie, które może wywołać szkodę.

OPIS POSTĘPOWANIA

I. SZACOWANIE RYZYKA

1. Identyfikowanie potencjalnych zagrożeń i podatności.

Ocena ryzyka przeprowadzana jest dla każdej operacji przetwarzania danych osobowych, rozpatruje trzy obszary:
1) prawdopodobieństwo wystąpienia zagrożenia,
2) podatność aktywów na zagrożenie,
3) skutki potencjalnych zagrożeń,

biorąc pod uwagę następstwa naruszenia lub utraty:
1) poufności,
2) integralności,
3) dostępności,

które mogą nastąpić w wyniku działań:
1) umyślnych – (U),
2) przypadkowych – (P),
3) naturalnych – (N).

Przyjmuje się, że zagrożenia (U,P) są wynikiem działań ludzkich, natomiast źródła zagrożeń (N) są niezależne od człowieka.
Listę potencjalnych zagrożeń dla podmiotu umieszczono w **Tabeli nr 1**. Wymienione zagrożenia należy uwzględnić podczas szacowania prawdopodobieństwa, podatności oraz skutków zdarzeń.
Należy uwzględnić, że podatność, nie powoduje jeszcze szkody, ale należy zgodnie z **Tabelą nr 2**

oszacować stopień zabezpieczenia aktywa pod kątem zidentyfikowanych zagrożeń.

Identyfikacja zagrożeń.
Tabela nr 1.

Lp.	Rodzaj	Zagrożenie	Źródło
1.	Zniszczenie fizyczne	Pożar, zalanie, zanieczyszczenie, poważny wypadek, zniszczenie urządzeń lub nośników, pył, korozja, wychłodzenie.	P,U,N
2.	Zjawiska naturalne	Zjawiska klimatyczne, zjawiska pogodowe, powódź.	N
3.	Naruszenie bezpieczeństwa informacji	Podsłuch, kradzież nośników lub dokumentów, kradzież urządzenia, szpiegostwo, kopiowanie danych, odtworzenie wyrzuconych nośników.	U
		Ujawnienie informacji, dane z niewiarygodnych źródeł, sfałszowanie oprogramowania, brak spełnienia wymagań prawnych dotyczących archiwizowania dokumentacji.	P, U
4.	Awarie techniczne	Awaria urządzenia, niewłaściwe funkcjonowanie urządzenia, niewłaściwe funkcjonowanie oprogramowania. Umyślne uszkodzenie urządzenia lub oprogramowania.	P U
5.	Utrata usług	Awaria systemu klimatyzacji, utrata dostaw prądu, awaria urządzenia telekomunikacyjnego.	P,U,N
6.	Zakłócenia spowodowane promieniowaniem	Promieniowanie elektromagnetyczne, promieniowanie cieplne, impuls elektromagnetyczny	P,U,N
7.	Nieautoryzowanie działania	Niewłaściwe funkcjonowanie urządzeń, niewłaściwe funkcjonowanie oprogramowania. Przeciążenie systemu informacyjnego, naruszenie zdolności utrzymania systemu informacyjnego.	P P,U
8.	Naruszenie bezpieczeństwa funkcji	Błąd użytkowania. Naruszenie praw. Fałszowanie praw, odmowa działania. Naruszenie dostępności personelu.	P P,U U P,U,N

Identyfikacja występujących podatności.
Tabela nr 2.

Rodzaj	Podatności	Zagrożenia
Sprzęt	Niezabezpieczone urządzenie do przechowywania danych.	Kradzież danych lub dokumentów
	Brak staranności przy pozbywaniu się nośników.	Kradzież nośników lub danych.
	Niekontrolowane kopiowanie.	Kradzież danych.
	Wrażliwość na wilgoć, pył, zanieczyszczenie.	Pył, korozja, wychłodzenie.
	Wrażliwość na zmiany temperatury.	Zjawiska pogodowe.
	Wrażliwość na zmiany napięcia zasilania.	Utrata zasilania.
	Brak planów okresowej wymiany sprzętu.	Niszczenie lub awaria urządzenia lub nośników.
Oprogramowanie	Brak wylogowania przy opuszczaniu stacji roboczej.	Nadużycie praw.
	Błędne przypisanie praw dostępu.	
	Brak mechanizmów identyfikacji i uwierzytelniania użytkownika.	Fałszowanie praw.

	Złe zarządzanie hałasami. Brak fizycznej kontroli budynków, drzwi i okien. Brak skutecznej kontroli zmian.	Kradzież nośników lub danych. Zakłócenie procesu.
Sieć	Niezabezpieczone linie telefoniczne. Złe łączenie kabli. Brak identyfikacji i uwierzytelniania nadawcy i odbiorcy. Niezabezpieczone połączenie z siecią publiczną. Uszkodzenie fizyczne sieci lub kabli.	Podsłuch. Awaria urządzenia telekomunikacyjnego. Fałszowanie praw. Nieautoryzowane użycie urządzeń. Zatrzymanie procesu.
Personel	Nieobecność personelu. Niewystarczające szkolenie z bezpieczeństwa, użycia oprogramowania lub sprzętu. Brak mechanizmów monitorowania. Praca personelu zewnętrznego lub sprzątającego bez nadzoru.	Naruszenie danych, brak dostępności. Błąd użytkowania. Nielegalnie przetwarzanie danych. Nieautoryzowane użycie urządzeń.
Siedziba	Lokalizacja na obszarach zagrożonych powodzią. Brak fizycznej ochrony budynków, drzwi i okien.	Powódź. Kradzież, zniszczenie.
Organizacja	Brak procedur regulujących bezpieczeństwo aktywów. Brak regularnego nadzoru Brak zdefiniowanego postępowania dyscyplinarnego.	Utrata danych, niezgodność z przepisami prawa, nieautoryzowany dostęp. Nadużycie praw. Kradzież urządzenia.

2) Szacowanie poziomu ryzyka

Metodyka oceny ryzyka, została ustanowiona w zgodzie z rzeczywistym stanem bezpieczeństwa aktywów w podmiocie oraz dostarcza rzetelnych wyników na temat faktycznego poziomu ryzyka. Za dane wejściowe do procesu oceny uważa się wszelkie informacje przedstawione w analizie ryzyka (dane z inwentaryzacji), a w szczególności miejsce, obecne zabezpieczenia oraz wagę przypisaną przez właściciela aktywa. Ponadto każde szacowanie prawdopodobieństwa, podatności oraz skutków zdarzenia powinno się odbywać w relacji z Tabelą nr 1 i 2 niniejszej procedury według zadanych kryteriów:

Szacowanie prawdopodobieństwa

Tabela nr.3

Badane kryterium	Ryzyko	Kategoria ryzyka	Wartość
(PO) Prawdopodobieństwo (możliwość wystąpienia)	Niskie, odległe, mało realne szanse na zdarzenie. Może się zdarzyć lub zdarza się sporadycznie. Bardzo realne szanse wystąpienia.	małe średnie duże	1 2 3

Szacowanie podatnością

Tabela nr 4

Badane kryterium	Ryzyko	Kategoria ryzyka	Wartość
(PR) Podatność (słabość aktywna)	Aktywa bardzo dobrze zabezpieczone. Aktywa dostatecznie zabezpieczone. Aktywa słabo lub nie zabezpieczone.	mała średnia duża	1 2 3

Szacowanie skutków
Tabela nr 4

Badane kryterium	Ryzyko	Kategoria ryzyka	Wartość
(S) Skutek (wpływ na organizację i/lub proces)	Utrata danych nie spowoduje utrudnień w pracy urzędu lub danego procesu, odtworzenie danych nie wymaga dużych nakładów czasu.	mały	1
	Utrata danych spowoduje zakłócenia w funkcjonowaniu i/lub wizerunku urzędu, odtworzenie danych jest możliwe ale pracochłonne.	średni	2
	Utrata danych spowoduje zatrzymanie procesu i/lub wywoła poważne konsekwencje prawne, odtworzenie danych i reputacji będzie trudne i kosztowne.	duży	3

Kategoria ryzyka zostaje ustanowiona zgodnie ze wzorem:
R=PR*PO*S
gdzie:
PR prawdopodobieństwo
PO podatność
S skutek

Wynik z działania zgodnie z poniższą tabelą należy przypisać ustanowionym kategoriom ryzyka, a następnie uruchomić czynności doskonalące bezpieczeństwo informacji w celu redukcji ryzyka do poziomu akceptowalnego. W uzasadnionych przypadkach można zaakceptować ryzyko kategorii drugiej lub trzeciej, szczególnie gdy działania profilaktyczne odnoszą się do długoterminowych i kosztownych inwestycji na rzecz bezpieczeństwa danego aktywa.

Wytyczne do postępowania z ryzykiem
Tabela nr 5

Lp.	Wartość ryzyka	Kategoria (poziom) ryzyka	Akceptacja ryzyka Tak/Nie	Działania zapobiegawcze (postępowanie z ryzykiem)	Właściciel ryzyka
1.	1 - 7	mały	Tak	Podejmowanie działań nie jest konieczne, zalecane jest utrzymywanie ryzyka na obecnym poziomie. Można podjąć działania doskonalące.	Dział (wydział, samodzielne stanowisko pracy lub inna wewnętrzna komórka organizacyjna)
2.	8 - 17	średni	nie	Należy zredukować ryzyko do poziomu akceptowalnego poprzez rozwiązania infrastrukturalne i/lub proceduralne	Dział (wydział, samodzielne stanowisko pracy lub inna wewnętrzna komórka organizacyjna)
3.	18 - 27	duży	nie	Należy zdecydowanie zredukować ryzyko poziomu akceptowalnego poprzez rozwiązania infrastrukturalne i/lub proceduralne usuwając lub przenosząc	Dział (wydział, samodzielne stanowisko pracy lub inna

				aktywa w bezpieczniejsze miejsce.	wewnętrzna komórka organizacyjna)

Szacowanie ryzyka oraz postępowanie z ryzykiem (Tabela nr 6), stanowi załącznik do niniejszej procedury.

3) Działania doskonalące bezpieczeństwo informacji.

Procesy doskonalące bezpieczeństwo informacji prowadzone są w oparciu i podjęcie działania zapobiegawcze i/lub korygujące adekwatnie do wagi potencjalnych problemów. W tym celu uruchamia się plan postępowania z ryzykiem. W wyniku tych działań należy według powyższych zasad powtórnie dokonać szacowania ryzyka w celu sprawdzenia skuteczności i odporności systemu na przypadek zaistnienia zadanych w pierwszej fazie oceny zagrożeń naruszających poufność, dostępność i/lub integralność. Wynik z powtórnego szacowania ryzyka stanowi o ryzyku szczątkowym, które jest pozostałością po podjęciu wszystkich możliwych kroków zmierzających do unikania ryzyka, jego kontrolowania lub przeniesienia (transferu).

4) Plan postępowania ryzykiem.

Dla aktywów gdzie ryzyko było nieakceptowalne, formułuje się plan postępowania z ryzykiem, w którym określone zostają odpowiednie działania, odpowiedzialności oraz chronologiczne priorytety w celu redukcji ryzyka do poziomu bezpiecznego – akceptowalnego. W tym celu kierownictwo podmiotu wdraża adekwatne do wynikającego ryzyka zabezpieczenia oraz mierzy ich skuteczność. Ostatecznie zatwierdzone i wdrożone zabezpieczenia należy wpisać w dokument szacowania poziomu ryzyka w kolumnie działań zapobiegawczych i/lub korygujących w celu poddania aktywa ponownej ocenie ryzyka.

5) Wprowadzenie zmian.

Dokonywanie zmian w ocenie ryzyka odbywa się w wyniku każdorazowego podjęcia działań korygujących i/lub zapobiegawczych, zidentyfikowania nowego – realnego zagrożenia oraz dokonanego incydentu naruszającego bezpieczeństwo informacji. Zapisy sporządzone w ocenie ryzyka nie ulegają przedawnieniu i są trwałe, w związku z czym każde działanie mające na celu ponowną ocenę ryzyka bezwzględnie dokonuje się w kolejnym cyklu analizy. Szacowanie poziomu ryzyka należy przeprowadzić co najmniej raz w roku.

Szacowanie ryzyka oraz postępowanie z ryzykiem
Tabela nr 6

Lp.	Czynność na zbiorze danych	Zagrożenie	Prawdopodobieństwo	Podatność	Skutek-koszt	Wartość ryzyka	Kategoria (poziom ryzyka	Akceptacja ryzyka	Działania zapobiegawcze (postępowanie z ryzykiem)	Właściciele ryzyka