Elektronicznie podpisany przez:
Maciej Kędzierski
dnia 30 maja 2023 r.

ZARZĄDZENIE NR 0050.38.2023
WÓJTA GMINY WAPNO

z dnia 30 maja 2023 r.

w sprawie sprawie ochrony danych osobowych w Urzędzie Gminy Wapno

Na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016) Wójt Gminy Wapno zarządza, co następuje:

§ 1. W Urzędzie Gminy Wapno wprowadza się:

1. Politykę bezpieczeństwa, stanowiącą załącznik nr 1 do niniejszego zarządzenia;

2. Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, stanowiącą załącznik nr 2 do niniejszego zarządzenia.

§ 2. Zobowiązuje się wszystkich pracowników Urzędu Gminy Wapno do zapoznania się z niniejszym zarządzeniem i załącznikami do zarządzenia w terminie do 7 dni od daty wejścia w życie niniejszego zarządzenia oraz do przestrzegania zasad zawartych w tych dokumentach. Oświadczenie o zapoznaniu się należy wpiąć do akt osobowych pracowników Urzędu Gminy Wapno.

§ 3. Nadzór nad wykonaniem zarządzenia powierzam Inspektorowi Ochrony Danych w Urzędzie Gminy Wapno.

§ 4. Traci moc zarządzenie nr 0050.49.2019 Wójta Gminy Wapno z dnia 2 lipca 2019 r. w sprawie ochrony danych osobowych w Urzędzie Gminy Wapno.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Wapno

Maciej Kędzierski

Załącznik Nr 1 do zarządzenia Nr 0050.38.2023

Wójta Gminy Wapno

z dnia 30 maja 2023 r.

POLITYKA BEZPIECZEŃSTWA w URZĘDZIE GMINY WAPNO

Rozdział 1. Postanowienia ogólne, definicje

§ 1. 1. Polityka Bezpieczeństwa w Urzędzie Gminy Wapno jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach danych osobowych administrowanych przez Urząd Gminy Wapno.

2. Podstawami do opracowania i wdrożenia dokumentu są:

1) 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. Urz. UE L 119 z 4.05.2016);

2) ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

3. Przetwarzanie danych osobowych w Urzędzie Gminy Wapno jest dopuszczalne wyłącznie pod warunkiem przestrzegania 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. Urz. UE L 119 z 4.05.2016) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

4. Polityka Bezpieczeństwa ma zastosowanie do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

§ 2. Określenia i skróty użyte w Polityce Bezpieczeństwa Informacji oznaczają:

1) RODO - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016);

2) Dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"), w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

3) Przetwarzanie – oznacza operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnienie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

4) Ograniczenie przetwarzania – oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

5) Profilowanie – oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy i prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

6) Pseudonimizacja – oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi

i organizacyjnymi uniemożliwiającymi ich przypisanie, zidentyfikowanie lub możliwe do zidentyfikowania osobie fizycznej;

7) Zbiór danych – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

8) Administrator – Administrator Danych Osobowych – Wójt Gminy Wapno;

9) Podmiot przetwarzający – oznacza osobę fizyczną lub prawną, która przetwarza dane osobowe w imieniu administratora;

10) Odbiorca – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią;

11) Strona trzecia – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający, czy osoby, które – z upoważnienia administratora lub pomiotu przetwarzającego – mogą przetwarzać dane osobowe;

12) Zgoda – zgoda osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

13) Naruszenie ochrony danych osobowych – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesłanych, przechowywanych lub w inny sposób przetwarzanych;

14) Urząd – Urząd Gminy Wapno;

15) IOD – Inspektor Ochrony Danych;

16) Zespół wspomagający – osoby wyznaczone przez Administratora do wspierania IOD (Sekretarz Gminy i Informatyk).

Rozdział 2.
Obszary przetwarzania danych osobowych, wykaz zbiorów danych osobowych oraz przepływ danych między systemami

§ 3. 1. Miejscem przetwarzania danych osobowych jest budynek Urzędu Gminy w Wapnie, ul. Solna 1/3, 62-120 Wapno.

2. Obszar przetwarzania danych osobowych określony jest w „Wykazie pomieszczeń, w których przetwarzane są dane osobowe”, stanowiącym załącznik nr 1 do Polityki Bezpieczeństwa Informacji. Wykaz ten zawiera następujące informacje:

1) lokalizację budynku;

2) numer pomieszczenia i jego przeznaczenie;

3) wskazanie piętra budynku;

4) określenie referatu/stanowiska pracy użytkującego dane pomieszczenie;

5) wskazanie liczby osób pracujących w pomieszczeniu: wskazanie stanowisk i liczby osób;

6) określenie zabezpieczenia pomieszczenia.

3. Obszar przetwarzania danych oraz warunki ochrony tego obszaru określone zostały w załączniku nr 2 do Polityki Bezpieczeństwa Informacji „Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe”.

§ 4. 1. Rejestr czynności przetwarzania danych, zwany dalej rejestrem czynności, w Urzędzie Gminy określony został w odrębnym zarządzeniu Wójta.

2. Szczegółowe informacje dotyczące stosowanego sprzętu oraz oprogramowania danego systemu informatycznego są zawarte w podręczniku użytkownika danego systemu. Używane systemy w Urzędzie Gminy Wapno to: Systemy firmy RADIX sp. z o.o., w skład których wchodzą EBOI+, ELUD+, GOK+, KADRY+, PŁACE+, FKB+, FAKTURA+, KASA+, WIP+, WYB+, POGRUN+, KSN+, INFO+, POST+, KSN+. Pozostałe programy: Płatnik, Bestia, Pośredni, Wodnik, Źródło, SIO.

3. Podmiot przetwarzający odpowiedzialny na podstawie pracowniczych zakresów czynności za funkcjonowanie podległych sobie zbiorów danych ma obowiązek zgłoszenia zamiaru przetwarzania nowych czynności na danych osobowych w formie wniosku do IOD. Wzór wniosku stanowi załącznik nr 3 do polityki bezpieczeństwa. IOD po otrzymaniu ww. wniosku odnotowuje w rejestrze czynności przetwarzania nowoutworzoną czynność przetwarzania danych osobowych. IOD dokonuje jej rejestracji.

4. Analogicznie podmioty przetwarzające mają obowiązek zgłoszenia zaprzestania przetwarzania danych osobowych w istniejącym zbiorze danych w formie wniosku do IOD. Wzór wniosku stanowi załącznik nr 3 do polityki bezpieczeństwa. IOD po otrzymaniu ww. wniosku wykreśla z rejestru czynności przetwarzania zbiór danych osobowych, w którym zaprzestano przetwarzania danych osobowych.

§ 5. Przetwarzanie danych osobowych odbywa się na serwerach i na stacjach roboczych pracowników.

§ 6. 1. W ramach procesów przetwarzania danych, ma miejsce przepływ danych pomiędzy różnymi systemami informatycznymi.

2. Systemy informatyczne zasilają się wzajemnie o dane osobowe, tzn. są ze sobą powiązane. Schemat przepływu danych w systemach używanych w Urzędzie Gminy oraz schemat przepływu danych między systemami RADIX stanowi załącznik nr 4 do PBI.

3. Ze względu na zmiany ustawowe związane z pełnymi danymi osobowymi system ELUD+ spełniający obecnie funkcję Rejestru mieszkańców zostaje systematycznie zasilany danymi z rządowej aplikacji Źródło. Aplikacja ta pełni funkcję Systemu Rejestru Państwowego, w której rejestruje się wszystkie zdarzenia związane z mieszkańcem.

§ 7. W systemie informatycznym obowiązują zabezpieczenia na poziomie podstawowym. Szczegółowe omówienie środków zabezpieczenia technicznego i organizacyjnego znajduje się w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Wapno".

Rozdział 3.
Zarządzanie przetwarzaniem danych osobowych oraz czuwanie nad ich bezpieczeństwem

§ 8. 1. Administrator powołuje Inspektora Ochrony Danych (IOD).

2. Administrator powołuje Zespół wspomagający – osoby wyznaczone przez Administratora do wspierania IOD (Sekretarz Gminy i Informatyk).

3. Oprogramowaniem w Urzędzie Gminy Wapno zarządzają członkowie zespołu wspomagającego.

§ 9. W celu realizacji powierzonych zadań IOD w Urzędzie ma prawo:

1) kontrolować podmioty przetwarzające Urzędu w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe;
2) wydawać podmiotom przetwarzającym polecenia w zakresie bezpieczeństwa danych osobowych;
3) informować Administratora o wszystkich przypadkach wystąpienia incydentu bądź też naruszenia bezpieczeństwa danych osobowych;
4) żądać od wszystkich pracowników Urzędu wyjaśnień w sytuacjach incydentu lub naruszenia bezpieczeństwa danych osobowych;
5) zapoznawanać personel urzędu z przepisami RODO odnoszącymi się do ochrony danych osobowych oraz regulacjami wewnętrznymi, a w szczególności z polityką bezpieczeństwa informacji i instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. W razie nieobecności IOD i konieczności niezwłocznego zapoznania pracowników z wymaganiami prawnymi odnoszącymi się do ochrony danych osobowych, takiego zapoznania dokonuje członek zespołu wspomagającego.

§ 10. 1. Administrator jest właścicielem danych osobowych.

2. Administrator udziela upoważnienia podmiotowi przetwarzającemu do przetwarzania danych osobowych.

3. Na mocy upoważnienia podmiot przetwarzający staje się odpowiedzialny za dany zbiór danych osobowych.

4. Do obowiązków podmiotów przetwarzających należy w szczególności:

1) zarządzanie zbiorem danych osobowych w ramach zadań realizowanych przez dane stanowisko pracy;

2) zgłaszanie do IOD zamiaru utworzenia zbioru danych osobowych oraz informacji dotyczących zmian w zakresie i sposobach przetwarzania tego zbioru;

3) udostępnianie danych osobowych innemu podmiotowi zgodnie z przepisami prawa;

4) przestrzeganie obowiązków dotyczących obszaru przetwarzania i zastosowania zabezpieczeń zbiorów;

5) udział minimum raz na rok w szkoleniu z zakresu ochrony danych osobowych.

§ 11. 1. Członkowie zespołu wspomagającego wspomagają IOD w zakresie:

1) zapewnienia bezawaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych w Urzędzie;

2) nadzór nad naprawami, konserwacją i likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;

3) nadzór nad przeglądami, konserwacją, uaktualnianiem systemów służących do przetwarzania danych osobowych;

4) podejmowania natychmiastowych działań zabezpieczających stan systemu informatycznego w Urzędzie w przypadku otrzymania informacji o naruszeniu zabezpieczeń informatycznych;

5) przestrzegania zasad bezpieczeństwa w przypadku udostępniania danych osobowych;

6) przeciwdziałania dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;

7) podejmowania działań w przypadku incydentów i naruszeń w systemie zabezpieczeń;

8) nadzoru nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;

9) podejmowania działań w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego.

Rozdział 4.
Gromadzenie danych osobowych

§ 12. Dane osobowe przetwarzane w Urzędzie mogą być uzyskiwane bezpośrednio od osób, których te dane dotyczą, lub z innych źródeł, w granicach dozwolonych przepisami prawa.

§ 13. 1. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.

2. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

§ 14. Jeżeli dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem RODO albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

Rozdział 5.
Przetwarzanie danych osobowych

§ 15. 1. Przetwarzanie danych osobowych odbywa się zgodnie z rejestrem czynności przetwarzania danych osobowych podjętym osobnym zarządzeniem.

2. W przypadku pozyskania danych osobowych od strony trzeciej, wymagających utworzenia nowego zbioru, podmiot przetwarzający postępuje analogiczne jak w przypadku rejestracji nowych czynności przetwarzania opisanych w § 4 ust. 3.

3. Wnioski o udostępnienie informacji publicznej dotyczących danych osobowych wpływające do Urzędu kierowane są do podmiotów przetwarzających zgodnie z ich zakresem obowiązków.

Rozdział 6.
Obowiązek informacyjny

§ 16. 1. Podmioty przetwarzające, które zbierają i przetwarzają dane osobowe, są odpowiedzialne za poinformowanie osób, których dane osobowe przetwarzają, o:

1) swojej tożsamości, danych kontaktowych oraz gdy ma to zastosowanie, tożsamości i danych kontaktowych swojego przedstawiciela;

2) gdy ma to zastosowanie – danych kontaktowych IOD;

3) celu przetwarzania danych osobowych oraz podstawie prawnej przetwarzania;

4) jeżeli przetwarzanie odbywa się na podstawie RODO art. 6 ust. 1 lit. f) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;

5) informacjach o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

6) gdy ma to zastosowania – informacjach o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

2. Poza informacjami, o których mowa w ust. 1, podczas pozyskiwania danych osobowych, administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:

1) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe kryteria ustalania tego okresu;

2) informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

3) informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

4) informacje o prawie wniesienia skargi do organu nadzorczego;

5) informacje, czy podanie danych osobowych jest wymogiem ustawowym, umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą jest zobowiązana do ich podania i jakie są ewentualne konsekwencje nie podania danych;

6) informacje o profilowaniu lub też nieprofilowaniu, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosowanych informacji, o których mowa w ust. 2.

3. Ust. 1, 2 i 3 nie mają zastosowania, gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami.

4. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, Administrator podaje osobie, której dane dotyczą, analogicznie informacje jak w przypadku pozyskania od osoby, której te dane dotyczą (zawarte w ust. 1 i 2).

5. Wzór formularza stosowanego dla spełnienia obowiązków, o których mowa w ust. 1 i 2, stanowi załącznik nr 5 do Polityki Bezpieczeństwa.

Rozdział 7.
Ochrona przetwarzania danych osobowych

§ 17. 1. Do przetwarzania danych upoważnione są osoby posiadające aktualne upoważnienie nadane przez Administratora. Wzór upoważnienia określa załącznik nr 6 do Polityki Bezpieczeństwa Informacji.

2. Z wnioskiem (załącznik nr 7 do Polityki Bezpieczeństwa Informacji) do Administratora o nadanie lub cofnięcie uprawnień do przetwarzania danych osobowych występuję bezpośredni przełożony osoby zamierzającej podjąć przetwarzanie danych osobowych związanych z wykonywaniem obowiązków zgodnie z zakresem czynności na podejmowanym stanowisku oraz do obsługi systemu informatycznego w poszczególnych programach oraz w danym zakresie.

3. Administrator opiniuje złożone wnioski o wydanie upoważnienia do przetwarzania danych osobowych i wydaje upoważnienie zgodne z zakresem pracy wnioskodawcy. Po zaopiniowaniu wniosku przez Administratora druk upoważnienia imiennego do przetwarzania danych osobowych (załącznik nr 6) do podpisu Administratora przygotowuje IOD.

4. Upoważnienie do przetwarzania danych osobowych wydawane jest w trzech egzemplarzach. Jeden egzemplarz przechowywany jest w aktach osobowych pracownika, drugi w dokumentacji prowadzonej przez IOD a trzeci dla podmiotu przetwarzającego.

5. IOD prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Wzór ewidencji stanowi załącznik nr 8 do Polityki Bezpieczeństwa Informacji.

6. Przetwarzać dane osobowe mogą podmioty przetwarzające wyłącznie po zapoznaniu się z przepisami ogólnymi odnoszącymi się do ochrony danych osobowych oraz regulacjami wewnętrznymi: z polityką bezpieczeństwa informacji, instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz rejestrem czynności przetwarzania danych osobowych. Za zapoznanie się podmiotów przetwarzających z przepisami odpowiada IOD, a w razie nieobecności IOD - członek zespołu wspomagającego. Pracownik po zapoznaniu się z ww. treściami i ewentualnym zasięgnięciu wyjaśnień ze strony IOD lub członka zespołu wspomagającego podpisuje oświadczenie, którego wzór stanowi załącznik nr 9 do Polityki Bezpieczeństwa Informacji.

§ 18. 1. Powierzenie przetwarzania danych osobowych może odbyć się po uprzednim podpisaniu umowy powierzenia przetwarzania danych osobowych pomiędzy Administratorem a Zleceniobiorcą. Wzór umowy stanowi załącznik nr 10.

2. IOD przygotowuje projekt umowy powierzenia danych osobowych innemu podmiotowi.

Rozdział 8.
Zarządzanie ryzykiem bezpieczeństwa danych osobowych

§ 19. 1. Ryzyko w zakresie bezpieczeństwa informacji, w tym danych osobowych, definiuje się jako prawdopodobieństwo wystąpienia zagrożeń i powstanie szkód, zniszczeń oraz przerw lub zakłóceń prawidłowego funkcjonowania systemu tradycyjnego oraz systemu informatycznego, w których przetwarza się dane osobowe.

2. Zarządzanie ryzykiem jest procesem identyfikacji zasobów, odpowiadających im podatności i zagrożeń, oceny prawdopodobieństwa ich wystąpienia, wielkości potencjalnych strat oraz przeciwdziałania i określenia kryteriów akceptowalności ryzyka.

3. Zarządzanie ryzykiem obejmuje możliwie jak najszybszą identyfikację ryzyka związanego z planowanym działaniem, ocenę stopnia wpływu ryzyka na uzyskane wyniki lub cele oraz zastosowanie odpowiednich środków kontroli ryzyka.

4. Proces zarządzania ryzykiem w zakresie bezpieczeństwa informacji, odnoszącym się do działalności Urzędu Gminy Wapno, dokonywany jest przez IOD we współpracy z osobami odpowiedzialnymi za poszczególne obszary działalności (właścicielami ryzyka) oraz Informatykiem w zakresie systemu informatycznego.

5. Narzędziem wsparcia w tym procesie jest Arkusz zarządzania ryzykiem w zakresie bezpieczeństwa danych osobowych zawierający ryzyka zidentyfikowane dla Urzędu Gminy Wapno. Katalog zidentyfikowanych ryzyk jest zbiorem otwartym. Wzór arkusza stanowi załącznik nr 11 do Polityki Bezpieczeństwa Informacji.

6. Pracownicy, do których przypisano poszczególne ryzyka (właściciele ryzyka), określają prawdopodobieństwo wystąpienia zidentyfikowanych ryzyk oraz ich skutek i wpływ na realizowane zadania z jednoczesnym wskazaniem istniejących mechanizmów kontroli i propozycją reakcji na ryzyko.

7. Lista możliwych do zastosowania mechanizmów kontroli redukujących ryzyko stanowi załącznik nr 12 do Polityki Bezpieczeństwa Informacji. Lista jest otwartym katalogiem i może ulec modyfikacji.

8. Wypełnione arkusze zarządzania ryzykiem przekazywane są do IOD. Na ich podstawie IOD, w przypadku ryzyk dotyczących bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym w porozumieniu z Informatykiem, opracowuje roczne sprawozdanie, które w postaci raportu o zidentyfikowanych ryzykach przekazuje Administratorowi.

§ 20. 1. Niezależnie od corocznej oceny ryzyka, IOD przeprowadza ocenę ryzyka po każdorazowym wystąpieniu incydentu oraz każdorazowej zmianie mogącej wpływać na poziom ryzyka, w tym szczególnie zmianie struktury organizacyjnej.

2. Niezwłocznie po wystąpieniu incydentu, IOD przedstawia Administratorowi wyniki oceny zidentyfikowanych ryzyk wraz z propozycjami działań korygujących i zapobiegawczych, do których należy w szczególności: określenie zadań do realizacji, zdefiniowanie odpowiedzialności, ram czasowych oraz propozycji zmian celem poprawy bezpieczeństwa informacji.

3. Na podstawie raportów i sprawozdań otrzymanych od IOD Administrator podejmuje ostateczną decyzję w zakresie realizacji działań zapewniających ochronę przetwarzanych informacji.

4. Do działań wskazanych w ust. 3 należy w szczególności:

a) zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia,

b) utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację,

c) przeprowadzenie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy,

d) podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji,

e) dokonanie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt d),

f) zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:

- zagrożenia bezpieczeństwa informacji,
- skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
- stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich,

g) zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:

- monitorowanie dostępu do informacji,
- czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
- zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji,

h) ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,

i) zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie,

j) zawieranie w umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,

k) ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych,

l) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

- dbałości o aktualizację systemu operacyjnego,
- minimalizowaniu ryzyka utraty informacji w wyniku awarii,
- ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
- stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,

- zapewnieniu bezpieczeństwa plików systemowych,
- redukcji ryzyka wynikającego z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
- niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
- kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i Polityką Bezpieczeństwa Informacji,

m) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w sposób, umożliwiający szybkie podjęcie działań korygujących,

n) zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

§ 21. 1. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

a) próby naruszenia ochrony danych,

b) ataki hakerskie w celu pozyskania danych osobowych lub zablokowania systemów informatycznych,

c) awarie sprzętu lub uszkodzone oprogramowanie,

d) kradzież sprzętu lub nośników z ważnymi danymi,

e) usiłowanie zakłóceń działania systemu teleinformatycznego,

f) inne skutkujące utratą danych osobowych bądź wejściem w ich posiadanie osób nieuprawnionych.

2. Do typowych incydentów zagrażających bezpieczeństwu danych osobowych należą:

a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,

b) niewłaściwe zabezpieczenie sprzętu IT i oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,

c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka, ochrony haseł, niezamykanie pomieszczeń),

d) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, nieumyślne skasowanie danych),

e) umyślne incydenty (włamania do systemu informatycznego lub pomieszczeń, kradzież danych, wyciek informacji, świadome zniszczenie dokumentów, działania wirusów komputerowych).

3. Do typowych źródeł informacji o incydentach, zagrożeniach lub słabościach systemu zalicza się:

a) zgłoszenia od użytkowników,

b) alarmy z systemów informatycznych,

c) analizy incydentów,

d) wyniki audytu/kontroli.

§ 22. Każdy pracownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować IOD lub Informatyka. Protokół uchybienia/zagrożenia stanowi załącznik nr 13 do PBI. Zasady działania w takich przypadkach określa poniższa tabela:

Kod uchybienia lub naruszenia	Uchybienie i zagrożenie nieświadome wewnętrzne i zewnętrzne	Postępowanie w przypadku uchybienia lub zagrożenia
1	Pomieszczenie, w którym przechowywane są dane osobowe pozostaje bez nadzoru	Należy zabezpieczyć dane osobowe oraz powiadomić IOD, który powiadamia Administratora. IOD sporządza protokół
2	Komputer nie jest zabezpieczony hasłem	Należy zabezpieczyć dane osobowe oraz powiadomić Informatyka i IOD, który powiadamia Administratora i sporządza protokół

3	Dostęp do danych mają osoby nieuprawnione	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić IOD, który powiadamia Administratora i sporządza protokół
4	Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym	Należy powiadomić Informatyka i IOD. IOD we współpracy z Informatykiem powinien sprawdzić system uwierzytelniania oraz sprawdzić, czy nie doszło do kradzieży lub zniszczeń danych. Na podstawie informacji uzyskanych od Informatyka, IOD powiadamia Administratora i sporządza protokół
5	Próba kradzieży danych osobowych poprzez zewnętrzny nośnik danych	Należy nie dopuścić do kradzieży danych i powiadomić IOD i Informatyka, który w porozumieniu z IOD powinien zabezpieczyć nośnik danych i powiadomić Administratora. IOD sporządza protokół
6	Próba kradzieży danych osobowych w formie papierowej	Należy nie dopuścić do kradzieży danych osobowych i powiadomić IOD. IOD powinien zabezpieczyć dane i powiadomić Administratora. IOD powiadamia Administratora i sporządza protokół
7	Nieuprawniony dostęp do danych osobowych w formie papierowej	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić IOD który sporządza protokół i powiadamia Administratora
8	Dane osobowe przechowywane są w niezabezpieczonym pomieszczeniu	Należy powiadomić IOD, który powinien zabezpieczyć pomieszczenie, powiadomić Administratora i sporządzić protokół
9	Próba włamania do pomieszczenia/budynku	Należy zabezpieczyć dowody i powiadomić IOD. IOD sprawdza stan uszkodzeń, zabezpiecza dowody i wzywa policję. IOD powiadamia Administratora i sporządza protokół
10	Działanie zewnętrzne aplikacji, wirusów, złośliwego oprogramowania	Należy zawiadomić Informatyka i IOD. Informatyk powinien przeprowadzić audyt systemów zabezpieczeń, a w szczególności systemów antywirusowych i firewall. Informatyk przekazuje wynik audytu IOD, który powinien ocenić, czy nie doszło do utraty danych osobowych i w zależności od tego sporządzić protokół. IOD powiadamia Administratora
11	Brak aktywnego oprogramowania antywirusowego	Należy powiadomić Informatyka. Informatyk powinien zaktualizować lub nabyć oprogramowanie antywirusowe i powiadomić IOD. IOD powiadamia Administratora i sporządza protokół
12	Zniszczenie lub modyfikacja danych osobowych w formie papierowej	Należy zabezpieczyć dowody i powiadomić IOD. IOD sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia Administratora. IOD sporządza protokół
13	Zniszczenie lub modyfikacja danych osobowych w systemie informatycznym	Należy zabezpieczyć dowody i powiadomić Informatyka. Informatyk sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia IOD. IOD powiadamia Administratora i sporządza protokół
14	Uszkodzenie komputerów, nośników danych	Należy powiadomić IOD, który w porozumieniu z Informatykiem powinien ocenić w wyniku czego doszło do zniszczenia i przywrócić dane z kopii zapasowej. IOD powiadamia Administratora i sporządza protokół
15	Próba nieprawidłowej interwencji przy	Należy uniemożliwić dostęp osób do sprzętu

	sprzęcie komputerowym	komputerowego oraz powiadomić Informatyka, który powiadamia IOD. IOD powiadamia Administratora i sporządza protokół
16	Zdarzenie losowe	IOD powoduje oszacowanie strat, powiadamia Administratora i sporządza protokół

§ 23. Przepisy niniejszego rozdziału stosuje się w przypadku:

1) stwierdzenia naruszenia zabezpieczenia systemu informatycznego w obszarze danych osobowych;

2) podejrzenia naruszenia bezpieczeństwa danych osobowych ze względu na stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci komputerowej.

§ 24. Zasady postępowania w przypadku naruszenia bezpieczeństwa danych osobowych obowiązują wszystkie podmioty przetwarzające.

§ 25. Naruszeniem zabezpieczenia systemu informatycznego, przetwarzającego dane osobowe jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

1) nieautoryzowany dostęp do danych;

2) nieautoryzowane modyfikacje lub zniszczenie danych;

3) udostępnienie danych nieautoryzowanym podmiotom;

4) nielegalne ujawnienie danych;

5) pozyskiwanie danych z nielegalnych źródeł.

§ 26. 1. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie IOD lub członka Zespołu Wspomagającego, a następnie postępować stosownie do podjętej przez niego decyzji.

2. Zgłoszenie naruszenia dokonuje się poprzez formularz zgłoszenie dostępny na stronie www.uodo.gov.pl.

§ 27. 1. IOD podejmuje działania mające na celu:

1) minimalizację negatywnych skutków zdarzenia;

2) wyjaśnienie okoliczności zdarzenia;

3) zabezpieczenie dowodów zdarzenia;

4) umożliwienie dalszego bezpiecznego przetwarzania danych.

2. Dla realizacji celów określonych w pkt. 1 IOD ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, w szczególności:

1) żądania wyjaśnień od pracowników;

2) korzystania z pomocy konsultantów;

3) nakazania przerwania pracy.

§ 28. Odmowa udzielenia wyjaśnień lub współpracy z IOD traktowana będzie, jako naruszenie obowiązków pracowniczych.

§ 29. IOD po zakończeniu działań związanych z naruszeniem ochrony danych opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, ograniczające możliwość wystąpienia zdarzenia w przyszłości; wzór raportu końcowego stanowi załącznik nr 14 do Polityki Bezpieczeństwa Informacji.

Rozdział 9.
Poczta elektroniczna

§ 30. 1. W sprawach służbowych do korespondencji mailowej używa się wyłącznie służbowego adresu email przydzielonego przez Informatyka.

2. Konto poczty elektronicznej zakładane jest na dane stanowisko pracy.

3. Pracownicy dane do logowania otrzymują od Informatyka.

4. Obowiązkiem Pracownika jest przy pierwszym logowaniu zmienić hasło.

5. W przypadku nowozatrudnionej osoby na stanowisko hasło do poczty mailowej nadaje Informatyk.

6. W przypadku zakończenia stosunku pracy, Informatyk blokuje dostęp do poczty elektronicznej, zmienia hasło i udostępnia je nowemu pracownikowi obejmującemu stanowisko.

7. Użytkownik poczty w każdej chwili ma prawo do zmiany hasła logowania. W przypadku zapomnienia hasła na prośbę pracownika zostaje ustalone nowe hasło do konta mailowego.

8. Nie wykorzystuje się służbowej poczty mailowej do celów prywatnych.

9. W przypadku likwidacji stanowiska pracy, adres mailowy zostaje zablokowany.

10. Podczas korzystania z poczty pracownik jest zobowiązany jest do:

1) zwracania szczególnej uwagi na pochodzenie wiadomości mailowej oraz zawartych w niej załącznikach;

2) zwracania szczególnej uwagi na odnośniki (linki) do stron internetowych;

3) wiadomości uznane za niebezpieczne pracownik winien trwale usuwać;

4) przy wysyłaniu wiadomości pracownik winien zwrócić szczególną uwagę na adresata danej wiadomości;

5) unikania korespondencji seryjnej;

6) nieprzesyłania w jednym mailu hasła do zaszyfrowanej wiadomości;

7) wysyłania wiadomości z potwierdzeniem otrzymania maila.

Rozdział 10.
Zasady korzystania z bankowości elektronicznej

§ 31. 1. Podmiot przetwarzający uprawniony do wykonywania rejestracji przelewów bankowych zobowiązany jest do:

a) regularnej zmiany hasła w bankowości elektronicznej,

b) nieprzechowywania hasła w formie pisemnej wraz z loginem,

c) udostępniania danych do logowania na swoim koncie,

d) używania karty kryptograficznej innego pracownika,

e) opuszczania stanowiska pracy bez wylogowania się i zamknięcia przeglądarki internetowej,

f) używania dedykowanej przeglądarki internetowej,

g) zapoznania się z zasadami bezpieczeństwa teleinformatycznego przekazanego przez bank, który obsługuje bankowość elektroniczną,

h) nieudostępniania danych o operacjach wykonywanych na kontach,

i) informowania Administratora o problemach przy logowaniu i pracy,

j) logowania się tylko w miejscu pracy.

2. W przypadku zakończenia stosunku pracy, podmiot przetwarzający zwraca się z wnioskiem do Administratora o zabranie uprawnień do bankowości elektronicznej oraz zdaje kartę kryptograficzną.

Rozdział 11.
Zasady dotyczące dokonywania transmisji i utrwalania obrad Rady Gminy Wapno

§ 32. 1. Administrator dokonuje transmisji i utrwalania obrad rady gminy zgodnie z art. 20 ust. 1b ustawy o samorządzie gminnym (Dz. U. 2023 r. poz. 40 ze zm.).

2. Obrady rady gminy są transmitowane i utrwalane za pomocą urządzeń rejestrujących obraz i dźwięk. Nagrania obrad są udostępniane w Biuletynie Informacji Publicznej i na stronie internetowej gminy.

3. Przed rozpoczęciem obrad, Przewodniczący Rady Gminy Wapno:

a) informuje radnych i innych uczestników, iż obrady są transmitowane na żywo oraz informuje o obowiązkach w zakresie nieujawniania, bez uzasadnionej potrzeby, danych osobowych osób niebędących funkcjonariuszami publicznymi, niepełniącymi funkcji publicznej, ani niezwiązanymi z tą funkcją,

b) realizuje obowiązek informacyjny wynikający z art. 13 ust. 1 i 2 RODO,

c) Administrator dokonuję teletransmisji sesji poprzez firmę obsługującą, której serwer znajduje się w na terytorium Europejskiego Obszaru Gospodarczego. W przypadku umieszczenia nagrania na serwerze państwa trzeciego należy uwzględnić wymagania stawiane w tym zakresie przez art. 44-49 RODO,

d) nagranie umieszczane jest na serwerze zewnętrznym,

e) firma obsługująca, która przygotowuje napisy do nagrania lub nagranie z takiego posiedzenia, w związku z jego udostępnieniem publicznym – zobowiązana jest do ochrony prawa do prywatności osób fizycznych, w tym ochrony ich danych osobowych. W związku z powyższym, jeżeli przy przygotowaniu ww. materiałów pojawią się dane osobowe osób niebędących funkcjonariuszami publicznymi, niepełniącymi funkcji publicznych ani niezwiązanych z tymi funkcjami, powinny być one anonimizowane. Powyższe dotyczy w szczególności danych wrażliwych, które anonimizować należy w sposób bezwzględny,

f) osoba wyznaczona przez Administratora okresowo dokonuje przeglądu nagrań z posiedzeń rady gminy, pod kątem ewentualnych nieprawidłowości związanych z brakiem anonimizacji danych osobowych osób prywatnych.

Rozdział 12.
Wewnętrzne środki bezpieczeństwa obowiązujące w Urzędzie Gminy Wapno

§ 33. 1. W celu zwiększenia bezpieczeństwa komputerów użytkowanych w Urzędzie wprowadza się rejestr haseł dla poszczególnych kont użytkowników.

2. Rejestr ten zawiera:

a) imię i nazwisko użytkownika;

b) konto użytkownika;

c) hasło użytkownika;

d) datę nadania hasła;

e) podpis użytkownika;

f) w przypadku blokady komputera, data blokady i podpis Informatyka.

3. Hasło musi zawierać co najmniej 8 znaków, w tym małe i duże litery, cyfry lub znaki specjalne.

4. Hasła użytkowników są zmieniane co 30 dni kalendarzowych.

5. Odpowiedzialną osobą na prowadzenie rejestru jest Informatyk, w razie jego nieobecności Sekretarz Gminy.

6. Po każdorazowej zmianie hasła Użytkownicy zobligowani są zgłosić zmianę hasła osobie odpowiedzialnej za prowadzenie rejestru.

7. Hasło do komputera może być udostępnione tylko i wyłącznie pracownikowi, który zastępuje nieobecną osobę.

8. Przy dłuższej nieobecności Użytkownika, Administrator zleca Informatykowi zablokowanie komputera do czasu powrotu pracownika do pracy.

9. Wzór rejestru stanowi Załącznik Nr 15.

§ 34. 1. W Urzędzie prowadzona jest Ewidencja Pobranych i Zdanych Kluczy do Pomieszczeń.

2. Ewidencja zawiera:

a) Datę pobrania/zdania klucza;

b) Nr biura;

c) Imię i nazwisko pobierającego/zdającego;

d) Godzinę pobrania klucza;

e) Godzinę zdania klucza;

f) Podpis osoby pobierającej/zdającej.

3. Za prowadzoną ewidencję odpowiedzialny jest Sekretarz Gminy Wapno.

Wykaz pomieszczeń Urzędu Gminy Wapno, w których przetwarzane są dane osobowe

LP.	**Lokalizacja Adres i numer budynku**	**Numer i przeznaczenie pomieszczenia***	**Piętro**	**Nazwa referatu/stanowiska pracy użytkującego pomieszczenie**	**Osoby pracujące w pomieszczeniu****	**Zabezpieczenie pomieszczenia*****
1.	**2.**	**3.**	**4.**	**5.**	**6.**	**7.**
1.						

*Należy podać numer pomieszczenia i jego przeznaczenie np. pokój biurowy, archiwum, kancelaria, serwerownia, biuro przepustek.

** Należy podać same stanowiska i liczbę osób bez imion i nazwisk.

*** Należy podać sposób zabezpieczenia pomieszczenia np. drzwi zamykane na klucz, kraty w oknach, pomieszczenie monitorowane, kontrola dostępu itp.

Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe

1. Administrator jest odpowiedzialny za należyte zabezpieczenie fizyczne zasobów danych osobowych.

2. IOD zobowiązany jest przeprowadzać bezpośrednią kontrolę stanu zabezpieczeń fizycznych danych osobowych oraz zgłaszać Administratorowi uwagi i możliwości wdrożenia nowych rozwiązań mających na celu lepsze zabezpieczenie danych.

3. Obszarem, w którym przetwarzane są dane osobowe jest Urząd Gminy Wapno, z siedzibą w Wapnie przy ul. Solnej 1/3.

4. IOD jest odpowiedzialny za prowadzenie i uaktualnianie wykazu pomieszczeń, w których przetwarzane są dane osobowe.

5. Pomieszczenia, w których przetwarzane są dane osobowe, muszą być zamykane na czas nieobecności w nich podmiotów przetwarzających.

6. Podmiot przetwarzający zabezpiecza obszar przetwarzania danych.

7. Budynek i pomieszczenia Urzędu Gminy Wapno posiadają następujące zabezpieczenia:

1) drzwi zewnętrzne (2 szt.) zaopatrzone są w podwójne zamki patentowe;

2) dostęp (klucze) do drzwi głównych wejściowych posiadają 2 osoby;

3) klucze zapasowe do wszystkich pomieszczeń znajdują się w sekretariacie;

4) klucze do pomieszczeń biurowych pobierane i zdawane są w sekretariacie. Fakt ten jest odnotowywany w ewidencji pobranych i zdanych kluczy do pomieszczeń;

5) drzwi do pomieszczeń zabezpieczone są zamkami patentowymi;

6) wszystkie szafy na dokumenty wyposażone są w zamki patentowe;

7) w wyniku uruchomienia alarmu aktywują się powiadamiania drogą sms-ową. Powiadamiani są Wójt Gminy, Sekretarz Gminy, sprzątaczka oraz pracownik gospodarczy.

8. Pozostawianie osób trzecich w pomieszczeniach, o których mowa w ust. 3, bez nadzoru podmiotu przetwarzającego jest zabronione.

Załącznik nr 3 do Polityki Bezpieczeństwa

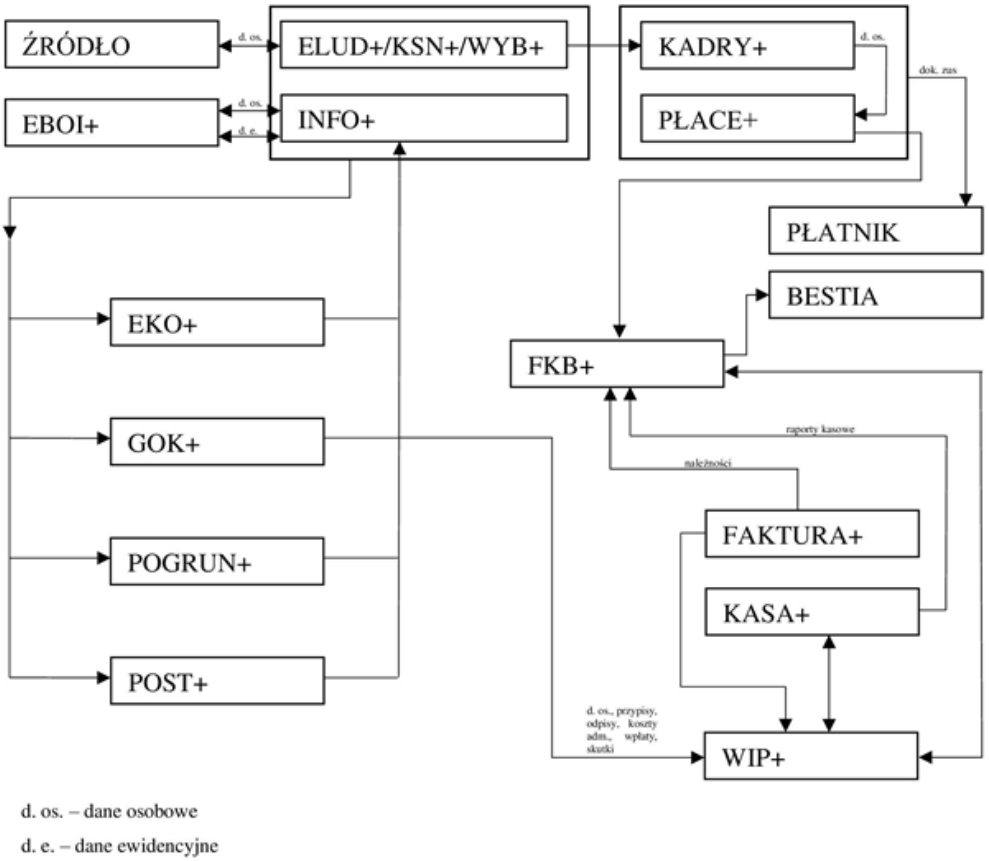
Wapno, dnia ……..….

Wniosek
o wpisanie/usunięcie do rejestru czynności przetwarzania następujących czynności wykazanych zgodnie z tabelą poniżej

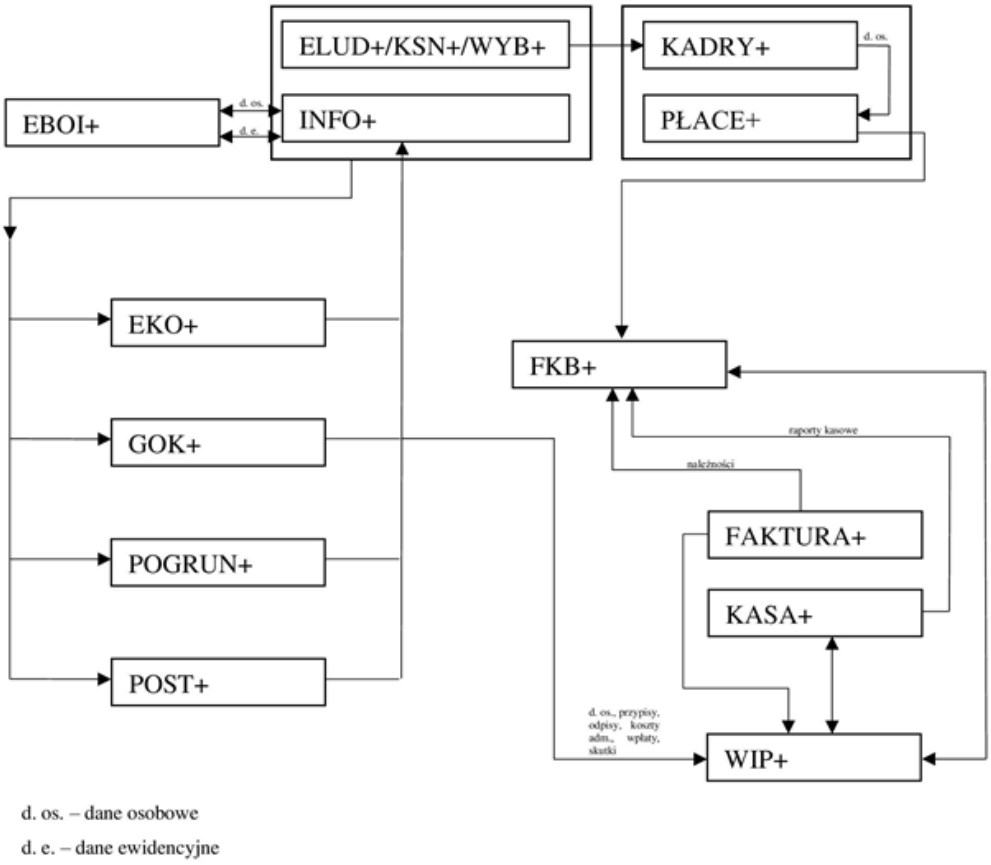
Lp.	Nazwa czynności przetwarzania	Jednostka organizacyjna	Cel przetwarzania	Kategorie osób, których dane dotyczą	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych	Kategorie odbiorców	Nazwa systemu lub oprogramowania	Opis technicznych i organizacyjnych środków bezpieczeństwa

…….....

data i podpis wnioskującego do IOD)



Schemat przepływu danych w systemach używanych w Urzędzie Gminy Wapno



Przepływ danych między systemami pakietu RADIX

…….

miejscowość, data

……..……

imię i nazwisko

……

adres zamieszkania

Oświadczenie zapoznania z klauzulą informacyjną

Oświadczam, że zgodnie z art. 13 ust 1 i 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* (Dz. Urz. UE L 119 z 2016 r.) **zapoznałem/zapoznałam**[1)] się z treścią klauzuli informacyjnej, w tym z przysługującym prawie dostępu do treści moich danych oraz ich poprawiania, jak również, że podanie tych danych było dobrowolne.

……..

podpis osoby składającej oświadczenie

[1)] nie potrzebne skreślić.

Załącznik nr 6 do Polityki Bezpieczeństwa

Wapno, dnia ……. r.

Pan/Pani ……

zatrudniony/a w ……

na stanowisku: ……..

UPOWAŻNIENIE
do przetwarzania danych osobowych

Upoważniam Panią/Pana **…….**

(imię i nazwisko)

zatrudnioną/zatrudnionego w **……**

(nazwa komórki organizacyjnej)

do przetwarzania danych osobowych, w celach związanych z wykonywaniem obowiązków zgodnie z zakresem na stanowisku: **…….** oraz poleceniami służbowymi oraz do obsługi systemu informatycznego w następujących programach w zakresie:

·Odczytu danych ……

·Zapisu i modyfikacji danych……

·Kasowania danych……..…….

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie tradycyjnej (kartoteki, ewidencje, rejestry, spisy itp.*) i elektronicznej zgodnie z posiadanym zakresem czynności.

……

(podpis Administratora)

Otrzymuje:

…….

Załącznik nr 7 do Polityki Bezpieczeństwa

Wapno, dnia …….. r.

Wniosek
o nadanie/cofnięcie uprawnień do przetwarzania danych osobowych

Na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1) wnoszę o nadanie/cofnięcie uprawnień dla

Pani/Pana

……

Zajmującego stanowisko

…….

do przetwarzania danych osobowych w celach związanych z wykonywaniem obowiązków zgodnie z zakresem czynności na stanowisku ……. oraz do obsługi systemu informatycznego w następujących programach w zakresie:

·**Odczytu danych ……**

·**Zapisu i modyfikacji danych……**

·**Kasowania danych……..……..**

na okres od …… r. do ……

.....

(data i podpis wnioskującego do Administratora)

Wyrażam zgodę / nie wyrażam zgody* (skreślić niepotrzebne)

.....

(data i podpis Administratora)

Załącznik nr 8 do Polityki Bezpieczeństwa

Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych w Urzędzie Gminy Wapno

Lp.	Imię i nazwisko	Data zapoznania z dokumentem	Stanowisko / funkcja	Typ umowy		Zakres rzeczowy uprawnienia oraz nadany identyfikator do systemu informatycznego	Ramy czasowe	
				Pracownik	Praktyka/Staż		od ….	do ….
1								
2								
3								
4								

Załącznik nr 9 do Polityki Bezpieczeństwa

Wapno, dnia …….

OŚWIADCZENIE

Ja niżej podpisany(a) …… oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał(a) dostęp w związku z wykonywaniem:

Rodzaj zadań	Właściwe zaznaczyć
Zadań i obowiązków wynikających z umowy o pracę zarówno w trakcie wykonywania umowy, jak i po jej rozwiązaniu	
Zadań wynikających z umowy cywilnoprawnej zarówno w trakcie wykonywania umowy, jak i po jej wygaśnięciu	
Zadań wynikających z umowy o staż/praktyki zarówno w trakcie wykonywania umowy, jak i po jej wygaśnięciu	

*Właściwe zaznaczyć.

Zobowiązuję się przestrzegać regulaminów, instrukcji i procedur obowiązujących w Urzędzie Gminy Wapno dotyczących ochrony danych osobowych, w szczególności oświadczam, że bez upoważnienia służbowego nie będę wykorzystywał(a) danych osobowych ze zbiorów Urzędu Gminy Wapno.

Oświadczam, że zostałem(am) poinformowany(a) o obowiązujących w Urzędzie Gminy Wapno zasadach dotyczących przetwarzania danych osobowych.

…… ……

(miejsce złożenia oświadczenia) *(data złożenia oświadczenia)*

……..……

(podpis osoby składającej oświadczenie)

Załącznik nr 10 do Polityki Bezpieczeństwa

Umowa powierzenia przetwarzania danych osobowych

zawarta w dniu ..... r. pomiędzy:

…….

z siedzibą w .....,

zarejestrowaną/ym w ..... pod numerem KRS .....,

numer NIP ....., oraz numer REGON .....,

reprezentowaną/ym przez: .....,

zwaną/ym dalej **Zleceniodawcą**, a…….……

z siedzibą w .....,

zarejestrowaną/ym w .....

pod numerem KRS .....,

numer NIP .....

oraz numer REGON .....,

reprezentowaną/ym przez: .....,

zwaną/ym dalej **Zleceniobiorcą**.

§ 1. Oświadczenia stron

1. Zleceniodawca powierza Zleceniobiorcy przetwarzanie danych osobowych w zakresie i celu objętym niniejszą umową.

2. Zleceniodawca oświadcza, że jest administratorem danych osobowych, które przetwarza zgodnie z obowiązującymi przepisami prawa. Zleceniodawca oświadcza ponadto, że zawiera niniejszą umowę w celu bezpośrednio związanym z jego działalnością gospodarczą lub zawodową.

3. Zleceniobiorca oświadcza, iż dysponuje odpowiednimi środkami, w tym należytymi zabezpieczeniami umożliwiającymi przetwarzanie danych osobowych zgodnie 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 ,(dalej zwane rozporządzeniem),

§ 2. Zakres i cel przetwarzania danych osobowych

1. Zleceniobiorca może przetwarzać dane osobowe przekazane przez Zleceniodawcę wyłącznie w zakresie i w celu określonych w niniejszej umowie.

2. Dane osobowe będą przetwarzane przez Zleceniobiorcę tylko i wyłącznie w celu ……*[wskazać cel przetwarzania]*.

3. Zakres przetwarzania obejmuje następujące dane osobowe …….. *[wskazać zakres przetwarzania]*

4. Poprzez przetwarzanie danych rozumie się jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

§ 3. Zobowiązania podmiotu, któremu powierzono przetwarzanie danych osobowych

1. Zleceniobiorca zobowiązuje się przed przystąpieniem do przetwarzania powierzonych przez Zleceniodawcę danych wdrożyć i utrzymywać przez czas przetwarzania wszelkie środki i zabezpieczenia związane z przetwarzaniem danych, zgodnie z wymaganiami ustawy oraz rozporządzenia.

2. Zleceniobiorca może powierzać przetwarzanie powierzonych przez Zleceniodawcę danych osobowych innym podmiotom, takim jak: ……. *[wskazać określone podmioty]*.

3. Zleceniobiorca odpowiada za wszelkie wyrządzone osobom trzecim szkody, które powstały w związku z nienależytym przetwarzaniem przez Zleceniobiorcę powierzonych danych osobowych.

4. Zleceniobiorca nie jest odpowiedzialny za udostępnienie powierzonych danych osobowych osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem tych danych osobowych w przypadku, gdy przyczyną powyższego jest działanie bądź zaniechanie Zleceniodawcy

§ 4. Postanowienia końcowe

1. W sprawach nieuregulowanych niniejszą umową zastosowanie znajdują przepisy ustawy oraz powiązanych z nią aktów wykonawczych, a także rozporządzenia i kodeksu cywilnego.

2. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

3. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

.....	.....
Zleceniodawca	Zleceniobiorca

Załącznik nr 11 do Polityki bezpieczeństwa

ARKUSZ ZARZĄDZANIA RYZYKIEM

Wapno, dnia ……..

Nazwa działu ……

Właściciel ryzyka……

Lp.	Ryzyko	Prawdopodobieństwo * wystąpienia ryzyka (skala 1-4pkt)	Skutek ** (skala 1-4 pkt)	Poziom wpływu ryzyka na bezpieczeństwo (istotność ryzyka) *** (skala1-16pkt)	Ocena ryzyka- wynik (dopuszczalność)	Istniejące mechanizmy kontroli	Propozycje reakcji na ryzyko	Uwagi
1	Nieuprawniony dostęp do pomieszczenia, w którym są przetwarzane dane osobowe							
2	Ujawnienie haseł dostępu do stanowiska komputerowego, na którym przetwarzane są dane osobowe							
3	Nieuprawnione przeniesienie informacji zawierających dane osobowe							
4	Utrata nośnika zawierającego dane osobowe							
5	Nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym							
6	Atak wirusa							
7	Klęska żywiołowa, wypadek, zdarzenie, w wyniku których utracono poufność danych osobowych							
8	Włamanie do systemu komputerowego							
9	Nielegalny dostęp do danych osobowych, w tym do stanowiska							

	komputerowego lub urządzenia mobilnego							
10	Błędy i pomyłki użytkowników							
11	Brak mechanizmów uniemożliwiających skasowanie lub zmianę logów przez administratora lub innego użytkownika							
12	Awaria sprzętu							
13	Brak w wykorzystywanych aplikacjach mechanizmów zapewniających integralność danych							
14	Brak kontroli nad dokumentami wykonywanymi na stanowisku komputerowym w zakresie ich kopiowania i drukowania							
15	Nieuprawnione wprowadzanie zmian w treści dokumentu zawierającego dane osobowe							
16	Błędy programowania lub sprzętu							

LEGENDA

*sposób oceny prawdopodobieństwa wystąpienia ryzyka

Prawdopodobieństwo wystąpienia ryzyka	Ilość punktów	Przesłanki
Bardzo wysokie (81-100%)	4	Przewiduje się, że zdarzenie z pewnością wystąpi w ciągu roku
Wysokie (61-80%)	3	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się wielokrotnie w ciągu roku
Średnie (21-60%)	2	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się raz lub kilka razy w ciągu roku
Niskie (0-20%)	1	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się raz lub nie zdarzy się w ciągu roku

**sposób oceny skutku ryzyka

Skutek wystąpienia ryzyka	Ilość punktów	Przesłanki
Bardzo wysoki	4	Poważna niezgodność z przepisami prawa. Brak procedur dla danego

		procesu. Olbrzymie zakłócenia pracy. Znaczny uszczerbek na wizerunku. Zagrożenia spowodują brak zachowania ciągłości procesów działania, utrzymania funkcjonalności systemów niezbędnych do wykonywania podstawowych celów. Brak osiągnięcia kluczowych celów. Straty finansowe.
Wysoki	3	Duże zagrożenie realizacji kluczowych zadań albo osiągania założonych celów. Dotkliwa strata finansowa. Znaczny uszczerbek na wizerunku. Długotrwały i trudny proces przywracania stanu poprzedniego.
Średni	2	Spadek efektywności działania i obniżenie jakości wykonywania zadań. Niewielka strata finansowa. Nieznaczny negatywny wpływ na wizerunek. Trudny proces przywracania stanu poprzedniego.
Niski	1	Zakłócenie lub opóźnienie w wykonywaniu zadań. Bez uszczerbku dla wizerunku. Skutki łatwe do usunięcia.

***skala dopuszczalności ryzyka

Oszacowanie ryzyka	**Dopuszczalność ryzyka**	**Działania**
Ryzyko poważne Skala: 13-16 pkt.	Niedopuszczalne (nieakceptowane)	Działania nie mogą być podjęte ani kontynuowane do czasu zmniejszenia ryzyka do poziomu dopuszczalnego.
Ryzyko wysokie Skala: 9-12 pkt.	Dopuszczalne (akceptowane)	Zaleca się zaplanowanie i podjęcie działań, których celem jest zdecydowane zmniejszenie ryzyka.
Ryzyko umiarkowane Skala: 5-8 pkt.	Dopuszczalne (akceptowane)	Zaleca się zaplanowanie i podjęcie działań, których celem jest zdecydowane i skuteczne zmniejszenie ryzyka.
Ryzyko nieznaczne Skala: 1-4 pkt.	Dopuszczalne (akceptowane)	Zaleca się rozważenie możliwości dalszego zmniejszenia poziomu ryzyka lub zapewnienie, że ryzyko pozostanie na tym samym poziomie.

Lista mechanizmów kontroli redukujących ryzyko:

1. Regulacje zewnętrzne i wewnętrzne.

2. Opis funkcji i stanowisk, zakresy czynności i obowiązków.

3. System obiegu informacji i raportowania.

4. Uzgadnianie stanowisk, kierunków działań.

5. Uzgadnianie danych, tzw. rekonsylidacja.

6. Zasada komisyjności „czworga oczu", „na dwie ręce" (wykonywanie czynności przy współudziale co najmniej dwóch osób, komisje inwentaryzacyjne, spisowe, zespoły kontrolne, rejestracja i autoryzacja dowodów księgowych lub transakcji).

7. System limitów i ograniczeń.

8. Analiza jednostek organizacyjnych/uczestników rynku.

9. Kontrola dostępu oraz zabezpieczenia teleinformatyczne (zakazy i ograniczenia dostępu fizycznego osób do pomieszczeń, systemów i danych, Internetu, zagranicznych rozmów telefonicznych, możliwości nagrywania rozmów telefonicznych).

10. Inwentaryzacja i spis z natury.

11. Zabezpieczenia fizyczne.

12. Kopie zapasowe, na wypadek utraty oryginalnych danych, zapasowe generatory prądotwórcze, na wypadek awarii zasilania.

13. Plany zarządzania kryzysem.

14. Rezerwy finansowe, na pokrycie strat związanych np. z niewypłacalnością jednostek organizacyjnych, koniecznością pokrycia strat.

15. Ubezpieczenie mienia od zdarzeń losowych, kradzieży, itp.

16. Usługi zewnętrzne, dzielenie się ryzykiem, które obciążałoby jednostkę w sytuacji, gdyby zadania były wykonywane przy wykorzystaniu zasobów własnych.

17. Audyt i kontrola bieżąca i następna.

18. Testowanie nowych rozwiązań, projektów, systemów informatycznych przed ich wdrożeniem.

19. Zarządzanie bezpieczeństwem informacji, szkolenie pracowników.

20. Analiza informacji przekazywanych od pracowników oraz pozyskiwanych od stron zewnętrznych.

Protokół uchybienia/zagrożenia*

Data i godzina wystąpienia uchybienia/zagrożenia*……

Kod uchybienia/zagrożenia*

…..……

Opis uchybienia/zagrożenia*

……
……

……
……

……
……

……
……

Przyczyny powstania uchybienia/zagrożenia*

……
……

……
……

……
……

……
……

……
……

Zaistniałe skutki uchybienia/zagrożenia*

……
……

……
……..

……
……

……
……

Podjęte działania naprawczo-zapobiegawcze

……
……

……
……

……
……

Inspektor Ochrony Danych Administrator

…… …….

*niewłaściwe skreślić

Załącznik nr 14 do Polityki Bezpieczeństwa

Wapno, dnia .....…….....

RAPORT
z naruszenia bezpieczeństwa zasad ochrony danych osobowych
w Urzędzie Gminy Wapno

1. Data: ……. …… Godzina: ……

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

……..……
……

(imię, nazwisko, stanowisko służbowe, nazwa użytkownika, jeśli występuje)

3. Lokalizacja zdarzenia:

……..……
……

(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

……..……
……..……..……
……

5. Przyczyny wystąpienia zdarzenia:

……..……
……..……..……
……

6. Podjęte działania:

……..……
……..……..……
……

7. Skutki zdarzenia:

……..……..……
……..……
……..……

8. Postępowanie wyjaśniające:

……..……
……..……..……
……

……..

(data, podpis IOD)

Rejestr haseł w roku …… dla użytkownika: ……..

(imię i nazwisko)

Lp.	Konto użytkownika	Hasło (8 znaków: małe i duże litery, cyfry lub znaki specjalne)	Data nadania	Podpis użytkownika	Data blokady komputera i podpis Informatyka
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					

Załącznik Nr 2 do zarządzenia Nr 0050.38.2023

Wójta Gminy Wapno

z dnia 30 maja 2023 r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Wapno

Rozdział 1.
Wprowadzenie

1. Niniejsza instrukcja określa zasady eksploatacji i zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Wapno.

2. Zasady opisane w niniejszym dokumencie są zgodne z obowiązującymi wymaganiami prawnymi zapisanymi w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016).

3. W instrukcji stosuje się następujące skróty:

1) Administrator – Administrator Danych Osobowych;

2) IOD – Inspektor Ochrony Danych;

3) Podmiot przetwarzający – oznacza osobę fizyczną lub prawną, która przetwarza dane osobowe w imieniu administratora;

4) Zespół wspomagający – osoby wyznaczone przez Administratora do wspierania IOD (Sekretarz Gminy i Informatyk)

5) Strona trzecia – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający, czy osoby, które – z upoważnienia administratora lub pomiotu przetwarzającego – mogą przetwarzać dane osobowe.

Rozdział 2.
Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

1. Podstawą do nadania uprawnień do przetwarzania danych osobowych w systemie informatycznym Urzędu jest upoważnienie do przetwarzania danych osobowych. Upoważnienie wydawane jest przez Administratora.

2. Upoważnienie wydawane jest na wniosek przełożonego danego pracownika, a w przypadku osoby będącej stroną trzecią na wniosek pracownika Urzędu, koordynującego działania strony trzeciej, dla której upoważnienie jest wydawane.

3. IOD:

1) w przypadku, gdy dany podmiot przetwarzający otrzymuje po raz pierwszy upoważnienie do przetwarzania danych osobowych informuje się go o obowiązkach związanych z zapewnieniem ochrony danych osobowych;

2) warunkiem przetwarzania danych osobowych jest zapoznanie się podmiotu przetwarzającego z obowiązującymi zasadami ochrony danych osobowych i podpisanie oświadczeniem o zapoznaniu się z polityką bezpieczeństwa informacji oraz upoważnienia do przetwarzania danych osobowych.

4. IOD prowadzi, w imieniu i z upoważnienia Administratora, ewidencję osób upoważnionych do przetwarzania danych osobowych. Każda zmiana w zakresie informacji zawartych w ewidencji podlega niezwłocznemu odnotowaniu przez IOD.

5. Uprawnienia dostępu do systemu informatycznego nadawane są na podstawie wniosku przełożonego danego podmiotu przetwarzającego. Na wniosek pracownika Urzędu uprawnienia dostępu dla strony trzeciej nadaje Administrator.

6. Za nadanie uprawnień w systemie informatycznym odpowiada IOD. Uprawnienia nie mogą być nadane w przypadku, jeżeli dana osoba nie posiada upoważnienia do przetwarzania danych osobowych w wymaganym zakresie.

7. IOD informuje podmiot przetwarzający wnioskujący o fakcie nadania lub odmowy nadania uprawnień.

8. W przypadku nadawania podmiotowi przetwarzającemu uprawnień do danego systemu informatycznego po raz pierwszy, IOD odnotowuje w ewidencji osób upoważnionych do przetwarzania danych osobowych nadanie identyfikatora.

9. Identyfikator podmiotu przetwarzającego w systemie informatycznym musi być unikalny. Nie może być to identyfikator, który w przeszłości był już stosowany w systemie informatycznym. Sprawdzenie unikalności identyfikatora odbywa się na podstawie ewidencji podmiotów przetwarzających upoważnionych do przetwarzania danych osobowych.

10. Podmiot przetwarzający jest zobowiązany do zmiany hasła przy pierwszym dostępie do systemu informatycznego na hasło zgodne z wymogami zawartymi w Rozdziale 4.

Rozdział 3.
Procedura odbierania uprawnień do przetwarzania danych w systemie informatycznym

1. W przypadku konieczności odebrania uprawnień podmiotowi przetwarzającemu, bezpośredni przełożony zgłasza ten fakt IOD. IOD powiadamia Administratora, który to odbiera w całości lub w części uprawnienia.

2. W przypadku nadania lub zmiany zakresu uprawnienia droga postępowania jest taka sama jak w pkt. 1, przy czym Administrator nadaje zakres uprawnienia.

3. O wyżej wymienionych okolicznościach poinformowany zostaje IOD.

4. W przypadku zlecenia przez Urząd wykonania prac, polegających na przetwarzaniu danych stronie trzeciej, należy uzyskać dla niej niezbędne uprawnienia od Administratora. Prace wykonywane przez stronę trzecią muszą być nadzorowane przez pracownika urzędu. Formalności odnośnie nadania bądź też odebrania uprawnienia koordynuje pracownik urzędu.

Rozdział 4.
Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Podmioty przetwarzające dane osobowe wykorzystują w procesie uwierzytelnienia identyfikatory i hasła.

2. Hasła dostępu do systemu informatycznego muszą spełniać poniższe warunki:

1) posiadać długość, co najmniej 8 znaków,

2) zawierać litery małe i duże,

3) zawierać cyfry lub znaki specjalne.

3. Hasło jest zmieniane przez podmiot przetwarzający nie rzadziej niż co 30 dni lub niezwłocznie w przypadku podejrzenia, iż mogło zostać użyte przez nieuprawnioną osobę. Zdarzenie to powinno zostać natychmiast zgłoszone IOD.

4. Hasło nie powinno się powtarzać i być unikalne.

5. Podmiot przetwarzający zobowiązany jest do:

1) nieujawniania hasła innym podmiotom przetwarzającym,

2) zachowania hasła w tajemnicy, również po jego wygaśnięciu,

3) niezapisywania hasła,

4) postępowania z hasłami w sposób uniemożliwiający dostęp do nich osobom trzecim,

5) przestrzegania zasad dotyczących jakości i częstości zmian hasła.

6. W przypadku zapomnienia hasła podmiot przetwarzający użytkownik powinien zwrócić się do Członka Zespołu Wspomagającego - Informatyka o ustanowienie nowego hasła pierwszego logowania.

Rozdział 5.
Procedura rozpoczęcia, zawieszenia i zakończenia pracy przeznaczona dla podmiotu przetwarzającego

1. Rozpoczynając pracę w systemie informatycznym przetwarzającym dane osobowe, podmiot przetwarzający:

1) uruchamia i loguje się do komputera za pomocą hasła użytkownika,

2) wprowadza niezbędne identyfikatory i hasła do pracy w systemach informatycznych,

3) hasła są wprowadzane w sposób minimalizujący ryzyko podejrzenia ich przez osoby trzecie,

4) w przypadku problemów z rozpoczęciem pracy, spowodowanych odrzuceniem przez system wprowadzonego identyfikatora i hasła, natychmiast kontaktuje się z Informatykiem,

5) w przypadku niestandardowego zachowania aplikacji przetwarzającej dane osobowe pracownik natychmiast powiadamia o zaistniałym fakcie IOD.

2. Zawieszając pracę w systemie informatycznym (w tym odchodząc od stanowiska pracy), podmiot przetwarzający wylogowuje się z systemu informatycznego oraz blokuje stację roboczą. Kontynuacja pracy może nastąpić po odblokowaniu stacji roboczej, po wprowadzeniu hasła, w sposób gwarantujący jego niepodejrzenie przez osoby trzecie.

3. Opuszczając pomieszczenie, w którym przetwarzane są dane osobowe, podmiot przetwarzający zobowiązany jest do zamknięcia pomieszczenia na klucz, jeżeli w pomieszczeniu tym nie przebywa inna osoba upoważniona do przebywania w tym pomieszczeniu. Zabronione jest pozostawianie bez nadzoru w pomieszczeniach, w których przetwarzane są dane osobowe, osób nieupoważnionych.

4. Kończąc pracę w systemie informatycznym podmiot przetwarzający wylogowuje się ze wszystkich systemów i aplikacji, z których korzystał, wyłącza stację roboczą, UPS i listwę zasilającą.

5. W przypadku, gdy podmiot przetwarzający jest ostatnią osobą opuszczającą pomieszczenie, sprawdza zamknięcie wszystkich szaf w pomieszczeniu, okien oraz wyłączenie wszelkiego typu urządzeń elektrycznych, zamyka na klucz drzwi do pomieszczenia oraz zdaje klucz odnotowując ten fakt w Ewidencji Pobranych i Zdanych Kluczy do Pomieszczeń.

Rozdział 6.
Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Członek Zespołu Wspomagającego - Informatyk odpowiada za wykonanie i przechowywanie kopii zapasowych.

2. Kopie zapasowe systemów przetwarzających dane osobowe są codziennie zapisywane na serwerze podstawowym. Archiwizacja dzienna wykonywana jest etapami: w pierwszym etapie serwer wykonuje codzienną kopię wszystkich systemów RADIX wykorzystywanych w urzędzie, w wersji skompresowanej. Drugim etapem jest codzienny zapis tego archiwum, jako kopii w wersji skompresowanej zabezpieczonej hasłem na serwerze backupowym QNAP. Trzecim etapem jest zgranie archiwum z dnia poprzedniego na komputer Informatyka. Dwa pierwsze etapy wykonują się automatycznie, trzeci wykonuje Informatyk. Kopie przechowywane są z ostatnich trzech miesięcy, poprzednie są trwale usuwane.

3. Kopia jest oznaczona, jako data jej utworzenia.

4. Utworzone kopie zapasowe podlegają weryfikacji pod względem możliwości odczytu danych.

5. Członek Zespołu Wspomagającego - Informatyk odpowiedzialny jest za realizację działań odtworzeniowych w przypadku konieczności podjęcia takich działań w związku z awarią systemu informatycznego Urzędu. Po odtworzeniu systemu informatycznego Informatyk odpowiedzialny jest za przeprowadzenie testów poprawności działania systemu przed jego oddaniem do użytkowania.

Rozdział 7.
Procedura usuwania kopii zapasowych zbiorów danych i nośników danych

1. W celu usunięcia kopii zapasowych, zbiorów danych i nośników Administrator powołuje komisję w składzie:

1) IOD,

2) Sekretarz,

3) Informatyk.

2. Z usunięcia, o którym mowa w ust. 1 sporządza się protokół, który zawiera:

1) Datę i miejsce sporządzenia protokołu,

2) Ilość usuniętych archiwów (daty archiwów),

3) Ilość usuniętych kopii systemowych systemów,

4) Ilość usuniętych archiwów na płytach CD i DVD,

5) Ilość usuniętych archiwów z serwera backup,

6) Ilość uszkodzonych dysków twardych,

7) Podpisy członków komisji.

3. Protokół sporządza się w 3 egzemplarzach (jeden dla Administratora, jeden dla IOD i jeden dla Informatyka).

4. Administrator może skontrolować pracę komisji.

Rozdział 8.
Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz nośników kopii zapasowych:

1. Dane osobowe przechowywane są w postaci elektronicznej na:

1) serwerze produkcyjnym,

2) serwerze backupowym QNAP,

1) komputerze Informatyka.

2. Dane osobowe w systemie informatycznym przechowywane są przez czas wymagany do spełnienia celu, dla którego są one przetwarzane.

3. W przypadku wycofania sprzętu komputerowego z użycia dane osobowe na nim zapisane są kasowane przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych zaakceptowanego do użycia w Urzędzie. W przypadku braku możliwości programowego usunięcia danych dysk podlega fizycznemu zniszczeniu. Za zniszczenie danych odpowiada Informatyk. Zniszczenie nośnika potwierdzane jest protokołem przechowywanym przez IOD.

4. Dopuszcza się powierzenie niszczenia nośników danych wyspecjalizowanym stronom trzecim, pod warunkiem:

1) zawarcia umowy wraz z stosownym upoważnieniem do przetwarzania,

2) zagwarantowania poufności danych przez usługodawcę,

3) umożliwienia prowadzenia nadzoru nad procesem niszczenia nośników przez Członka Zespołu Wspomagającego,

4) udokumentowania faktu zniszczenia nośników protokołem.

Rozdział 9.
Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem działania jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. W celu zabezpieczenia systemu informatycznego przed działaniem niebezpiecznego oprogramowania zabrania się:

1) uruchamiania jakiegokolwiek oprogramowania, które nie zostało zatwierdzone do użytku przez Administratora;

2) samowolnego korzystania z nośników przenośnych;

3) otwierania poczty elektronicznej, której tytuł nie sugeruje związku z pełnionymi obowiązkami służbowymi; w przypadkach wątpliwych należy skonsultować się z IOD;

4) korzystania z Internetu w celach niezwiązanych z pełnionymi obowiązkami służbowymi.

2. W przypadku zauważenia objawów mogących wskazywać na obecność niebezpiecznego oprogramowania użytkownik jest zobowiązany powiadomić IOD lub Informatyka.

3. Do objawów powyższych można zaliczyć:

1) istotne spowolnienie działania systemu informatycznego,

2) nietypowe działanie aplikacji,

3) nietypowe komunikaty,

4) utratę danych lub modyfikację danych.

4. System informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:

1) oprogramowanie antywirusowe,

2) zaporę sieciową,

3) aktualizację oprogramowania systemowego,

4) konfigurację oprogramowania minimalizującą ryzyko naruszenia bezpieczeństwa.

5. Informatyk jest odpowiedzialny za nadzór nad działaniem powyższych zabezpieczeń, a w szczególności za:

1) weryfikację aktualności sygnatur systemu antywirusowego i podejmowanie ewentualnych działań korekcyjnych,

2) weryfikację logów systemu antywirusowego i podejmowanie działań korekcyjnych,

3) przegląd logów zapory sieciowej oraz podejmowanie działań mających na celu zablokowanie ataków sieciowych,

4) weryfikację poprawności aktualizacji oprogramowania systemowego.

Rozdział 10.
Odnotowanie informacji o udostępnieniu danych osobowych

1. Urząd udostępnia dane osobowe jedynie w przypadkach prawnie dopuszczalnych.

2. Podmiot przetwarzający udostępniający dane zachowuje wniosek o udostępnienie danych wraz z udzieloną odpowiedzią.

Rozdział 11.
Procedura wykonywania przeglądu i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

1. Przegląd i konserwacja sprzętu informatycznego realizowana jest przez upoważnionych pracowników Urzędu oraz przez strony trzecie.

2. Prace serwisowe wykonywane na terenie Urzędu przez strony trzecie podlegają bezpośredniemu nadzorowi IOD lub Informatyka.

3. Przekazanie sprzętu teleinformatycznego do naprawy poza teren Urzędu jest dopuszczalne, jeżeli spełnione zostaną poniższe warunki:

1) sprzęt przekazywany jest bez nośników zawierających dane osobowe, zaś fakt usunięcia nośników danych lub stwierdzenia braku nośników danych jest potwierdzany protokołem,

2) przekazanie sprzętu potwierdzane jest protokołem, pozwalającym na jednoznaczne wskazanie osoby przekazującej i osoby odbierającej sprzęt.

4. Protokoły, o których mowa w punkcie 3, lub ich kopie przechowywane są przez IOD.

5. Wszelkie prace serwisowe wykonywane przez strony trzecie wymagają sporządzenia protokołu serwisowego, zawierającego co najmniej poniższe informacje:

1) wskazanie osoby przeprowadzającej prace serwisowe,

2) wskazanie osoby nadzorującej przebieg prac serwisowych (dotyczy sytuacji, gdy prace realizowane są w siedzibie Urzędu),

3) przedmiot prac serwisowych (w szczególności identyfikator sprzętu w przypadku prac serwisowych dotyczących sprzętu),

4) zakres prac serwisowych i ich wynik,

5) czas przeprowadzania prac serwisowych.

Rozdział 12.
Używanie prywatnych urządzeń

1. Zakazuje się używania prywatnych urządzeń do celów służbowych.

2. W szczególnych przypadkach wykorzystanie w/w urządzeń może nastąpić wyłącznie za zgodą Administratora.

Rozdział 13.
Praca zdalna

1. Zasady pracy zdalnej regulują odrębne zarządzenie.