Zarządzenie nr 72/2018
Wójta Gminy Świdnica
z dnia 9 lipca 2018 r.

w sprawie wprowadzenia *Polityki Bezpieczeństwa Informacji* oraz *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych* w Urzędzie Gminy Świdnica.

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2018 roku, poz. 994 z późn.zm.), 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 uchylenie dyrektywy 95/46/WE (Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000) zarządza się, co następuje:

§ 1. Wprowadza się *Politykę Bezpieczeństwa Informacji* w Urzędzie Gminy Świdnica w brzmieniu stanowiącym *załącznik nr 1* do niniejszego Zarządzenia.

§ 2. Wprowadza się *Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych* w Urzędzie Gminy Świdnica w brzmieniu stanowiącym *załącznik nr 2* do niniejszego Zarządzenia.

§ 3. Zobowiązuje się wszystkich pracowników Urzędu Gminy Świdnica do zapoznania się i stosowania *Polityki Bezpieczeństwa Informacji* oraz *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych* w Urzędzie Gminy Świdnica.

§ 4. Traci moc zarządzenie nr 110/2015 Wójta Gminy Świdnica w sprawie wprowadzenia „Polityki bezpieczeństwa w Urzędzie Gminy Świdnica" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Świdnica".

§ 5. Nadzór nad realizacją zarządzenia powierza się Sekretarzowi Gminy.

§ 6. Zarządzenie wchodzi w życie z dniem podpisania.

z up. WÓJTA
Zbigniew [illegible]
Zastępca Wójta

Uzasadnienie
do Zarządzenia nr 72/2018
Wójta Gminy Świdnica
z dnia 9 lipca 2018 r.

W związku z wprowadzeniem przepisów wynikających z 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 uchylenie dyrektywy 95/46/WE, zasadnym jest wdrożenie nowej *Polityki Bezpieczeństwa Informacji* oraz *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych* w Urzędzie Gminy Świdnica.

Kierownik Działu:
SEKRETARZ GMINY
Jadwiga Generowicz

Sporządził:
Ireneusz Filiacz
I. Filiacz

Otrzymują:
1. DSOA
2. DIIT
3. DBF
4. DROŚ
5. SRP
6. SDG
7. RP
8. AW
9. a/a

Radca Prawny:
RADCA PRAWNY
Anna Sapińska-Maćkowiak
WŁ/WB/604
.....

Załącznik nr 1
do zarządzenia nr 72/2018
Wójta Gminy Świdnica
z dnia 9 lipca 2018r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Urząd Gminy Świdnica

Tytuł:	**POLITYKA BEZPIECZEŃSTWA INFORMACJI** **Urząd Miasta i Gminy Świdnica**		
Status:	Obowiązujący		**Wersja: 1.2**
Zatwierdził:	Wójt		
	Data:		
Autor dokumentu:	Imię i Nazwisko:	Krzysztof Olejniczak	

Historia zmian dokumentu

Data	Wersja	Opis zmiany	Autor zmian
4.05.2018r.	1.0	Utworzenie dokumentu	K. Olejniczak
10.05.2018r.	1.1	Opracowanie załącznika nr 3	K. Olejniczak
25.05.2018r.	1.2		

SPIS TREŚCI

DEFINICJE

Użyte w dokumencie określenia oznaczają:

Administrator Danych	Wójt Gminy Świdnica
Analiza Ryzyka	proces mający na celu oszacowanie wagi Ryzyka rozumianej jako funkcja prawdopodobieństwa wystąpienia Skutku i krytyczności jego następstw dla UG.
Autentyczność	właściwość oznaczająca, że zawartość Zasobu Teleinformatycznego oraz tożsamość osoby lub innego Systemu Teleinformatycznego, mającego dostęp do tego Zasobu, jest taka jak deklarowana.
Bezpieczeństwo Danych osobowych	stan, w którym na każdym etapie Przetwarzania, zapewnione są równocześnie: - Poufność, - Integralność, - Rozliczalność, - Dostępność, - Autentyczność.
Bezpowrotne Usuwanie Informacji	sposób postępowania z Nośnikami danych osobowych mający na celu usunięcie zapisanych na nich Informacji tak, aby ich odtworzenie w całości lub w części było niemożliwe.
Dane osobowe	informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, 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;
Dane Testowe	dane wykorzystywane jedynie na etapie rozwoju lub testowania Systemu Teleinformatycznego, a powstałe poprzez losowe ich wygenerowanie lub taką modyfikację Informacji rzeczywistych, która zapewnia obniżenie ich kategorii do Podstawowej oraz uniemożliwia przywrócenie ich pierwotnej postaci i wartości biznesowej (Kategorii).
Dostępność	właściwość Zasobu Teleinformatycznego oznaczająca, że wymagana Informacja lub funkcjonalność Systemu Teleinformatycznego jest dostępna dla uprawnionych osób lub uprawnionych Systemów Teleinformatycznych, w żądanym czasie, miejscu i zakresie.
Incydent Bezpieczeństwa	każde wykryte naruszenie lub wykryta próba naruszenia Bezpieczeństwa Informacji będąca naruszeniem obowiązujących wewnętrznych aktów normatywnych UG lub przepisów prawa. Źródłem Incydentu Bezpieczeństwa może być zarówno przypadkowe, jak i celowe działanie albo jego zaniechanie przez pracowników UG lub inne osoby.
Integralność	właściwość Zasobu Teleinformatycznego oznaczająca, że nie nastąpiła jego niezamierzona lub nieuprawniona zmiana.
Konta Techniczne	konta, które istnieją w Systemach Teleinformatycznych jedynie w celu zapewnienia ich prawidłowego funkcjonowania i w związku z tym nie są przypisane żadnej osobie, ale jedynie konkretnemu Systemowi np. konto wykorzystywane do automatycznego transferu plików z użyciem FTP.
UG	Urząd Gminy Świdnica
Nośniki danych	wszelkiego rodzaju nośniki danych osobowych, używane w procesie Przetwarzania, w szczególności dyski twarde, płyty CD, pendrive, pamięci przenośne, dyski magneto-optyczne.
Ochrona	zespół środków organizacyjnych, technicznych i prawnych zapewniających Bezpieczeństwo

	Danych Osobowych.
Osoba Trzecia	osoba fizyczna lub prawna współpracująca z UG na podstawie odrębnej umowy.
Podatność	słabość Zasobu Teleinformatycznego, która może zostać wykorzystana przez Zagrożenie.
Poufność	właściwość Zasobu Teleinformatycznego oznaczająca, że jest on dostępny wyłącznie uprawnionym osobom lub uprawnionym Systemom Teleinformatycznym.
Rozliczalność	właściwość Zasobu Teleinformatycznego oznaczająca, że wykonane na nim działania mogą być jednoznacznie przypisane do wykonującej je osoby lub Systemu Teleinformatycznego.
Ryzyko	prawdopodobieństwo tego, że Zagrożenie wykorzysta Podatność powodując Skutek.
Ryzyko Szczątkowe	Ryzyko pozostające po wdrożeniu Właściwej Ochrony przy założeniu, że jego poziom jest akceptowalny.
Skutek	negatywne dla UG następstwo naruszenia Bezpieczeństwa Informacji –(np. finansowe, prawne, biznesowe).
System Teleinformatyczny (System)	zespół środków technicznych wraz z oprogramowaniem, stanowiący integralną i logiczną całość wyodrębnioną ze względu na dostarczaną funkcjonalność przy założeniu, że głównym jego celem jest Przetwarzanie informacji.
Użytkownik	każdy pracownik UG lub Osoba Trzecia mająca uprawniony dostęp wyłącznie do funkcjonalności biznesowej Systemu Teleinformatycznego oraz przetwarzanych w nim danych osobowych.
Właściwa Ochrona	zespół środków organizacyjnych, technicznych i prawnych stosowanych w celu zapewnienia Bezpieczeństwa przy jednoczesnym uwzględnieniu opłacalności ekonomicznej, akceptacji Ryzyka Szczątkowego oraz spełnieniu wymogów prawnych, które w szczególności wynikają z 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 5 kwietnia 2016 r.).
Zagrożenie	potencjalna przyczyna naruszenia Bezpieczeństwa Danych Osobowych.
Zasób Teleinformatyczny	Dane oraz przetwarzający je System Teleinformatyczny wraz z procesami zaangażowanymi w jego rozwój, utrzymanie, bezpieczeństwo i eksploatację.
Zbiór Danych	uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

ROZDZIAŁ I

Deklaracja o ustanowieniu Polityki Bezpieczeństwa Informacji

§ 1

Istotnym elementem sprawnej realizacji zadań UG jest niezakłócone działanie Systemów Teleinformatycznych oraz właściwe zabezpieczenie przetwarzanych Informacji przed istniejącymi Zagrożeniami oraz zapewnienie, że dane osobowe są pozyskiwane, przetwarzane i udostępniane zgodnie z prawem i na podstawie prawa.

§ 2

W związku z powyższym Wójt UG Świdnica ustanawia Politykę Bezpieczeństwa Informacji.

§ 3

Wójt UG Świdnica deklaruje zapewnienie optymalnych warunków i niezbędnych środków finansowych dla realizacji celów zawartych w Polityce Bezpieczeństwa Informacji.

§ 4

Polityka Bezpieczeństwa Informacji jest dokumentem nadrzędnym w stosunku do obowiązujących w UG aktów wewnętrznych w zakresie ochrony Zasobów Teleinformatycznych UG oraz danych osobowych i wynikających z nich regulacji.

§ 5

1. Zapewnienie Bezpieczeństwa Informacji w UG opiera się na dokumentach definiujących Zasoby Teleinformatyczne, określeniu zagrożeń i analizie ryzyka ich wystąpienia, wskazaniu właścicieli zasobów informacyjnych, a także sprecyzowaniu odpowiedzialności za realizację poszczególnych procesów, procedur, regulaminów i standardów.
2. Bezpieczeństwo Informacji należy osiągnąć, wdrażając katalog zasad, oraz odpowiedni zestaw środków, którymi są w szczególności procedury, procesy, regulaminy, standardy, struktury organizacyjne oraz środki techniczne.

§ 6

Zasoby Teleinformatyczne uznaje się za jawne tylko wtedy, gdy zostały one podane do publicznej wiadomości przez upoważnionych do tego pracowników UG lub gdy są one ogólnie dostępne ze względu na swą specyfikę.

§ 7

Dokumentami powiązanymi z Polityką Bezpieczeństwa Informacji są Instrukcja Zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych oraz zestaw procedur, procesów, regulaminów i standardów.

ROZDZIAŁ II

Cel opracowania i zawartość dokumentu

§ 8

Celem opracowania dokumentu Polityka Bezpieczeństwa Informacji jest zdefiniowanie ogólnych wymagań i zasad ochrony informacji, które będą fundamentem dla wszystkich dokumentów związanych z bezpieczeństwem informacji.

§ 9

Polityka niniejsza została opracowana w celu:

1) Zapewnienia ochrony informacji przed nieuprawnionym dostępem;
2) Zapewnienia poufności , integralności i rozliczalności informacji przetwarzanych w UG zgodnie z określonymi wymaganiami;
3) Zapewnienia, że eksploatowane w UG Systemy Teleinformatyczne spełniają określone wymogi bezpieczeństwa;
4) Zapewnienia, że dane osobowe są pozyskiwane, przetwarzane i udostępnianie zgodnie z prawem;
5) Zapewnienia, że szkolenia z zakresu bezpieczeństwa informacji są zagwarantowane pracownikom;
6) Zapewnienia możliwości rejestracji wszelkiego rodzaju naruszeń bezpieczeństwa informacji;
7) Zapewnienia możliwości analizy ryzyka aktywów informatycznych;
8) Zapewnienia, że plany zachowania ciągłości działania są opracowywane, utrzymywane i testowane w stopniu umożliwiającym nieprzerwaną realizację zadań.

§ 10

Wdrożenie niniejszej Polityki Bezpieczeństwa Informacji jest ważne dla wykazania należytej dbałości o poufność, integralność i dostępność informacji w ramach kontaktów z klientami oraz instytucjami współpracującymi.

ROZDZIAŁ III

Zakres Polityki Bezpieczeństwa Informacji

§ 11

Zakres Polityki Bezpieczeństwa Informacji odnosi się do:

1. Komórek organizacyjnych znajdujących się w strukturze organizacyjnej UG.

2. Zasobów informatycznych (aktywów) zaangażowanych w realizacje zadań UG, a w szczególności:

   a) Potencjału ludzkiego, czyli wszystkich pracowników UG w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów oraz inne osoby i instytucje mające dostęp do informacji podlegających ochronie,

   b) Informacji w formie papierowej i elektronicznej Przetwarzanych przez UG o ile są własnością UG lub zostały przekazane na podstawie przepisów prawa lub umów,

   c) Sprzętu komputerowego oraz innych Nośników Danych, na których znajdują się informacje podlegające ochronie.

3. Technologii służących pozyskiwaniu, przetwarzaniu i udostępnianiu informacji, do których zalicza się zarówno systemy tradycyjne oparte o dokumenty w formie papierowej jak i systemy elektroniczne wspomagające realizację zadań UG.

§ 12

Do stosowania zasad określonych przez Politykę Bezpieczeństwa Informacji zobowiązani są wszyscy pracownicy UG oraz inne osoby i instytucje mające dostęp do informacji podlegającej ochronie na podstawie przyjętego na siebie zobowiązania dotyczącego przestrzegania jej zasad.

ROZDZIAŁ IV

Role i odpowiedzialności związane z bezpieczeństwem informacji

§ 13

Administratorem Danych w UG jest Wójt UG Świdnica. Do zadań Administratora Danych należy:

1) Decydowanie o celach, sposobach i środkach przetwarzania danych;

2) Zapewnienie optymalnych warunków i niezbędnych środków finansowych dla realizacji celów zawartych w Polityce Bezpieczeństwa Informacji oraz stałą współpracę z osobami oraz zespołem powołanymi do opracowania, wdrożenia i doskonalenia Polityki Bezpieczeństwa Informacji.

§ 14

1. Inspektor Ochrony Danych odpowiada za właściwe przetwarzanie danych osobowych w UG. Do prawnych obowiązków Inspektora Ochrony Danych należy:

   1. informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

   2. monitorowanie przestrzegania rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu

przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

3. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
4. współpraca z organem nadzorczym;
5. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Do pozostałych obowiązków Inspektora Ochrony Danych należy:

1) Wydawanie i anulowanie Upoważnień do przetwarzania danych osobowych.
2) Prowadzenie Ewidencji osób upoważnionych do przetwarzania danych osobowych.
3) Prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych.
4) Nadzór nad bezpieczeństwem danych osobowych.
5) Kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych.
6) Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.
7) Prowadzenie rejestru incydentów bezpieczeństwa.
8) Kierowanie procesem Zarządzania ryzykiem.

§ 15

Administrator Systemów Informatycznych w ramach Polityki Bezpieczeństwa Informacji sprawuje nadzór nad funkcjonowaniem Systemów Teleinformatycznych UG, funkcjonowaniem infrastruktury sieciowej, urządzeń peryferyjnych oraz oprogramowania. Do zadań Administratora Systemów Informatycznych należy w szczególności:

1. Identyfikacja i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.
2. Dbałość aby zasoby informatyczne UG były sprawne, spełniały wymagania określone w przepisach, spełniały wymagania licencyjne, miały zapewnione wsparcie techniczne, były na bieżąco aktualizowane oraz były jak najmniej podatne na zagrożenia integralności, poufności i dostępności.
3. Wykonywanie lub zlecanie testów i audytów w celu potwierdzenia skuteczności istniejących zabezpieczeń.
4. Prowadzenie dziennika administratora.
5. Prowadzenie ewidencji sprzętu teleinformatycznego i oprogramowania.

6. Przygotowanie procedur określających zasady zarzadzania Systemami Teleinformatycznymi.
7. Przygotowanie procedur bezpieczeństwa danego systemu przetwarzania danych chronionych.
8. Przygotowanie procedur Zarządzania kontami użytkowników.
9. Przygotowanie dokumentów procedur kryzysowych związanych z incydentami w systemach przetwarzania informacji.
10. Nadzorowanie zgłaszanych incydentów i zdarzeń bezpieczeństwa dotyczących Systemów Teleinformatycznych.
11. Zapewnienie, że do informacji chronionych mają dostęp wyłącznie osoby upoważnione i że mogą one wykonywać wyłącznie uprawnione operacje.
12. Kontrolę procesu przyznawania uprawnień.
13. Nadzór nad wdrożeniem nowych aplikacji/systemów.
14. Dopuszczanie systemów przetwarzania informacji do eksploatacji.
15. Przeprowadzanie analizy ryzyka.

§ 16

Właściciele zasobów (Kierownicy wydziałów) są odpowiedzialni za wdrożenie, utrzymanie i doskonalenie Polityki Bezpieczeństwa Informacji w Komórkach organizacyjnych UG, a w szczególności za:

1. Okresowe raportowanie o poziomie bezpieczeństwa informacji w dziale.
2. Określanie, które osoby i w jakim zakresie mają dostęp do informacji chronionych.
3. Tworzenie i aktualizację i nadzór nad procedurami związanymi z bezpieczeństwem informacji z udziałem pracowników działów.
4. Podejmowanie w uzgodnieniu z Inspektorem Ochrony Danych decyzji w sprawie sposobu realizacji zadań w przypadku wystąpienia sytuacji nietypowej (nie opisanej w procedurze).
5. Wspieranie procesów Zarządzania ryzykiem w tym monitorowanie zmian zagrożeń i ich podatności oraz uczestniczenie w procesie kategoryzacji informacji i Systemów Teleinformatycznych.
6. Powiadamiania Inspektora Ochrony Danych o zakładaniu zbioru danych osobowych na lokalnych urządzeniach komputerowych oraz w formie dokumentacji papierowej (dotyczy również zbiorów istniejących w momencie wprowadzania niniejszej polityki).
7. Przeciwdziałanie próbom naruszenia Bezpieczeństwa Informacji.

§ 17

Pracownicy są odpowiedzialni za realizację zadań służbowych zgodnie z postanowieniami niniejszej Polityki Bezpieczeństwa Informacji, a w szczególności za:

1. Przestrzeganie tajemnicy w zakresie przez prawo przewidzianym.

2. Zgłaszanie wszelkich przypadków działań niezgodnych z regulaminami i procedurami, mogących być incydentami bezpieczeństwa.
3. Zgłaszanie przełożonemu konieczności lub propozycji zmian w dokumencie (procesie, procedurze) z zakresu Zarządzania bezpieczeństwem informacji.
4. Ochronę identyfikatorów osobistych oraz haseł.
5. Uczestnictwo w organizowanych przez UG szkoleniach z zakresu bezpieczeństwa informacji.
6. Przeciwdziałanie próbom naruszenia bezpieczeństwa informacji.

§ 18

Osoby trzecie przed uzyskaniem dostępu do informacji przetwarzanej w UG muszą zapoznać się z Polityka Bezpieczeństwa Informacji. Do obowiązków osób trzecich należy:

1. Przestrzeganie tajemnicy w zakresie przez prawo przewidzianej.
2. Stosowanie się do obowiązującej Polityki Bezpieczeństwa Informacji oraz innych dokumentów z zakresu ochrony informacji.
3. Zgłaszanie wszelkich przypadków działań niezgodnych z regulaminami i procedurami, mogących być incydentami bezpieczeństwa.
4. Przeciwdziałanie próbom naruszenia bezpieczeństwa informacji.

ROZDZIAŁ V

Obszar przetwarzania danych osobowych

§ 19

Szczegółowe rozmieszczenie zbiorów danych osobowych prowadzonych w postaci dokumentacji papierowej i elektronicznej znajduje się w załączniku nr 1 do Polityki Bezpieczeństwa Informacji.

ROZDZIAŁ VI

Wykaz zbiorów danych osobowych

§ 20

Inspektor Ochrony Danych prowadzi wykaz zbiorów danych osobowych.

§ 21

Szczegółowy wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych opisany jest w załączniku nr 1.

§ 22

Przetwarzanie danych osobowych w zbiorze, który nie figuruje w wykazie jest niedozwolone.

§ 23

Kierownicy działów zobowiązani są do przekazania Inspektorowi Ochrony Danych informacji dotyczących nowych zbiorów.

§ 24

Utworzenie nowego zbioru danych osobowych może być wynikiem:

1) realizacji nowego celu;
2) zidentyfikowania zbioru, który nie został wpisany do wykazu zbiorów;
3) przyjęcia zbioru danych osobowych w wyniku zawarcia umowy o powierzeniu przetwarzania.

§ 25

Aktualizacja załącznika nr 1 nie jest zmianą Polityki Bezpieczeństwa Informacji i nie wymaga formy zarządzenia.

§ 26

Tworzenie nowego zbioru danych w systemie informatycznym może nastąpić tylko po uzgodnieniach z Administratorem Systemów Informatycznych i po akceptacji przez Inspektora Ochrony Danych.

§ 27

Tworzenie nowego zbioru w formie dokumentu papierowego może nastąpić po akceptacji Inspektora Ochrony Danych.

§ 28

Przetwarzanie danych wrażliwych opisuje procedura będąca załącznikiem nr 4 do Polityki Bezpieczeństwa Informacji.

§ 29

Działania związane z usunięciem zbioru danych osobowych z wykazu podejmuje Inspektor Ochrony Danych na wniosek kierowników działów.

§ 30

W przypadku usunięcia z wykazu zbioru danych kierownicy działów, z uwzględnieniem przepisów o archiwizacji, w porozumieniu z Administratorem Systemów Informatycznych podejmują decyzję z w sprawie usunięcia zbioru danych osobowych z Systemu Teleinformatycznego UG.

ROZDZIAŁ VII

Rejestr czynności przetwarzania danych osobowych

§ 31

Rejestr czynności przetwarzania danych osobowych stanowi załącznik nr 2 do Polityki Bezpieczeństwa Informacji.

§ 32

Rejestr czynności przetwarzania danych osobowych prowadzi Inspektor Ochrony Danych.

ROZDZIAŁ VII

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

§ 33

W celu zapewnienia bezpieczeństwa danych przetwarzanych w UG wprowadzono zabezpieczenia organizacyjne polegające na:

1) Wyznaczeniu Inspektora Ochrony Danych, którego zadaniem jest nadzorowanie przestrzegania zasad ochrony przetwarzanych danych osobowych;
2) Opracowaniu i wdrożeniu Polityki Bezpieczeństwa Informacji;
3) Opracowaniu i wdrożeniu Instrukcji Zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych;
4) Dopuszczeniu do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienia nadane przez Administratora Danych;
5) Prowadzeniu ewidencji osób upoważnionych do przetwarzania danych;

6) Zapoznaniu osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;

7) Zobowiązaniu osób zatrudnionych przy przetwarzaniu danych osobowych do zachowania ich w tajemnicy;

8) Stosowaniu pisemnych umów powierzenia przetwarzania danych;

9) Wprowadzeniu procedur zabezpieczających dane przed dostępem osób nieupoważnionych;

10) Wdrożeniu procedury, zgodnie z którą przebywanie osób nieuprawnionych w pomieszczeniach gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;

11) Analizowaniu ryzyka.

§ 34

Zabezpieczenia fizyczne pomieszczeń, w których przetwarzane są dane osobowe opisane są w załączniku nr 1 do Polityki Bezpieczeństwa Informacji.

§ 35

Zastosowane w UG zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej opisane są szczegółowo w Instrukcji Zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

§ 36

Zabezpieczenia narzędzi programowych i baz danych opisane są szczegółowo w Instrukcji Zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

§ 37

Dostęp osób trzecich do Zasobów Teleinformatycznych UG opisuje Załącznik nr 6 do Polityki Bezpieczeństwa Informacji.

ROZDZIAŁ VIII

Procedura postepowania z incydentami

§ 38

Wszyscy pracownicy UG oraz Osoby Trzecie mające dostęp do Zasobów Teleinformatycznych zobowiązane są do:

- niezwłocznego zgłaszania wszelkich zauważonych zdarzeń, które noszą znamiona lub są Incydentami Bezpieczeństwa, zgodnie z obowiązującymi w UG procedurami,
- udzielania wszelkich niezbędnych informacji oraz wsparcia pracownikom UG zaangażowanym z racji pełnionych obowiązków w proces obsługi Incydentów Bezpieczeństwa.

§ 39

Procedura postępowania z incydentami opisuje sposób postępowania w przypadku wystąpienia zdarzeń, które naruszają lub mogą naruszać przepisy prawa oraz zasady zawarte w polityce, instrukcji regulaminach i procedurach dotyczących bezpieczeństwa informacji.

§ 40

Celem obsługi Incydentów Bezpieczeństwa w UG jest:

1. wykrywanie lub umożliwienie zgłaszania Incydentów Bezpieczeństwa,
2. identyfikowanie źródeł Incydentów Bezpieczeństwa,
3. zabezpieczenia dowodów wystąpienia Incydentów Bezpieczeństwa,
4. identyfikowanie i dokumentowanie skutków Incydentów Bezpieczeństwa,
5. minimalizowanie skutków Incydentów Bezpieczeństwa,
6. dostarczanie dokumentacji z przebiegu Obsługi Incydentów Bezpieczeństwa w celu pociągnięcia osób odpowiedzialnych za ich powstanie do odpowiedzialności przewidzianej prawem,
7. opracowanie dokumentacji z przebiegu Obsługi Incydentów Bezpieczeństwa wraz z rekomendacjami mającymi na celu zminimalizowanie ryzyka wystąpienia podobnych Incydentów Bezpieczeństwa w przyszłości.

§ 41

Rejestr incydentów bezpieczeństwa prowadzi Inspektor Ochrony Danych. Rejestr ten podlega analizie Zespołu ds. Bezpieczeństwa Informacji co najmniej raz w roku.

§ 42

Szczegółowe zasady oraz wykazy naruszeń bezpieczeństwa opisane są w Instrukcji Zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych .

ROZDZIAŁ IX

Procedura działań korygujących i zapobiegawczych

§ 43

Celem procedury jest uporządkowanie i przedstawienie czynności związanych z inicjowaniem oraz realizacją działań korygujących i zapobiegawczych wynikających z zaistnienia incydentów bezpieczeństwa lub zagrożeń systemu ochrony danych osobowych.

§ 44

Procedura działań korygujących i zapobiegawczych obejmuje wszystkie te procesy, w których incydenty bezpieczeństwa lub zagrożenia mogą wpłynąć na stopień ryzyka utraty praw osób, których dane są przetwarzane jak również na poprawne funkcjonowanie systemu ochrony danych osobowych.

§ 45

Osobą odpowiedzialną za nadzór nad procedurą jest Inspektor Ochrony Danych.

§ 46

Opis czynności

1. Inspektor Ochrony Danych jest odpowiedzialny za analizę incydentów bezpieczeństwa lub zagrożeń ochrony danych osobowych. Typowymi źródłami informacji o incydentach, zagrożeniach lub słabościach są:
   a. zgłoszenia od pracowników,
   b. wiedza Inspektora Ochrony Danych,
   c. wyniki kontroli wewnętrznych lub kontroli UOD.
2. W przypadku, gdy Inspektor Ochrony Danych stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa: źródło powstania incydentu lub zagrożenia, zakres działań korygujących lub zapobiegawczych, termin realizacji, osobę odpowiedzialną
3. Inspektor Ochrony Danych jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych.
4. Po przeprowadzeniu działań korygujących lub zapobiegawczych, Inspektor Ochrony Danych jest zobowiązany do oceny efektywności ich zastosowania.

ROZDZIAŁ X

Kontrola wewnętrzna stanu ochrony danych osobowych

§ 47

Celem procedury jest uporządkowanie i przedstawienie czynności związanych ze sprawdzaniem zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych (na podstawie 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 5 kwietnia 2016 r.).

§ 48

Za przeprowadzenie kontroli odpowiada Inspektor Ochrony Danych.

§ 49

Kontroli podlegają: zbiory, systemy informatyczne przetwarzające dane osobowe, zabezpieczenia fizyczne, zabezpieczenia organizacyjne, bezpieczeństwo osobowe oraz zgodność stanu faktycznego z wymaganiami Rozporządzenia.

§ 50

Inspektor Ochrony Danych przygotowuje plan kontroli (możliwy kwartalny lub roczny) uwzględniając zakres oraz termin przeprowadzenia poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania. W okresie 5 lat należy dokonać kontroli wszystkich zbiorów i systemów Administratora Danych.

§ 51

Inspektor Ochrony Danych ma obowiązek przedstawienia Wójtowi UG planu kontroli najpóźniej na 2 tygodnie przed dniem rozpoczęcia okresu objętego planem.

§ 52

Inspektor Ochrony Danych prowadzi kontrole zgodnie z planem lub może wszcząć kontrole doraźne na skutek podejrzenia lub naruszenia ochrony danych osobowych.

§ 53

Administrator Bezpieczeństwa Informacji zobowiązany jest do powiadomienia kierowników kontrolowanych jednostek o kontroli w terminie co najmniej 7 dni przed jej przeprowadzeniem.

§ 54

Po dokonanej kontroli, Inspektor Ochrony Danych przygotowuje i przekazuje Wójtowi UG raport pokontrolny. W przypadku sprawdzenia planowego, sprawozdanie powinno być przekazane nie później niż w terminie 30 dni od zakończenia sprawdzenia. W przypadku sprawdzenia doraźnego, sprawozdanie powinno być dostarczone niezwłocznie po zakończeniu sprawdzenia.

ROZDZIAŁ XI

Zapoznanie się osób z zasadami ochrony danych osobowych

§ 55

Każda osoba przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami w wersji papierowej winna być poddana przeszkoleniu lub zapoznana z:

1) 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 (ogólne rozporządzenie o ochronie danych (Dz. Urz. UE L 119 z 5 kwietnia 2016 r.).
2) zasadami ochrony danych osobowych zawartymi w Polityce Bezpieczeństwa Informacji oraz Instrukcji Zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

§ 56

1. Za przeprowadzenie szkolenia lub zapoznania z zasadami ochrony danych osobowych odpowiada Inspektor Ochrony Danych.
2. Inspektor Ochrony Danych sporządza roczny plan szkoleń.

§ 57

Każda osoba po szkoleniu lub po zapoznaniu z zasadami ochrony danych osobowych zobowiązana jest do podpisania Oświadczenia o poufności.

ROZDZIAŁ XII

Właściwa Ochrona Nośników Danych

§ 58

Wszystkie Nośniki Danych podlegają Właściwej Ochronie stosownie do Kategorii zapisanych na nich Informacji na wszystkich etapach ich składowania, transportowania, przekazywania i wycofywania z użycia.

§ 59

Za zapewnienie Właściwej Ochrony Nośników Danych odpowiada osoba będąca formalnie w ich posiadaniu. W przypadku Nośników Danych, które nie zostały formalnie nikomu przypisane, za zapewnienie ich Właściwej Ochrony odpowiada osoba będąca faktycznie w ich posiadaniu.

\

§ 60

W przypadku wycofywania Nośników Danych z użycia na osobie będącej w ich posiadaniu spoczywa obowiązek Bezpowrotnego Usunięcia zawartych na nich Informacji, zgodnie ze standardami obowiązującymi w UG.

§ 61

Osoby korzystające z Nośników Danych powinny być świadome wynikających z tego zagrożeń, a tym samym są zobowiązane do zachowania należytej staranności oraz użycia udostępnionych środków organizacyjnych i technicznych w celu zabezpieczenia tych Nośników Informacji.

§ 62

Szczegółowe zasady użytkowania Nośników Danych procedowane są w Instrukcji Zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

ROZDZIAŁ XIII

Bezpieczeństwo Sprzętu i Oprogramowania

§ 63

Sprzęt teleinformatyczny i oprogramowanie jako elementy tworzące System Teleinformatyczny przyczyniają się w istotny sposób do zapewnienia Bezpieczeństwa Informacji, a tym samym podlegają Właściwej Ochronie.

§ 64

Sprzęt komputerowy oraz oprogramowanie wykorzystywane w Systemach Teleinformatycznych muszą być zgodne ze standardami obowiązującymi w UG w tym zakresie.

§ 65

Odstępstwa od obowiązujących w UG standardów w zakresie bezpieczeństwa wymagają zgody Administratora Danych.

§ 67

System Teleinformatyczny może składać się wyłącznie z przetestowanego, formalnie dopuszczonego do eksploatacji sprzętu i oprogramowania. Decyzje o dopuszczeniu do eksploatacji podejmuje Administrator Danych na wniosek Administratora Systemów Informatycznych.

§ 68

Odstępstwa od wymogów zawartych w § 65 możliwe są jedynie w celu:

a) przywrócenia dostępności Systemu Teleinformatycznego,

b) prowadzenia prac związanych z Rozwojem Systemów Teleinformatycznych – wyłącznie w odniesieniu do sprzętu i oprogramowania, wobec których te prace są prowadzone.

§ 69

Sprzęt i oprogramowanie powinny być eksploatowane, serwisowane i wycofywane z eksploatacji z zachowaniem Właściwej Ochrony.

§ 70

Wszelkie działania związane z Utrzymaniem i Eksploatacją Systemu Teleinformatycznego mogą być podejmowane wyłącznie przez dopuszczony do tego, wykwalifikowany personel UG lub upoważnione – na zasadach opisanych w załączniku nr 6 – Osoby Trzecie.

§ 71

Wszelkie oprogramowanie wykorzystywane w UG musi być użytkowane z poszanowaniem praw własności intelektualnej, w szczególności zgodnie z „Ustawą o prawie autorskim i prawach pokrewnych".

§ 72

Oprogramowanie instalowane w Systemach Teleinformatycznych, adekwatnie do Kategorii tego Systemu, powinno być zabezpieczone przed nieuprawnioną modyfikacją w celu zapewnienia jego Integralności.

§ 73

Sprzęt wchodzący w skład Systemów Teleinformatycznych musi być objęty ochroną fizyczną odpowiednią do Kategorii Systemu oraz uwzględniającą konieczność zapewnienia Właściwej Ochrony. Za określenie standardów i szczegółowych procedur bezpieczeństwa fizycznego odpowiada Administrator Systemów Informatycznych.

§ 74

Komputery i inne urządzenia przenośne, w których zapisane są Informacje, muszą być zabezpieczone w sposób odpowiedni do Kategorii przetwarzanych Informacji i zapewniający ich Właściwą Ochronę. Osoby korzystające z takich urządzeń przenośnych powinny być świadome wynikających z tego Zagrożeń dla Bezpieczeństwa Informacji i zobowiązane są do zachowania należytej staranności w celu zapewnienia ich bezpieczeństwa.

§ 75

Zabrania się użytkowania komputerów i urządzeń przenośnych zawierających dane osobowe bez zapewnienia ich Właściwej Ochrony przy użyciu środków organizacyjnych i technicznych dostępnych w UG.

§ 76

Szczegółowe zasady bezpieczeństwa sprzętu i oprogramowania opisane są w instrukcji Zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

ROZDZIAŁ XIV

Powierzenie danych

§ 77

W przypadku powierzenia przetwarzania danych Podmiotowi przetwarzającemu Administrator Danych jest zobowiązany do zawarcia z tym Podmiotem umowy powierzenia danych osobowych.

§ 78

Szablon umowy powierzenia danych osobowych do przetwarzania stanowi załącznik nr 7 do Polityki Bezpieczeństwa Informacji

ROZDZIAŁ XV

Udostępnianie danych

§ 79

Administrator Danych udostępnia dane osobowe wyłącznie na podstawie wniosku.

§ 80

Wniosek, o którym mowa w § 79 musi zawierać podstawę prawną, określony cel udostępnienia i opisany zakres czynności.

§ 81

Kierownicy Działów prowadzą rejestr udostepnień będący załącznikiem nr 8 do Polityki Bezpieczeństwa Danych.

ROZDZIAŁ XVI

Postanowienia końcowe

§ 82

Prawo dostępu do Polityki Bezpieczeństwa Informacji posiadają przede wszystkim pracownicy UG oraz osoby i instytucje mające dostęp do informacji podlegającej ochronie a także interesanci, strony umów i porozumień.

§ 83

Wszelkie zmiany w Polityce Bezpieczeństwa Informacji są dokonywane na wniosek Inspektora Ochrony Danych. Jest on również odpowiedzialny za zakomunikowanie zmian w Polityce i dostosowanie planu szkoleń.

§ 84

Inspektor Ochrony Danych zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego załącznik nr 9 do niniejszego dokumentu.

§ 85

Naruszenie postanowień wynikających z niniejszej Polityki Bezpieczeństwa przez pracowników UG traktowane jako rażące naruszenie obowiązków.

§ 86

Za naruszenie postanowień wynikających z niniejszej Polityki Bezpieczeństwa Osoby Trzecie ponoszą odpowiedzialność przewidzianą w zawartych z nimi umowach lub na zasadach ogólnych przewidzianych w przepisach prawa powszechnie obowiązującego.

.

ZAŁACZNIK_PBI_01
Do Polityki Bezpieczeństwa Informacji
w UG Świdnica

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Lp.	Nazwa zbioru/zasobu danych osobowych	System przetwarzania	Lokalizacja miejsca przetwarza-nia	Zastosowa-ne oprogramo-wanie	Pełny zakres danych osobowych w systemie	Pola informacyjne w systemie	Sposób przepływu danych pomiędzy systemami
1.	Ewidencja ludności, dowody osobiste	Zbiór przetwarzany elektronicznie	- Sala Obsługi Klienta, - Pok. 119	Magislud, PUMA ŹRÓDŁO,	- imiona i nazwisko - nazwisko rodowe - imię ojca - imię matki - nazwisko rodowe matki - PESEL - miejsce urodzenia - data urodzenia - dokument tożsamości - stan cywilny - poprzedni adres - aktualny adres - służba wojskowa - kod terytorialny - wystawca dowodu - przyczyna złożenia wniosku o wystawienia dowodu	- imiona - nazwisko - nazwisko rodowe - imię ojca - imię matki - nazwisko rodowe matki - PESEL - miejsce urodzenia (ulica, miejscowość, kod-pocztowy) - data urodzenia - dokument tożsamości (seria i numer) - stan cywilny - poprzedni adres (ulica, miejscowość, kod-pocztowy) - aktualny adres (ulica, miejscowość, kod-pocztowy) - służba wojskowa - kod terytorialny - wystawca dowodu - przyczyna złożenia wniosku o wystawienia dowodu	Źródło<-> Magislud Źródło<-> PUMA

2.	Podatki i opłaty lokalne	Zbiór przetwarzany elektronicznie	Pok. 304	Magistrat, PUMA	- imiona i nazwisko - adres zamieszkania lub pobytu - powierzchnia gruntu - powierzchnia mieszkalna i gospodarcza - należność do zapłaty - zaległości w opłatach	- imiona - nazwisko - adres zamieszkania lub pobytu (ulica, miejscowość, kod-pocztowy) - powierzchnia gruntu w ha - powierzchnia mieszkalna i gospodarcza w m2 - należność do zapłaty - zaległości w opłatach	Przepływ danych do/z modułów Kasa i Ewidencja Działalności Gospodarczej
3.	Wpłaty podatku od nieruchomości	Zbiór przetwarzany elektronicznie	Pok. 317	Magistrat, PUMA	- imiona i nazwisko - adres zamieszkania - wysokość opłaty	- imiona -nazwisko - adres zamieszkania (ulica, miejscowość, kod-pocztowy) - wysokość opłaty	Przepływ danych do/z modułów Kasa i Ewidencja Działalności Gospodarczej
4.	Warunki zabudowy i zagospodarowania oraz zmiany planu zagospodarowania terenu	Zbiór przetwarzany elektronicznie	Pok. 207		- imiona i nazwisko - adres zamieszkania lub pobytu	- imiona -nazwisko - adres zamieszkania (ulica, miejscowość, kod-pocztowy)	Brak przepływu
5.	Ewidencja użytkowników wieczystych gruntów	Zbiór przetwarzany w formie papierowej	- Sala Obsługi Klienta - Stanowisko 105 (A.Jurkiewicz)		- imiona i nazwisko - adres zamieszkania lub pobytu - adres i nr działki - powierzchnia i wartość gruntu - wysokość opłaty	- imiona - nazwisko - adres zamieszkania lub pobytu (ulica, miejscowość, kod-pocztowy) - powierzchnia gruntu w ha - nr i rodzaj działki - należność do zapłaty - zaległości w opłatach	
6.	Ewidencja numeracji porządkowej nieruchomości	Zbiór przetwarzany w formie papierowej	- Sala Obsługi Klienta - Stanowisko 105 (M.Cieśla)		- imiona i nazwisko - adres zamieszkania lub pobytu - nr porządkowy nieruchomości miejscowość i nr działki		

7.	Ewidencja najemców lokali mieszkaniowych i użytkowych	Zbiór przetwarzany elektronicznie	Pok. 109	Systemy ADA Czynsze, PUMA	- imiona i nazwisko - adres zamieszkania lub pobytu - adres lokalu - wysokość nadpłaty lub zadłużenia	- imiona - nazwisko - adres zamieszkania lub pobytu (ulica, miejscowość, kod-pocztowy) - adres lokalu (ulica, miejscowość, kod-pocztowy) - wysokość nadpłaty lub zadłużenia	Brak przepływu
8.	Wykaz radnych Gminy Świdnica	Zbiór przetwarzany w formie papierowej	Pok. 204		- imiona i nazwisko - data urodzenia - adres zamieszkania lub pobytu - wykształcenie - numer telefonu - adres zakładu pracy		
9.	Ewidencja właścicieli psów agresywnych	Zbiór przetwarzany w formie papierowej	Pok. 307		- imiona i nazwisko - adres zamieszkania lub pobytu		
10.	Rejestr skarg, wniosków, petycji	Zbiór przetwarzany w formie papierowej	Sekretariat		- imiona i nazwisko - adres zamieszkania lub pobytu - numer telefonu - adres e-mail		
11.	Ewidencja osób posiadających umowę na odbiór odpadów komunalnych i nieczystości	Zbiór przetwarzany elektronicznie	Pok. 310, 311, 115 (Kasa)	**Systemy WYDRA, PUMA**	- imiona i nazwisko - adres zamieszkania lub pobytu - deklarowana ilość osób zamieszkujących lokal - wysokość opłaty	- imiona - nazwisko - adres zamieszkania lub pobytu (ulica, miejscowość, kod-pocztowy)	Brak przepływu

12.	Ewidencja formacji obrony cywilnej i akcji kurierskiej	Zbiór przetwarzany w formie papierowej	Pok. 118		- imiona i nazwisko - data urodzenia - imiona rodziców - adres zamieszkania lub pobytu - zawód - miejsce pracy - stopień wojskowy		
13.	Ewidencja przedpoborowych, poborowych i osób o nieuregulowa-nym obowiązku służby wojskowej	Zbiór przetwarzany w formie papierowej	Pok. 118		- imiona i nazwisko - data urodzenia - imiona rodziców - adres zamieszkania lub pobytu - PESEL - seria i nr dowodu osobistego - wykształcenie zawód		
14.	Rejestr korespondencji	Zbiór przetwarzany w formie papierowej	Sala Obsługi Klienta Stanowisko 100	OpenOffice CALC	- imiona i nazwisko - adres zamieszkania lub pobytu		
15.	Zezwolenia na sprzedaż napojów alkoholowych	Zbiór przetwarzany w formie papierowej	Pok. 109		- imiona i nazwisko - adres zamieszkania lub pobytu		
16.	Oświadczenia radnych o stanie majątkowym	Zbiór przetwarzany w formie papierowej	Pok. 204		- nazwisko i imiona - adres zamieszkania - data urodzenia - seria i nr dowodu osobistego - dane o stanie majątkowym		

17.	Rejestr ofert CV osób ubiegających się o pracę	Zbiór przetwarzany w formie papierowej	Pok. 315		- imiona i nazwisko - data urodzenia - adres zamieszkania lub pobytu - wykształcenie - zawód przebieg dotychczasowego - zatrudnienia - informacja o niekaralności - zainteresowania umiejętności		
18.	Zapis monitoringu wizyjnego terenu wokół budynku Urzędu Gminy (wejścia, parkingi) oraz wnętrza budynku (korytarz).	Zbiór przetwarzany elektronicznie	Sekretariat		- wizerunek osoby - nr rejestracyjny pojazdu - data i godzina rejestracji		Brak przepływu

19.	Pracownicy Urzędu Gminy	Zbiór przetwarzany w formie papierowej	Pok. 315	Systemy KOMAX, PUMA	- PESEL - imiona i nazwisko - płeć - imiona rodziców - obywatelstwo - dowód osobisty (seria numer przez kogo wydany data wydania) - data i miejsce urodzenia - adres zameldowania - adres korespondencyjny - numer telefonu - stan rodzinny - urząd skarbowy - nr świadczenia emerytalnego - stopień niepełnosprawności - przebieg zatrudnienia - wykształcenie (nazwa szkoły rok ukończenia) - tytuł zawodowy - zawód wyuczony - zawód wykonywany - przebyte szkolenia - posiadane uprawnienia - warunki zatrudnienia (umowy) - forma zatrudnienia - forma wynagrodzenia (płaca zasadnicza godzinowa) - wysokość wynagrodzenia	- PESEL - imiona - nazwisko - płeć - imię ojca - imię matki - obywatelstwo - dowód osobisty (seria numer przez kogo wydany data wydania) - data urodzenia - miejsce urodzenia (ulica, miejscowość, kod-pocztowy) - adres zameldowania (ulica, miejscowość, kod-pocztowy) - adres korespondencyjny (ulica, miejscowość, kod-pocztowy) - numer telefonu - stan rodzinny - urząd skarbowy - nr świadczenia emerytalnego - stopień niepełnosprawności - przebieg zatrudnienia - wykształcenie (nazwa szkoły rok ukończenia) - tytuł zawodowy - zawód wyuczony - zawód wykonywany - przebyte szkolenia - posiadane uprawnienia - warunki zatrudnienia (umowy) - forma zatrudnienia	

20.	Płace	Zbiór przetwarzany elektronicznie	Pok. 315	Systemy: KOMAX, PUMA	- imiona i nazwisko - data i miejsce urodzenia - adres zamieszkania lub pobytu - PESEL - NIP - seria i nr dowodu osobistego - wykształcenie - zawód - wynagrodzenie - dodatki do wynagrodzenia - potrącenia - premie - nagrody - składki ZUS	- Imiona - nazwisko - data urodzenia - miejsce urodzenia (ulica, miejscowość, kod-pocztowy) - adres zamieszkania lub pobytu (ulica, miejscowość, kod-pocztowy) - PESEL - NIP - seria i nr dowodu osobistego - wykształcenie - zawód - wynagrodzenie - dodatki do wynagrodzenia - potrącenia - premie - nagrody - składki ZUS	-Przepływ danych z programu Kadrowego Pracownicy Urzędu gminy - Przepływ danych do programu Płatnik, -Przepływ danych do systemu bankowego
21.	Rejestr aktualizacji badań lekarskich	Zbiór przetwarzany w formie papierowej	Pok. 315		- imiona i nazwisko - stanowisko służbowe - orzeczenia lekarskie		

22.	Ewidencja zatrudnionych	Zbiór przetwarzany elektronicznie	Pok. 315	KOMAX, PUMA	- imiona i nazwisko - miejsce urodzenia - imiona rodziców - adres zamieszkania - wykształcenie - data zatrudnienia - wymiar czasu pracy - data zwolnienia	- imiona - nazwisko - miejsce urodzenia (ulica, miejscowość, kod-pocztowy) - imiona rodziców - adres zamieszkania (ulica, miejscowość, kod-pocztowy) - wykształcenie - data zatrudnienia - wymiar czasu pracy - data zwolnienia	Przepływ danych do programu Płace
23.	Karty ewidencji czasu pracy	Zbiór przetwarzany elektronicznie	Pok. 315		- imiona i nazwisko - stanowisko służbowe - czas pracy	- imiona - nazwisko - stanowisko służbowe - czas pracy	
24.	Karty ewidencji obecności	Zbiór przetwarzany w formie papierowej	Sala Obsługi Klienta, Pok. 315, Sekretariat		- imiona i nazwisko - data zatrudnienia - data zwolnienia - wymiar urlopu - etatowość - stopień niepełnosprawności - imiona i nazwisko - data zatrudnienia - data zwolnienia		
25.	Deklaracje wydanych legitymacji	Zbiór przetwarzany w formie papierowej			- nr legitymacji - rodzaj wydanej legitymacji - imiona i nazwisko - data wydania legitymacji - data zwrotu legitymacji - informacje dotyczące utraty legitymacji		

26.	Zwolnienia lekarskie	Zbiór przetwarzany w formie papierowej	Pok. 315		- imiona i nazwisko - PESEL - adres - okres ochrony		
27.	Oświadczenia zgody dot. zgody na potrącenia z wynagrodzeń	Zbiór przetwarzany w formie papierowej	Pok. 315		- imiona i nazwisko - adres - nr konta - nazwa banku - inne tytuły potrąceń np zw zawodowe PZU		
28.	Zbiór zajęć komorniczych i egzekucyjnych	Zbiór przetwarzany w formie papierowej	Pok. 315		- imiona i nazwisko - PESEL - adres - imiona rodziców - nr sprawy - kwota egzekucji		
29.	Praktyki studenckie	Zbiór przetwarzany w formie papierowej	Pok. 315, Sekretariat		- imiona i nazwisko - data i miejsce urodzenia - PESEL - adres zamieszkania - nr telefonu - nazwa uczelni - nr legitymacji studenckiej - nr dowodu osobistego		
30.	Staże studenckie (umowy)	Zbiór przetwarzany w formie papierowej	Pok. 315, Sekretariat		- imiona i nazwisko - adres zamieszkania - nr telefonu - e-mail - nazwa uczelni - rok studiów - wydział uczelni - kierunek studiów - odbyte praktyki - znajomość języków - doświadczenie zawodowe - nr konta bankowego		

31.	Deklaracje przystąpienia do ubezpieczenia grupowego na życie w Urzędzie Gminy Świdnica	Zbiór przetwarzany w formie papierowej	Pok. 315		- imiona i nazwisko - data urodzenia - PESEL - adres - data zatrudnienia - imiona i nazwisko osoby - upoważnionej		
32.	Dokumentacja wypadków pracowników	Zbiór przetwarzany w formie papierowej	Pok. 315		- imiona i nazwisko - imiona rodziców - PESEL - NIP - seria i nr dowodu osobistego - data urodzenia - miejsce urodzenia - adres zamieszkania lub pobytu - stan zdrowia		
33.	Ubezpieczenie ZUS - Informacje o pracownikach potrzebne do ubezpieczenia w ZUS	Zbiór przetwarzany w formie papierowej	Pok. 315		- imię nazwisko - data urodzenia - PESEL - NIP - adres zamieszkania lub pobytu		
34.	Zakładowy Fundusz Świadczeń Socjalnych	Zbiór przetwarzany w formie papierowej	Pok. 316		- imiona i nazwisko - imiona i rok urodzenia dzieci - adres szkoły - imię małżonka - adres zamieszkania lub pobytu - dochody gospodarstwa		
35.	Rejestr zapomóg z Zakładowego Funduszu Świadczeń Socjalnych	Zbiór przetwarzany w formie papierowej	Pok. 316		- imiona i nazwisko - imiona i rok urodzenia dzieci - adres szkoły - imię małżonka - adres zamieszkania lub pobytu - dochody gospodarstwa		

36.	Kasa zapomogowo-pożyczkowa – deklaracje	Zbiór przetwarzany w formie papierowej	Pok. 316		- imiona i nazwisko - data urodzenia - adres - miejsce pracy - nazwisko i imiona żyrantów oraz osób upoważnionych - wysokość pożyczki		
37.	Rejestr udzielonych pożyczek z kasy zapomogowo-pożyczkowej.	Zbiór przetwarzany w formie papierowej	Pok. 316		- imiona i nazwisko - data urodzenia - adres - miejsce pracy - nazwisko i imiona żyrantów oraz osób upoważnionych - wysokość pożyczki		
38.	Ewidencja tytułów wykonawczych (dłużnicy)	Zbiór przetwarzany w formie papierowej	Pok. 317		- imiona i nazwisko - adres zamieszkania/zameldowania - adres korespondencyjny - PESEL - data urodzenia - imiona rodziców - adres e-mail - nr telefonu - adres zakładu pracy. Gdy zachodzi wspólność ustawowa: analogiczne dane współmałżonka. Dla spółek i osób prawnych: dane wszystkich wspólników. - kwota należności - rodzaj należności pieniężnej - zabezpieczenie należności pieniężnej (nr księgi wieczystej)		

39.	Czynsze	Zbiór przetwarzany elektronicznie	Pok. 109	ADA-Czynsze, PUMA	- imiona i nazwisko - adres zasobu (lokalu) - adres korespondencyjny - nazwa firmy - nr konta bankowego - kwota czynszu - kwota zaległości (nadpłaty)	- imiona - nazwisko - adres zasobu (lokalu) - (ulica, miejscowość, kod-pocztowy) - adres korespondencyjny (ulica, miejscowość, kod-pocztowy) - nazwa firmy - nr konta bankowego - kwota czynszu - kwota zaległości (nadpłaty)	Brak przepływu
40.	Ewidencja szkoleń BHP I PPOŻ	Zbiór przetwarzany w formie papierowej	Pok. 204		- imiona i nazwisko - data odbycia przeszkolenia BHP i PPOŻ		
41.	Rejestr zarządzeń	Zbiór przetwarzany w formie papierowej	Sekretariat		- numer zarządzenia - data zarządzenia		
42.	Rejestr delegacji służbowych pracowników	Zbiór przetwarzany w formie papierowej	Sekretariat, Pok. 317		- imię i nazwisko pracownika - data delegacji od do - miejsce wyjazdu służbowego - cel wyjazdu służbowego		
43.	Rejestr wyjazdów szkoleniowych pracowników	Zbiór przetwarzany w formie papierowej	Sekretariat		- imię i nazwisko pracownika - data szkolenia od do - miejsce szkolenia - cel wyjazdu służbowego		

44.	Rejestr faksów	Zbiór przetwarzany w formie papierowej	Sekretariat		- numer faksu - nazwiska, imiona - nazwa adresata/nadawcy - adres adresata/nadawcy - data wysłania/odebrania		
45.	Rejestr umów Urzędu Gminy	Zbiór przetwarzany w formie papierowej	Sekretariat		- imiona i nazwiska stron umowy - adresy stron umowy		
46.	Rejestr działalności lobbingowej	Zbiór przetwarzany w formie papierowej	Sekretariat, BIP		- Imiona i nazwiska - nr wpisu do rejestru podmiotów wykon. zawodowo działalność lobbingową,		
47.	Rejestr szkoleń pracowników	Zbiór przetwarzany w formie papierowej	Sekretariat		- Imiona i nazwiska pracownika - Data i czas szkolenia - Organizator szkolenia - Temat szkolenia - Ocena szkolenia		
48.	Rejestr Skarg i wniosków	Zbiór przetwarzany w formie papierowej	Sekretariat		- Imię i nazwisko, - adres zamieszkania		
49.	Rejestr Skarg na działalność Wójta i Kierowników Działów	Zbiór przetwarzany w formie papierowej	Sekretariat		- Imię i nazwisko, - adres zamieszkania		

50.	Rejestr Korespondencji	Zbiór przetwarzany w formie papierowej	Sekretariat		- Imię i nazwisko, - adres zamieszkania		
51.	Ewidencja Komisji Wyborczych	Zbiór przetwarzany w formie papierowej	Sekretariat		- Imię i nazwisko, - adres zamieszkania		
52.	Spis Wyborców	Zbiór przetwarzany w formie papierowej	104		- Imię i nazwisko, - adres zamieszkania, - Nr PESEL		
53.	Wnioski o udostępnienie informacji publicznej	Zbiór przetwarzany w formie papierowej	213		- Imię i nazwisko, - adres zamieszkania,		

Rejestr czynności przetwarzania danych osobowych

Administrator danych	Urząd Gminy Świdnica ul. Głowackiego 4, 58-100 Świdnica, tel. 74/8523067
Współadministratorzy	
Inspektor Ochrony Danych	Krzysztof Olejniczak

Kategoria osób: Pracownicy obecni i byli, ubiegający się o pracę.

Czynność przetwarzania	Cel przetwarzania	Kategoria danych (dane wrażliwe oznaczone (W))	Podstawa prawna	Czas przetwarzania / Co się dzieje z danymi potem?	Niezbędne (konieczne minimum) / Adekwatne do celu	Kategorie odbiorców	Przekazywane poza ue lub org. międzynarodowej	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa
Prowadzenie rejestru pracowników, akt pracowniczych i ewidencja czasu pracy	Obsługa zatrudnienia, prowadzenie ewidencji pracowników	Imiona, nazwisko adres data urodzenia nr/seria dowodu osobistego PESEL NIP wykształcenie numer konta bankowego stanowisko / zakres obowiązków wysokość wynagrodzenia ilość etatu czas umowy o pracę wysługa lat informacje o karach i nagrodach zwolnienia lekarskie (W) stopień niepełnosprawności (W) akt urodzenia dziecka (w czasie trwania zatrudnienia) akt ślubu akt zgonu członka rodziny informacje o innym zatrudnieniu	Kodeks Pracy art. 22.1	50 lat / niszczone [art. 51u ust. 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r., poz. 217 t.j.)]	Tak / Tak	ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe	Nie	Każda osoba pracująca przy przetwarzaniu danych osobowych została upoważniona do przetwarzania danych osobowych i zobowiązana do zachowania poufności oraz przeszkolona z zasad bezpiecznego przetwarzania danych osobowych. Prowadzona jest ewidencja upoważnień do przetwarzania danych. Przetwarzanie danych odbywa się w pomieszczeniach lub strefach pomieszczeń z ograniczeniem dostępu dla osób nieuprawnionych. Dane w formie papierowej i na nośnikach danych przechowywane w zamkniętych szafach w pomieszczeniach z ograniczonym dostępem Na komputerach używanych do przetwarzania jest zainstalowany regularnie aktualizowany program antywirusowy. Dostęp do programów i danych jest zabezpieczony identyfikatorem użytkownika i hasłem. Regularnie wykonywane kopie zapasowe

Prowadzenie rozliczeń z pracownikami, naliczanie potrąceń, obliczanie składek ZUS	Prowadzenie rozliczeń z pracownikami, naliczanie potrąceń, obliczanie składek ZUS	Imiona, nazwisko adres data urodzenia nr/seria dowodu osobistego PESEL NIP adres numer konta bankowego wysokość wynagrodzenia ilość etatu wysługa lat informacje o nagrodach składki związkowe umowy ubezpieczeniowe PIT zajęcia komornicze (W)	Umowa o pracę. Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2018 r. poz. 108 t.j.) Dział III - Wynagrodzenia; ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz.U. z 2017 r., poz. 1778 t.j.) - art. 1, 6 oraz 6a;	50 lat / niszczone [art. 51u ust. 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r., poz. 217 t.j.)]	Tak / Tak	Banki, urzędy skarbowe, ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe	Nie	jw.
Zgłoszenia pracownika i członków jego rodziny do ZUS, aktualizacja zgłoszenia oraz przekazywanie informacji o zwolnieniach	Zgłoszenia pracownika i członków jego rodziny do ZUS, aktualizacja zgłoszenia oraz przekazywanie informacji o zwolnieniach	Informacja o składkach ZUS	Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych	10 lat / niszczone	Tak / Tak	ZUS, pracownicy	Nie	jw
Rekrutacja	Rekrutacja	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, stażu pracy, uprawnieniach zawodowych.	Kodeks Pracy art. 22.1	Czas rekrutacji / niszczone	Tak / Tak	Dyrektor, pracownicy	Nie	jw
Obsługa stażystów	Obsługa stażystów	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, stażu pracy, uprawnieniach zawodowych.	Kodeks Pracy art. 22.1	Umowy: 50 lat Inne dane niszczone / zwracane do organizacji zlecającej staż	Tak / Tak	Organizacja zlecająca staż	nie	jw
Obsługa praktykantów	Obsługa praktykantów	Dane identyfikacyjne, dane adresowe, dane o wykształceniu	Kodeks Pracy art. 22.1	Czas praktyk / niszczone / zwracane do organizacji zlecającej praktyki	Tak / Tak	Organizacja zlecająca praktyki	nie	jw

Administrator danych	Urząd [illegible]iny Świdnica ul. Głow[illegible]kiego 4, 58-100 Świdnica, tel. 74/8523067
Współadministratorzy	
Inspektor Ochrony Danych	Krzysztof Olejniczak

Kategoria osób: Klienci.

Czynność przetwarzania	Cel przetwarzania	Kategoria danych (dane wrażliwe oznaczone (W))	Podstawa prawna	Czas przetwarzania / Co się dzieje z danymi potem?	Niezbędne (konieczne minimum) / Adekwatne do celu	Kategorie odbiorców	Przekazywane poza ue lub org. międzynarodowej	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa
Prowadzenie rejestru klientów,	Obsługa umów zawartych z UG Świdnica	Imiona, nazwisko adres data urodzenia nr/seria dowodu osobistego PESEL	Kodeks Cywilny	Czas realizacji umowy	Tak / Tak		Nie	Każda osoba pracująca przy przetwarzaniu danych osobowych została upoważniona do przetwarzania danych osobowych i zobowiązana do zachowania poufności oraz przeszkolona z zasad bezpiecznego przetwarzania danych osobowych. Prowadzona jest ewidencja upoważnień do przetwarzania danych. Przetwarzanie danych odbywa się w pomieszczeniach lub strefach pomieszczeń z ograniczeniem dostępu dla osób nieuprawnionych. Dane w formie papierowej i na nośnikach danych przechowywane w zamkniętych szafach w pomieszczeniach z ograniczonym dostępem Na komputerach używanych do przetwarzania jest zainstalowany regularnie aktualizowany program antywirusowy. Dostęp do programów i danych jest zabezpieczony identyfikatorem użytkownika i hasłem. Regularnie wykonywane kopie zapasowe
Prowadzenie rozliczeń z klientami UG Świdnica	Obsługa finansowa realizowanej sprzedaży	Imiona, nazwisko adres data urodzenia nr/seria dowodu osobistego PESEL	Ustawa o rachunkowości	6 lat	Tak / Tak		Nie	jw.

ZAŁACZNIK_PBI_03
Do Polityki Bezpieczeństwa Informacji
UG Świdnica

Procedura zarządzania ryzykiem

I Definicje

Użyte w procedurze określenia oznaczają:

1. analiza ryzyka - systematyczne wykorzystanie informacji do zidentyfikowania źródeł i estymowania ryzyka,
2. następstwo – potencjalną stratę o charakterze materialnym lub niematerialnym wynikającą z incydentu związanego z bezpieczeństwem informacji,
3. ocena ryzyka – działanie polegające na porównywaniu oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka,
4. podatność - słabość zasobu lub grupy zasobów, która może być wykorzystana, przez co najmniej jedno zagrożenie,
5. postępowanie z ryzykiem – działanie polegające na wyborze i wdrażaniu środków modyfikujących ryzyko,
6. program szacowania ryzyka – zaplanowane działania w odniesieniu do wskazanego procesu realizowanego w UG Świdnica podejmowane w celu uszczegółowienia wyników szacowania ryzyka,
7. ryzyko szczątkowe – ryzyko pozostałe po postępowaniu z ryzykiem,
8. scenariusz incydentu – opis sytuacji incydentu związanego z bezpieczeństwem informacji, w której zagrożenie wykorzystuje określoną podatność lub zbiór podatności,
9. szacowanie ryzyka - całościowe działanie polegające na analizie i ocenie ryzyka,
10. zagrożenie - potencjalną przyczynę niepożądanego incydentu, który może wywołać szkodę w systemie lub organizacji,
11. zarządzanie ryzykiem - skoordynowane działania kierowania i zarządzania organizacją z uwzględnieniem ryzyka,
12. źródło - czynnik lub działanie stanowiące potencjalną przyczynę incydentu, w odniesieniu do ryzyka związanego z bezpieczeństwem informacji są identyfikowane źródła ryzyka w postaci zagrożeń i podatności.

II Cele i zadania procesu zarządzania ryzykiem

1. Celem wdrożenia w Urzędu Gminy Świdnica procesu zarządzania ryzykiem jest zapewnienie bezpieczeństwa danych osobowych przetwarzanych w UG ŚWIDNICA jak również zapewnienie w najbardziej możliwy sposób ciągłości działania UG ŚWIDNICA.
2. Do podstawowych zadań opisanych w niniejszej procedurze należą:

a) Identyfikacja i klasyfikacja zasobów (aktywów) UG ŚWIDNICA w zakresie przetwarzania informacji,

b) Zdefiniowanie zagrożeń i podatności,

c) Oszacowanie ryzyk,

d) Określenie zasad postępowania w odniesieniu do poszczególnych klas ryzyka,

e) Wdrożenie procedur zarządzania ryzykiem w UG ŚWIDNICA.

III Role i odpowiedzialności w procesie zarządzania ryzykiem

1. Każdy pracownik UG ŚWIDNICA zobowiązany jest do wspierania procesu zarządzania ryzykiem w szczególności w zakresie monitorowania zagrożeń i podatności.

2. Administrator Danych zapewnia optymalne warunki i niezbędne środki w celu realizacji procesu zarządzania ryzykiem w UG ŚWIDNICA,

3. Inspektor Ochrony Danych koordynuje proces zarządzania ryzykiem. Do jego obowiązków w tym zakresie należy w szczególności:

   a) Analizowanie znaczących zmian w obszarze ryzyka związanego z bezpieczeństwem informacji,

   b) Zatwierdzenie programów szacowania ryzyka,

   c) Inicjowanie zmian w metodyce,

   d) Koordynowanie działań związanych z zarządzaniem ryzykiem,

   e) Przygotowanie raportów z przeglądów systemu zarządzania ryzykiem,

4. Administrator Systemów Informatycznych kieruje procesem zarządzania ryzykiem w obszarze systemów informatycznych. Do jego obowiązków w tym zakresie należy w szczególności:

   a) Zdefiniowanie i klasyfikacja (zasobów) aktywów informatycznych na potrzeby szacowania ryzyka,

   b) Zidentyfikowanie podatności i zagrożeń,

   c) Określanie następstw wystąpienia ryzyka,

   d) Oceny ryzyka,

   e) Przygotowywanie i aktualizacja planów postępowania z ryzykiem,

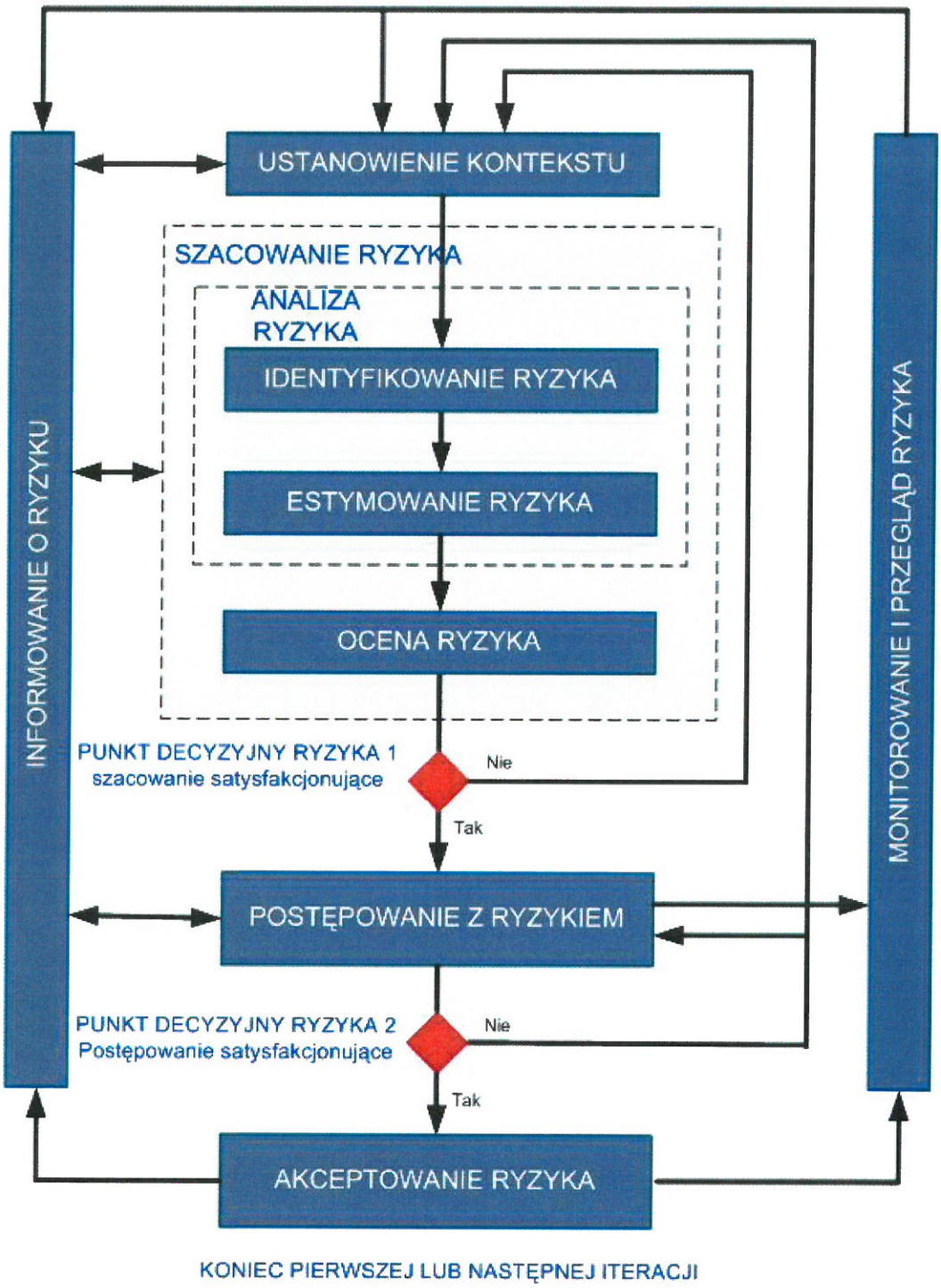
   f) Opracowanie kryteriów szacowania następstw.

5. Zespół ds. bezpieczeństwa informacji opiniuje dokumenty, procedury i instrukcje związane z procesem zarządzania ryzykiem.

6. Właściciele zasobów (Kierownicy Działów) wspierają proces zarządzania ryzykiem poprzez monitorowanie zmian zagrożeń i ich podatności oraz uczestniczenie w procesie kategoryzacji informacji i Systemów Teleinformatycznych oraz zmian warunków funkcjonowania zasobów mających wpływ na szacowanie ryzyka.

IV Proces zarządzania ryzykiem

1. Proces zarządzania ryzykiem dla potrzeb UG ŚWIDNICA został opracowany na podstawie normy ISO/IEC 27005. Główne komponenty procesu zarządzania ryzykiem zostały przedstawione na rysunku 1.



Rysunek 1. Model zarządzania ryzykiem *(na podstawie ISO/IEC 27005)*

2. Komponenty zarządzania ryzykiem.

   a) Wyznaczenie kontekstu – wyznaczenie konteksty strategicznego, organizacyjnego zarządzania ryzykiem. Przyjęcie sposobu szacowania i akceptowania ryzyka,

   b) Szacowanie ryzyka – składa się z analizy ryzyka i oceny ryzyka,

   c) Analiza ryzyka to identyfikacja i estymacja ryzyka,

   d) Identyfikacja ryzyka – obejmuje identyfikowanie zasobów, zagrożeń, podatności i potencjalnych następstw,

   e) Estymacja ryzyka - szacowanie konsekwencji w kontekście istniejących zabezpieczeń technicznych i organizacyjnych,

   f) Ocena ryzyka – porównanie wyznaczonych poziomów ryzyka z ustalonymi kryteriami,

   g) Postępowanie z ryzykiem – opracowanie i wdrożenie planów zarządzania ryzykiem z uwzględnieniem kryteriów oceny ryzyka,

   h) Akceptowanie ryzyka – po rozważeniu wariantów postępowania z ryzykiem ryzyka szczątkowe są akceptowane,

   i) Informowanie o ryzyku – informowanie i konsultowanie się z wszystkimi uczestnikami procesu zarządzania ryzykiem na każdym etapie procesu,

   j) Monitorowanie i przegląd ryzyka – monitorowanie i przegląd ryzyka, jak i procesu zarządzania ryzykiem oraz doskonalenie tego procesu.

3. Programy szacowanie ryzyka opracowuje Administrator Systemów Informatycznych w obrębie analizy zasobów informatycznych.
4. Programy szacowania ryzyka w UG ŚWIDNICA zatwierdza Inspektor Ochrony Danych.
5. Kierownicy działów współpracują z Inspektorem Ochrony Danych oraz Administratorem Bezpieczeństwa Systemów przy opracowywaniu programów szacowania ryzyka w zakresie identyfikacji aktywów, zagrożeń i podatności.
6. Na program szacowania ryzyka składają się działania w następujących obszarach:

   a) Identyfikowanie i klasyfikacja zasobów (aktywów) organizacji. Inwentaryzacja aktywów polega na określeniu grup aktywów, które podlegają ochronie przed incydentami bezpieczeństwa lub niewłaściwym użyciem. Zidentyfikowane grupy zestawiono tabelarycznie poniżej.

L.P.	**Aktywa (grupy aktywów)**
1	Dokumenty (wersja papierowa, wersja elektroniczna, know-how)
2	Media (zasilanie, łączność)
3	Outsourcing
4	Oprogramowanie (własne, zakupione) do przetwarzania danych

5	Infrastruktura IT (sieć wraz z elementami, poczta, Internet)
6	Infrastruktura (obiekty, transport)
7	Pracownicy i współpracownicy

b) Identyfikowanie i klasyfikacja zagrożeń. Poniżej przedstawiono bazę zagrożeń dla poszczególnych grup zasobów (aktywów):

Typ zagrożenia	**Zagrożenia**
Zagrożenia środowiskowe	1. Pożar obiektu/pomieszczeń 2. Zalanie wodą dokumentów/serwera/komputerów 3. Braki zasilania 4. Utrata łączności telefonicznej / internetowej 5. Zamieszki gospodarcze / społeczne / polityczne
Zagrożenia przypadkowe	1. Awarie serwera, komputerów, oprogramowania systemowego, aplikacji 2. Pomyłki informatyków, użytkowników 3. Utrata danych z twardych dysków / nośników 4. Wyrzucenie, porzucenie danych poza organizacją 5. Zagubienie dokumentacji / nośników 6. Utrata kluczowych pracowników
Zagrożenia umyślne	1. Włamanie do systemu informatycznego 2. Włamanie do obiektu/pomieszczeń 3. Kradzież danych / komputerów 4. Nieautoryzowany dostęp do systemu 5. Ujawnienie tajemnicy przedsiębiorstwa lub Danych Osobowych osobom nieupoważnionym 6. Szpiegostwo / podsłuchiwanie danych 7. Świadome zniszczenie / sfałszowanie dokumentów/danych 8. Awaria, zawodność oprogramowania 9. Podszycie się pod uprawnionego użytkownika 10. Błędy użytkowników 11. Infiltracja łączności 12. Podsłuch 13. Utrata poufności, integralności, dostępności informacji

c) Identyfikowanie i klasyfikowanie podatności. Na podstawie danych zebranych w trakcie przeglądu zabezpieczeń wdrożonych i oceny ich skuteczności zbudowano referencyjna bazę podatności zamieszczoną poniżej.

Aktywa	Podatności
Dane/Dokumenty	1. Niechronione przechowywanie 2. Nieodpowiednie niszczenie 3. Niekontrolowane kopiowanie 4. Niechronione przekazywanie 5. Brak dzienników systemów 6. Brak rejestrów systemów 7. Brak ustanowionych mechanizmów monitorowania incydentów bezpieczeństwa 8. Brak listy osób upoważnionych do dostępu do określonej informacji 9. Brak dokumentacji systemów
Media	1. Niestabilna sieć elektryczna 2. Brak alternatywnych dróg połączenia 3. Brak umów 4. Przesyłanie haseł w postaci jawnej 5. Brak dowodu wysłania lub odebrania wiadomości 6. Niechronione połączenia do sieci publicznej
Outsourcing	1. Brak umów 2. Niewłaściwy nadzór
Oprogramowanie	1. Niechronione tablice haseł 2. Złe zarządzanie hasłami (łatwe do odgadnięcia hasła, złe przechowywanie, niedostateczna częstotliwość zmian) 3. Niewłaściwy przydział praw dostępu 4. Brak kontroli pobierania i użytkowania oprogramowania 5. Brak dokumentacji do systemów i aplikacji 6. Brak kopii zapasowych 7. Niedostateczne sprecyzowanie wymagań przy zakupie 8. Brak lub niedostateczne przetestowanie oprogramowania 9. Brak mechanizmów identyfikacji i uwierzytelniania 10. Dobrze znane słabe punkty oprogramowania (tzw. Dziury w oprogramowaniu) 11. Znane podatności baz danych (replikacja) 12. Niekontrolowane instalowanie oprogramowania 13. Usunięcie lub ponowne użycie nośników pamięci bez odpowiedniego skasowania informacji 14. Niewylogowanie się po opuszczenie stanowiska pracy 15. Brak licencji 16. Niewłaściwe użycie oprogramowania 17. Użytkowanie usług/aplikacji powszechnie uznanych za niegwarantujące bezpieczeństwa
Infrastruktura IT	1. Niezabezpieczenie serwerowni 2. Użycie złej jakości sprzętu, niedostateczne wyposażenie 3. Brak UPS 4. Niewłaściwa konserwacja/wadliwa instalacja nośników 5. Brak dokumentacji 6. Błędy instalacyjne nośników pamięci 7. Brak wystarczającej kontroli zmian konfiguracji 8. Usuwanie lub ponowne użycie nośników bez odpowiedniego kasowania ich zawartości 9. Przechowywanie kopii w miejscach wytworzenia 10. Brak rozliczalności działań administratora
Infrastruktura	1. Lokalizacja na terenie zagrożonym powodzią 2. Brak wyposażenia PPOŻ 3. Brak fizycznej ochrony budynku, drzwi i okien 4. Niewłaściwe lub nieuważne użycie fizycznej kontroli dostępu do budynków, pomieszczeń 5. Wrażliwość na wahania napięcia 6. Wrażliwość na wahania temperatury 7. Wrażliwość na wilgoć, kurz, brud 8. Wrażliwość na promieniowanie elektromagnetyczne

	9. Niewłaściwy stan techniczny instalacji grzewczych 10. Niewłaściwy stan techniczny instalacji odgromnych 11. Błąd administratora
Pracownicy i współpracownicy	1. Brak zakresów obowiązków 2. Brak przeszkolenia pracowników z zakresu bezpieczeństwa 3. Brak stosowania „polityki czystego biurka" 4. Kradzież danych 5. Nieobecność personelu 6. Praca personelu zewnętrznego lub sprzątającego bez nadzoru 7. Brak mechanizmów monitorujących 8. Błąd użytkownika systemu 9. Znaczna liczba użytkowników mających dostęp do systemu 10. Niewłaściwe procedury zatrudniania 11. Natura ludzka / niezadowolenie z pracy

d) Identyfikowanie i klasyfikacja następstw zrealizowania się scenariuszy ryzyka. Szacowanie konsekwencji zmaterializowania się ryzyka utraty poufności, integralności i dostępności informacji obejmuje ich wartościowanie z punktu widzenia możliwych następstw (skutków) i prawdopodobieństwa realizacji. W celu wyznaczenia ryzyk określa się parametry liczbowe:

Prawdopodobieństwo wystąpienia zagrożeń

PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	**WAGA**
Niskie	1
Średnie	2
Wysokie	3

Skutki wystąpienia ryzyka

SKUTKI	**WAGA**	**OPIS**
Małe	1	Incydent prasowy, złamanie zasad etyki zawodowej, brak strat finansowych, krótkotrwała niedostępność zasobów
Średnie	2	Wszczęcie postępowania karnego, naruszenie przepisów wewnętrznych, trwała niedostępność zasobów podstawowych, strata finansowa do 20 000 PLN
Duże	3	Naruszenie przepisów ustawowych, niedostępność zasobów krytycznych i ważnych, utrata poziomu bezpieczeństwa informacji ważnej i krytycznej, strata finansowa powyżej 20 000 PLN

e) Ocena w(wyznaczenie) poziomu ryzyka. Poziom **ryzyka** wyliczony formułą:
Ryzyko = Prawdopodobieństwo wystąpienia zagrożenia (waga) * Skutki (waga) [**R = P*S**]

POZIOM RYZYKA	**WARTOŚĆ [R = P*S]**
Ryzyko pomijalne i akceptowalne	1-2
Ryzyko opcjonalne	3-6
Ryzyko nieakceptowalne	9

7. Wyliczenie i ocena ryzyka

a) Za wyliczenie ryzyk odpowiedzialny jest Administrator Systemów Informatycznych.

b) Krok 1 wyznaczenie zagrożeń

- Dla każdego aktywu wyznaczana jest lista charakterystycznych zagrożeń. Ich wyboru dokonuje się z listy typowych zagrożeń zawartych,
- Zagrożenie (analizowane dla danego aktywu) uważa się za wyznaczone, gdy istnieją podatności, które mogą spowodować zmaterializowanie się tego zagrożenia,
- Wyznaczone zagrożenia dla wszystkich aktywów umieszcza się w dokumencie Arkusz analizy ryzyka.

c) Krok 2 – wyliczenie ryzyk

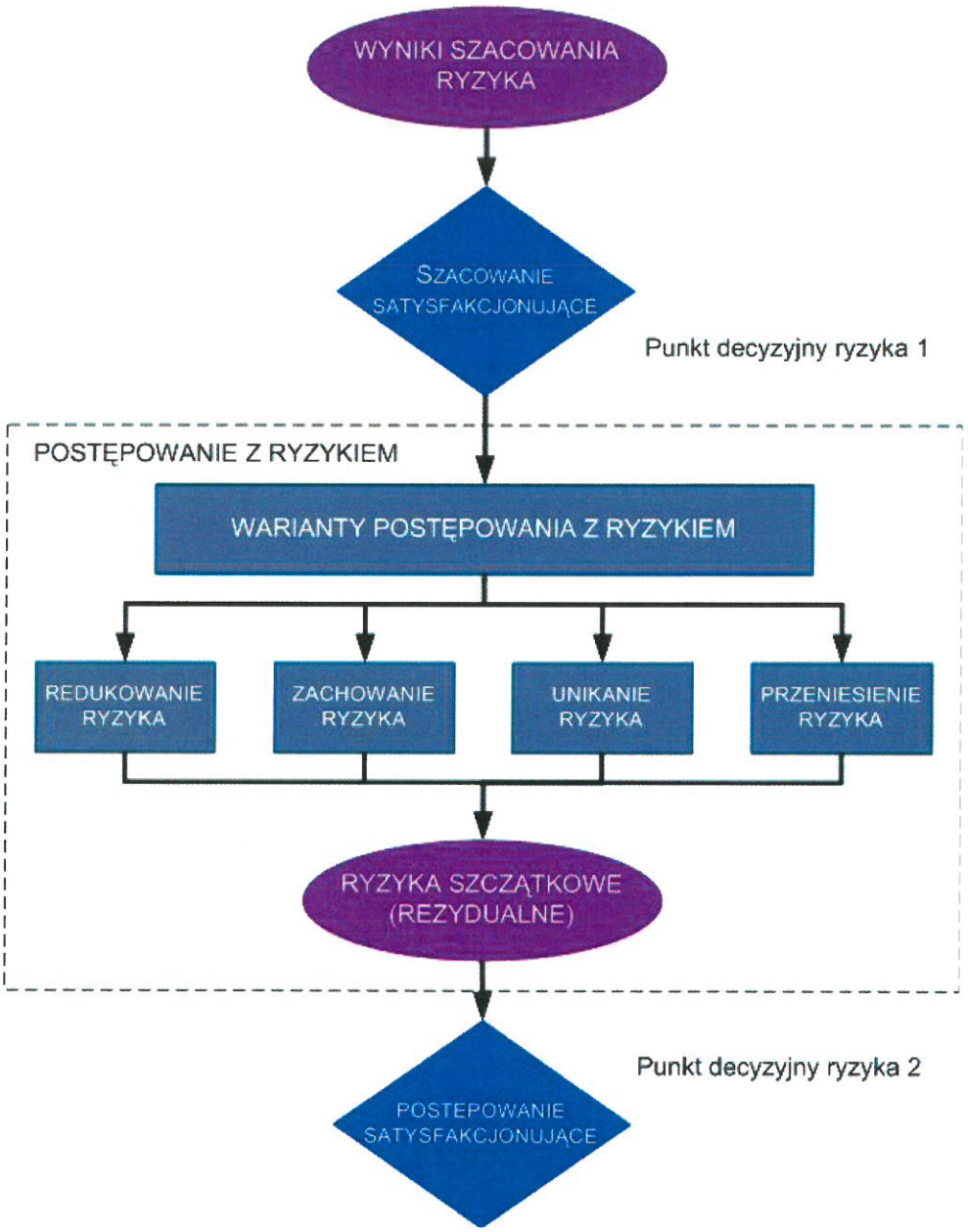
- Dla każdego zagrożenia określa się liczbowo prawdopodobieństwo jego wystąpienia zgodnie z wagami określonymi w tabeli: **Prawdopodobieństwo wystąpienia zagrożenia.** Wartości wyznacza się dla wszystkich aktywów, gdzie dane zagrożenie może wystąpić,
- Dla każdego zagrożenia określa się liczbowo skutki jego wystąpienia (w podziale na skutki utraty poufności, skutki utraty dostępności oraz skutki utraty integralności), zgodnie ze skalą określoną w tabeli: **Skutki**. Do **Arkusza Analizy ryzyka** wpisywana jest najwyższa wartość spośród skutków utraty poufności/dostępności/integralności
- Ryzyko dla danego zagrożenia jest wyliczane według formuły opisanej w tabeli: **Poziom ryzyka**.

d) Krok 3 – ocena ryzyka

- Jeżeli wyliczone ryzyko (**R**) wynosi 1 lub 2, wówczas jest akceptowalne i nie wymaga podejmowania czynności mających na celu jego obniżenie
- Jeżeli wyliczone ryzyko (**R**) wynosi 3 lub 4 lub 6, wówczas uznane jest za opcjonalne, czyli wymagające podjęcia decyzji, czy ryzyko pozostanie niezmienione, czy podjęte będą czynności mające na celu jego obniżenie
- Jeżeli wyliczone ryzyko (**R**) wynosi 9, ryzyko uznaje się za nieakceptowalne a co za tym idzie wymagane jest podjęcie działań mających na celu jego obniżenie

8. Wybór wariantów postępowania z ryzykami.

W UG ŚWIDNICA przyjmuje się następujący model postępowania z ryzykami:



W zależności od wyników uzyskanych w procesie oceny ryzyka, możliwe są następujące scenariusze:

- Zastosowanie odpowiednich zabezpieczeń mających na celu **redukowanie (obniżenie)** ryzyka do poziomu akceptowalnego.
  Wybór powinien być uzasadniony kryteriami akceptowania ryzyka, jak również wymaganiami prawnymi, regulacyjnymi. Analiza doboru zabezpieczeń wykonywana jest w aspekcie technicznym, organizacyjnym i finansowym. Jej celem jest ocena, w jaki sposób zastosowane zabezpieczenia mogą zmniejszyć prawdopodobieństwo lub skutki wystąpienia danego zagrożenia. Analizę wykonuje Administrator Systemów Informatycznych.

Analiza powinna brać pod uwagę:

- Istniejącą infrastrukturę organizacyjną i techniczną, oraz ewentualną konieczność wprowadzenia w niej zmian,
- Parametry techniczne wdrożenia,
- Planowane zmiany w chronionych zasobach lub wprowadzenia nowych zasobów,
- Wpływ środków ochrony na chroniony zasób: utrudnienie w dostępie do danych lub zmniejszenie wydajności procesu,

Należy stosować zabezpieczenia określone w normie ISO 27001 lub w § 20 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Wyboru dokonuje się z uwzględnieniem kosztów danego środka ochrony oraz spodziewanego ograniczenia ryzyka w wyniku zastosowania danego zabezpieczenia.

- **Zachowanie (zaakceptowanie)** ryzyk w sposób świadomy i obiektywny, przy założeniu, że jasno spełniają warunki wyznaczone w polityce organizacji oraz kryteria akceptowania ryzyk. Ryzyko jest akceptowalne wobec korzyści, które przynoszą zasoby podlegające ryzyku.
- **Unikanie** ryzyk. Rezygnacja z zagrożonego zasobu (np. rezygnacji z określonego procesu lub danego obszaru działalności). Ryzyko jest na tyle duże wobec korzyści, które przynoszą zagrożone zasoby, że nie może być zaakceptowane. Brak opłacalnych środków ochrony, które mogłyby ograniczyć ryzyko.
- **Przeniesienie** ryzyk na innych uczestników, np. ubezpieczycieli, dostawców.

9. Informowanie o ryzyku

a) W UG ŚWIDNICA powinno ustanowić procedury informowania o ryzyku realizowane na styku kierownictwa i pozostałych uczestników tego procesu,

b) Plany informowania o ryzyku powinny uwzględniać zarówno normalny przebieg procesów ustawowych, statutowych, jak i działania w sytuacjach nadzwyczajnych,

c) Należy opracować procedury komunikacji między wewnętrznymi oraz zewnętrznymi uczestnikami procesu (np. organami nadzorującymi), ze szczególnym uwzględnieniem komórek odpowiedzialnych za wizerunek UG ŚWIDNICA.

10. Monitorowanie i przegląd procesu zarządzania ryzykiem w UG ŚWIDNICA

a) Poziom ryzyka w organizacji powinien być ciągle aktualizowany przez monitorowanie jego następujących elementów:

- nowych lub zwiększonych zagrożeń pojawiających się zarówno na zewnątrz, jak i wewnątrz UG ŚWIDNICA,
- szacowaniu prawdopodobieństwa zdarzeń,

- analizowaniu, czy nowe lub zwiększone podatności mogą umożliwić zagrożeniom ich wykorzystanie,
- analizowaniu zwiększonych konsekwencji szacowanych zagrożeń, podatności i ryzyk, których agregacja może spowodować przekroczenie kryteriów akceptacji ryzyka.

b) Przebieg procesu monitorowania ryzyka sprawia, że należy zapewnić ciągłą dostępność zasobów organizacyjnych i technicznych, które mogą go realizować.

c) Proces monitorowania ryzyka obejmuje ponadto regularną weryfikację kryteriów i wartości progowych używanych do pomiaru ryzyka oraz jego elementów, zapewniając, że są one spójne z celami ustawowymi, statutowymi, strategiami i politykami a zmiany w tym zakresie są odpowiednio adresowane w procesie zarządzania ryzykiem.

d) Monitorowanie i przegląd procesu zarządzania ryzykiem dotyczy w szczególności:
   - kontekstu prawnego i umownego UG ŚWIDNICA,
   - kryteriów szacowania ryzyka,
   - kategorii zasobów i ich wartościowania,
   - kryteriów akceptowania ryzyka,
   - kontrolowania kosztów zarządzania ryzykiem.

ZAŁACZNIK_PBI_04
Do Polityki Bezpieczeństwa Informacji
w UG Świdnica

Procedura przetwarzania danych wrażliwych

1. Dane osobowe zawierające dane wrażliwe są przetwarzane w Urzędzie Gminy Świdnica w celu:
   a) Ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora;
   b) Niezbędnym do dochodzenia spraw przed sądem;
   c) Niezbędnym do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie;
   d) Realizacji praw i obowiązków wynikających z orzeczenia wydanego w postepowaniu sądowym lub administracyjnym.

2. Dokumenty zawierające dane wrażliwe nie podlegają kopiowaniu.

3. Materiałom zawierającym dane wrażliwe nadaje się klauzulę DW.

4. Obrót dokumentami lub materiałami zawierającymi dane wrażliwe musi być tak zorganizowany, by w każdej chwili można było określić miejsce ich przechowywania.

5. Przesyłanie dokumentów lub materiałów zawierających dane wrażliwe w formie papierowej musi być rejestrowane zgodnie z obowiązującą instrukcją.

6. Dystrybucja dokumentów lub materiałów zawierających dane wrażliwe odbywa się wyłącznie do imiennie wskazanego adresata.

7. Podczas przesyłania dokumenty lub materiały zawierające dane wrażliwe muszą być zabezpieczone przed wglądem osób nieupoważnionych do ich analizowania.

8. Dokumenty lub materiały zawierające dane wrażliwe nie podlegają skanowaniu.

9. Dokumenty lub materiały zawierające dane wrażliwe muszą być przechowywane w szafie zamykanej na klucz.

10. Archiwizacja dokumentów lub materiałów zawierających dane wrażliwe odbywa się zgodnie z obowiązującymi w UG Świdnica instrukcjami.

ZAŁACZNIK_PBI_05
Do Polityki Bezpieczeństwa Informacji
w UG Świdnica

Warunki dostępu Osoby Trzeciej do Systemów lub Zasobów Teleinformatycznych UG Świdnica

I. Definicje

Użytym poniżej wyrażeniom nadaje się poniższe znaczenie wyłącznie na potrzeby niniejszego załącznika:

Bezpieczeństwo Informacji – stan, w którym na każdym etapie Przetwarzania, zapewnione są równocześnie: poufność, integralność, rozliczalność, dostępność i autentyczność w rozumieniu Normy PN-I-13335-2 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych.

Dostęp lokalny – dostęp do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA realizowany z urządzeń podłączonych bezpośrednio do Sieci Wewnętrznej UG ŚWIDNICA lub dostęp realizowany bezpośrednio do Systemów Teleinformatycznych.

Dostęp zdalny - dostęp do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA realizowany spoza Sieci Wewnętrznej UG ŚWIDNICA.

Incydent Bezpieczeństwa – każde wykryte naruszenie lub wykryta próba naruszenia Bezpieczeństwa Informacji. Źródłem Incydentu Bezpieczeństwa może być zarówno przypadkowe, jak i celowe działanie albo jego zaniechanie przez Użytkowników.

Informacje – dane Przetwarzane przy użyciu Systemów Teleinformatycznych, niezależnie od ich formy (pliki, rekordy bazy danych, e-mail, obrazy dokumentów, zapis na taśmach DDS/DLT itp.) i celu Przetwarzania.

Kontrahent – strona umowy, osoba fizyczna, osoba prawna lub jednostka organizacyjna nie posiadająca osobowości prawnej współpracująca z UG ŚWIDNICA na podstawie odrębnej umowy; w wewnętrznych aktach normatywnych zwany Osobą Trzecią.

Przetwarzanie – jakiekolwiek operacje wykonywane na danych przy użyciu Systemów Teleinformatycznych, w szczególności takie jak ich zbieranie, utrwalanie, przechowywanie, opracowywanie, modyfikowanie, udostępnianie, przesyłanie i usuwanie.

Sieć UG ŚWIDNICA - sieć teleinformatyczna, składająca się z sieci lokalnych (LAN), stanowiąca własność UG ŚWIDNICA., wykorzystywana na potrzeby UG ŚWIDNICA.

System Teleinformatyczny (System) – zespół środków technicznych wraz z oprogramowaniem, stanowiący integralną i logiczną całość wyodrębnioną ze względu na dostarczaną funkcjonalność przy założeniu, że głównym jego celem jest Przetwarzanie Informacji.

Użytkownik – każda osoba zaangażowana ze strony Kontrahenta w realizację umowy, mająca uprawniony dostęp do Systemu Teleinformatycznego lub Zasobu Teleinformatycznego UG ŚWIDNICA

Zasób Teleinformatyczny – Informacje oraz przetwarzający je System Teleinformatyczny wraz z procesami zaangażowanymi w jego zarządzanie, rozwój, utrzymanie, bezpieczeństwo i eksploatację.

Warunki - Warunki dostępu Kontrahenta do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA

II. Ogólne zasady dostępu Kontrahenta do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA

1. Dostęp Kontrahenta do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA może odbywać się wyłącznie na zasadach określonych w niniejszych Warunkach oraz zgodnie z zasadami obowiązującymi w UG ŚWIDNICA.
2. Kontrahent, który w ramach wykonywania umowy głównej posiada dostęp do danych osobowych musi przed uzyskaniem dostępu podpisać umowę o powierzeniu danych osobowych do przetwarzania.
3. Kontrahent zobowiązany jest wykorzystywać przyznany dostęp do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA wyłącznie w celach i w zakresie uzasadnionym realizacją zadań wynikających z przedmiotu umowy, zgodnie z umową oraz obowiązującymi przepisami prawa.
4. Kontrahent zobowiązany jest zapewnić właściwą ochronę udostępnionych mu Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA, polegającą w szczególności na zapewnieniu zespołu środków organizacyjnych, technicznych i prawnych stosowanych w celu zapewnienia Bezpieczeństwa Informacji.
5. Kontrahent w związku z dostępem do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA ma obowiązek stosować się do zaleceń oraz wymagań UG ŚWIDNICA mających na celu zapewnienie Bezpieczeństwa Informacji, w tym m.in. zapoznać Użytkowników i zapewnić przestrzeganie wskazanych przez UG ŚWIDNICA zasad bezpiecznego użytkowania Systemu Teleinformatycznego oraz zasad bezpiecznego użytkowania środowiska biurowego. Kontrahent jednocześnie zapewnia, że dostęp do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA będą posiadać wyłącznie uprawnieni i przeszkoleni Użytkownicy, w zakresie i na czas niezbędny do realizacji przez nich przedmiotu Umowy,
6. UG ŚWIDNICA wyznacza Opiekuna Kontrahenta (zwanego Opiekunem Osoby Trzeciej w wewnętrznych aktach normatywnych UG ŚWIDNICA), który sprawuje nadzór nad korzystaniem przez Kontrahenta z dostępu do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA

   Zmiana osób pełniących obowiązki ww. opiekunów może być dokonana poprzez złożenie przez każdą ze stron umowy stosownych pisemnych oświadczeń na adres wskazany przez strony do korespondencji i nie wymaga konieczności sporządzania pisemnego aneksu.
7. Wszelkie oprogramowanie wykorzystywane w ramach realizacji przedmiotu umowy musi być użytkowane z poszanowaniem praw własności intelektualnej, w szczególności zgodnie z ustawą o prawie autorskim i prawach pokrewnych.
8. Kontrahent ponosi pełną odpowiedzialność za działania Użytkowników w Systemach lub Zasobach Teleinformatycznych UG ŚWIDNICA oraz za wszelkie szkody powstałe w związku z korzystaniem przez Kontrahenta z dostępu do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA w sposób sprzeczny z niniejszymi Warunki.

9. Brak dostępu do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA po stronie Kontrahenta, wynikający z przyczyn leżących po jego stronie, nie wyłącza odpowiedzialności Kontrahenta z tytułu prawidłowego wykonania Umowy.

III. Tryb przyznawania i odbierania Kontrahentowi dostępu do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA

1. Dostęp do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA przyznaje się Kontrahentowi jedynie na czas i w zakresie niezbędnym do właściwego wykonywania przedmiotu umowy.
2. Dostęp do Zasobów Teleinformatycznych UG ŚWIDNICA odbywa się jedynie na podstawie „Wniosku o Dostęp Osoby Trzeciej do Zasobów Teleinformatycznych UG ŚWIDNICA.". Na żądanie UG ŚWIDNICA Kontrahent ma obowiązek udzielić wszelkich informacji niezbędnych dla przyznania mu dostępu do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA. Niekompletność wniosku będzie stanowić podstawę do zwrotu wniosku bez rozpatrzenia do wnioskodawcy, w celu jego uzupełnienia.
3. Kontrahentowi przyznaje się dostęp do Zasobów Teleinformatycznych UG ŚWIDNICA na czas określony, nie dłuższy niż 6 miesięcy. Po upływie tego czasu, przedłużenie dostępu Kontrahenta do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA może nastąpić wyłącznie po ponownej weryfikacji zakresu oraz warunków jego przyznania, z zachowaniem procedur, o których mowa w niniejszych Warunkach.
4. Dostęp do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA jest odbierany Kontrahentowi niezwłocznie w następujących przypadkach:
   1) z upływem czasu, na który dostęp został przyznany,
   2) jeśli dalszy dostęp do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA nie jest niezbędny Kontrahentowi do realizacji umowy,
   3) w wyniku decyzji osób upoważnionych do wyrażenia zgody na dostęp,
   4) w wyniku decyzji osób odpowiedzialnych za zarządzanie bezpieczeństwem Systemów Teleinformatycznych w UG ŚWIDNICA lub osoby przez niego upoważnionej o zablokowaniu Kontrahentowi lub Użytkownikowi, ze skutkiem natychmiastowym, przyznanego dostępu w przypadku, gdy dalszy dostęp Kontrahenta do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA zagraża Bezpieczeństwu Informacji lub w przypadku stwierdzenia rażącego naruszenia przez Kontrahenta lub Użytkowników postanowień niniejszych Warunków.

IV. Incydenty bezpieczeństwa

1. Kontrahent zobowiązany jest do niezwłocznego zgłaszania wszelkich zauważonych zdarzeń, które noszą znamiona lub są Incydentami Bezpieczeństwa do Opiekuna Kontrahenta oraz udzielania wszelkich niezbędnych informacji oraz wsparcia pracownikom UG ŚWIDNICA zaangażowanym, z racji pełnionych obowiązków, w proces obsługi Incydentów Bezpieczeństwa.
2. UG ŚWIDNICA zastrzega sobie prawo do zbierania i zabezpieczania wszelkich dowodów wskazujących na wystąpienie i powstanie skutków Incydentu Bezpieczeństwa, w szczególności prawo do wystąpienia do każdego z Użytkowników z pisemnym żądaniem niezwłocznego włączenia się w obsługę Incydentu Bezpieczeństwa, w tym niezwłocznego podania wszelkich niezbędnych informacji w zakresie badanego Incydentu Bezpieczeństwa. O fakcie takiego wystąpienia wraz ze wskazaniem osób upoważnionych do żądania ww. informacji UG ŚWIDNICA zobowiązany jest niezwłocznie powiadomić Kontrahenta.

V. Uprawnienia kontrolne UG ŚWIDNICA

1. UG ŚWIDNICA zastrzega sobie prawo do przeprowadzenia kontroli zastosowanych przez Kontrahenta rozwiązań organizacyjno-technicznych, zgodności zaimplementowanych mechanizmów bezpieczeństwa z obowiązującym prawem i niniejszymi Warunkami oraz sposobu korzystania przez Użytkowników z udostępnionych im Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA
2. Kontrola może być przeprowadzona w dniach roboczych w godz. 8.00 – 15.00, w terminie ustalonym przez UG ŚWIDNICA i przekazanym pisemnie do wiadomości Kontrahenta, z co najmniej 2 - dniowym wyprzedzeniem.
3. Kontrahent zobowiązany jest do umożliwienia przeprowadzenia kontroli w szczególności poprzez:
   1) umożliwienie osobom kontrolującym wstępu do pomieszczeń, w których jest wykonywana działalność związana z umową,
   2) zapewnienie osobom kontrolującym dostępu do wszelkich wymaganych informacji, urządzeń oraz Systemów Teleinformatycznych wykorzystywanych do realizacji umowy oraz Użytkowników i dokumentów Kontrahenta w zakresie wynikającym z niniejszej Umowy,
   3) udzielanie osobom kontrolującym przez osoby zaangażowane w realizację umowy ze strony Kontrahenta wyjaśnień w żądanej formie - pisemnej lub ustnej w zakresie wynikającym z realizacji przedmiotu niniejszej Umowy.
4. W przypadku stwierdzenia uchybień w zakresie objętym kontrolą, UG ŚWIDNICA ma prawo wezwać Kontrahenta do podjęcia działań w celu ich usunięcia w wyznaczonym terminie. Nie usunięcie uchybień w wyznaczonym terminie, może stanowić podstawę do wypowiedzenia umowy.

VI. Realizacja dostępu do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA

1. Kontrahent jest zobowiązany do zapewnienia, przy dochowaniu najwyższej staranności, właściwej ochrony udostępnionych przez UG ŚWIDNICA Systemów lub Zasobów Teleinformatycznych, w tym w szczególności wdrożenia po stronie Kontrahenta organizacyjno – technicznych mechanizmów gwarantujących:
   - dostęp do Systemów lub Zasobów Teleinformatycznych wyłącznie dla Użytkowników;
   - rozliczalność Użytkowników, rozumianą jako możliwość jednoznacznego przypisania działań prowadzonych w Systemie lub Zasobie Teleinformatycznym UG ŚWIDNICA do konkretnego Użytkownika.
2. Realizując wymagania, o których mowa w pkt 1 Kontrahent zapewni w szczególności:
   1) ochronę wszelkich udostępnionych mu przez UG ŚWIDNICA urządzeń, a także wszystkich komponentów sprzętowych (np. karty PKI, tokeny) oraz programowych (np. dedykowanej aplikacji) oraz wszelkich informacji (np. loginy i hasła) przed dostępem osób nieuprawnionych;
   2) skuteczne mechanizmy organizacyjne i techniczne uniemożliwiające Użytkownikom:
   a) dokonywanie ominięć, wyłączeń, usunięć czy też innych działań powodujących nieskuteczność zastosowanych przez UG ŚWIDNICA technicznych mechanizmów bezpieczeństwa Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA;

b) podejmowanie działań, które pośrednio lub bezpośrednio mogą prowadzić do naruszenia bezpieczeństwa udostępnionych Systemów lub Zasobów.

3. W przypadku rozpoznanych i ujawnionych do publicznej wiadomości luk bezpieczeństwa w systemie teleinformatycznym lub oprogramowaniu działającym na jego dowolnym komponencie, Kontrahent zobowiązany jest do niezwłocznego wprowadzenia odpowiedniej aktualizacji (poprawki bezpieczeństwa) eliminującej rozpoznaną lukę bezpieczeństwa w jego systemie teleinformatycznym lub oprogramowaniu. W sytuacji, gdy Kontrahent o wystąpieniu luki bezpieczeństwa, o której mowa w zadaniu poprzednim, zostanie zawiadomiony przez UG ŚWIDNICA, jest on zobowiązany wprowadzić odpowiednią aktualizację w terminie wskazanym przez UG ŚWIDNICA. Jeżeli Kontrahent nie dokona niezbędnych i wymaganych aktualizacji w wyznaczonym przez UG ŚWIDNICA terminie, UG ŚWIDNICA zastrzega sobie prawo eliminacji ujawnionej luki bezpieczeństwa we własnym zakresie, przy czym nie będzie to miało wpływu na ważność pozostałych postanowień tej Umowy.
4. Standardy zabezpieczeń dla urządzeń wykorzystywanych przy realizacji dostępu Kontrahenta do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA.

4.1 Standardy zabezpieczeń dla urządzeń będących własnością UG ŚWIDNICA

1) Zabrania się Kontrahentowi samodzielnego dokonywania zmian w konfiguracji i oprogramowaniu urządzeń udostępnionych przez UG ŚWIDNICA do realizacji dostępu do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA, w tym w szczególności podejmowania jakichkolwiek działań powodujących nieskuteczność zastosowanych środków technicznych służących zapewnienia bezpieczeństwa Zasobów Teleinformatycznych.
2) UG ŚWIDNICA zastrzega sobie prawo do pełnej kontroli udostępnionych Kontrahentowi urządzeń, z których jest umożliwiony dostęp Kontrahenta do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA

4.2 Standardy zabezpieczeń dla urządzeń nie będących własnością UG ŚWIDNICA

1) Urządzenia Kontrahenta, wykorzystywane przez niego do realizacji dostępu do Zasobów Teleinformatycznych UG ŚWIDNICA nie mogą zagrażać bezpieczeństwu Systemów lub Zasobów Teleinformatycznych udostępnionych przez UG ŚWIDNICA. W szczególności Kontrahent zobowiązany jest do zastosowania odpowiednich zabezpieczeń chroniących Systemy lub Zasoby Teleinformatyczne UG ŚWIDNICA przed oprogramowaniem złośliwym (np. wirusami, robakami, itd.).
2) Urządzenia Kontrahenta, o których mowa w ust. 1 muszą być chronione w sposób uniemożliwiający bezpośrednie lub pośrednie pozyskanie przez osoby nieupoważnione dostępu do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA. Kontrahent w szczególności ma obowiązek wyeliminować możliwość przejęcia kontroli nad tymi urządzeniami lub ich wykorzystanie w trakcie komunikacji z Systemami / Zasobami Teleinformatycznymi UG ŚWIDNICA.

3) Urządzenia oraz oprogramowanie, z których korzysta Kontrahenta nie mogą powodować wykorzystania Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA (w tym zasobów sieciowych) ponad zakres niezbędny do wykonywania działań niezbędnych do realizacji przedmiotu umowy oraz wynikających z zakresu przyznanego dostępu oraz powodować niedostępność Zasobów Teleinformatycznych UG ŚWIDNICA.

5. Warunki realizacji Dostępu do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA.

5.1 Warunki realizacji Dostępu Zdalnego do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA.

1) Zdalny Dostęp do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA może odbywać się wyłącznie za pośrednictwem bezpiecznego punktu styku kontrolowanego i administrowanego przez UG ŚWIDNICA.
2) komunikacja z siecią UG ŚWIDNICA musi być chroniona kryptograficznie,
3) dostęp do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA wymaga zastosowania mechanizmów uwierzytelniających.
4) kanały komunikacyjne zestawiane na potrzeby dostępu do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA mogą być wykorzystywane tylko i wyłącznie przez Użytkowników w zakresie zarówno czasowym, jak i funkcjonalnym nie wykraczającym poza zakres wynikający z przedmiotu umowy.

5.2. Warunki realizacji Dostępu Lokalnego do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA.

1) dostęp lokalny do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA może odbywać się wyłącznie w miejscach do tego przeznaczonych i wskazanych przez UG ŚWIDNICA
2) UG ŚWIDNICA zastrzega sobie prawo do kontroli urządzeń nie będących własnością UG ŚWIDNICA, a wykorzystywanych przez Osobę Trzecią do realizacji dostępu do Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA w celu stwierdzenia, czy ich podłączenie nie spowoduje zagrożenia dla bezpieczeństwa Systemów lub Zasobów Teleinformatycznych UG ŚWIDNICA. Negatywna ocena skutkuje zakazem wykorzystania danego urządzenia do realizacji Dostępu Lokalnego do czasu usunięcia stwierdzonych w trakcie kontroli zagrożeń.

ZAŁACZNIK_PBI_06
Do Polityki Bezpieczeństwa Informacji
w UG Świdnica

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia .....w ..... pomiędzy:

zawarta dnia .....w ..... pomiędzy:

Urzędem Gminy Świdnica
Ul. Głowackiego 4, 58 -100 Świdnica

reprezentowanym przez Wójta –

zwanym dalej Administratorem Danych,

a

.....

zwanym dalej Zleceniobiorcą

§ 1
Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Zleceniobiorcy, w trybie art. 28 ogólnego Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (zwanego w dalszej części „RODO"), dane osobowe do przetwarzania zgodnie z zapisami i w celu realizacji niniejszej Umowy powierzenia danych osobowych zwanej dalej „Umową".
2. Zleceniobiorca zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Zleceniobiorca zobowiązuje się stosować ochronę powierzonych danych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem (zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych) oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (zgodnie z zasadą „integralność i poufność").

§ 2
Zakres i cel przetwarzania danych

Zleceniobiorca będzie przetwarzał, powierzone na podstawie umowy dane osobowe w postaci ..... wyłącznie w celu ..... zgodnie z zapisami umowy głównej nr .....

§ 3
Obowiązki podmiotu przetwarzającego

1. Zleceniobiorca zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
2. Zleceniobiorca jako podmiot przetwarzający niniejszym oświadcza, że zna zasady ochrony danych osobowych oraz obowiązki podmiotu przetwarzającego wynikające z przepisów obowiązującego prawa, w szczególności z RODO.
3. Zleceniobiorca niniejszym oświadcza i gwarantuje, że jako profesjonalista przetwarzający dane osobowe w imieniu innych podmiotów, posiada wymagane, niezbędne zasoby ludzkie (w tym należycie wykwalifikowany personel w liczbie adekwatnej do zakresu i celu świadczonych przez Zleceniobiorcę usług), infrastrukturę teleinformatyczną, oprogramowanie (w tym zapobiegające naruszeniom ochrony danych osobowych oraz zapewniające realizację zasady rozłączalności wynikającą z art. 5 ust. 2 RODO), sprzęt komputerowy oraz warunki umożliwiające należyte wykonanie Umowy na najwyższym profesjonalnym poziomie oczekiwanym od podmiotów prowadzących działalność gospodarczą.
4. Zleceniobiorca oświadcza, że od momentu rozpoczęcia przetwarzania danych osobowych w imieniu Administratora danych, aż do dnia zaprzestania tego przetwarzania, będzie przetwarzał te dane osobowe zgodnie z przepisami obowiązującego prawa, postanowieniami Umowy oraz wyłącznie na polecenie Administratora.
5. Zleceniobiorca zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy i zobowiąże osoby uprawnione do przetwarzania tych danych do zachowania poufności zarówno w trakcie zatrudnienia ich u Zleceniobiorcy, jak i po jego ustaniu.
6. Postanowienia Umowy nie wyłączają możliwości aby Zleceniobiorca występował w charakterze samodzielnego Administratora względem danych osobowych, o których mowa w § 2, o ile taki status będzie wynikał w szczególności z obowiązujących przepisów prawa. Umowa nie znajduje zastosowania w zakresie w jakim Zamawiający, w związku z wykonywaniem umowy głównej, przetwarza Dane Osobowe otrzymane od Administratora danych na podstawie przepisów powszechnie obowiązującego prawa.

7. Zleceniobiorca po zakończeniu świadczenia usług, zobowiązany jest do usunięcia powierzonych danych osobowych (oraz wszystkie ich kopie i kopie zapasowe) z wszystkich nośników, programów i aplikacji, chyba że wymogi prawne, wynikające z przepisów prawa powszechni obowiązującego, a obowiązujące Zleceniobiorcę stanowią inaczej (w tym przypadku Zleceniobiorca powinien wcześniej poinformować Administratora danych o takim obowiązku). Zleceniobiorca zobowiązany jest potwierdzić usunięcie każdej partii lub całości danych osobowych i niezwłocznie przekazać Administratorowi danych potwierdzenie (pisemny protokół) każdego takiego usunięcia. 8. W miarę możliwości Zleceniobiorca pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 RODO.

9. Zleceniobiorca po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi Danych, nie później jednak niż w ciągu 12 godzin od stwierdzenia tego naruszenia. Zawiadomienie, o którym mowa w zdaniu poprzedzającym powinno nastąpić drogą elektroniczną i telefonicznie, na adres i pod numerem telefonu wskazanym w § 10 Umowy, a jego treść powinna co najmniej:
    a) opisywać charakter naruszenia ochrony danych osobowych, w tym wskazywać kategorie i przybliżoną liczbę objętych naruszeniem osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
    b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
    c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
    d) opisywać środki zastosowane lub proponowane przez Zleceniobiorcę w celu zaradzenia naruszeniu ochrony danych osobowych, w tym, w stosownych przypadkach, w celu zminimalizowania jego ewentualnych negatywnych skutków.

§ 4
Kontrola

1. Administrator danych ma prawo kontroli, czy środki zastosowane przez Zleceniobiorcę przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Kontrole mogą być prowadzone przez Administratora danych lub osobę trzecią działającą w imieniu Administratora, na przykład w trybie wizytacji dowolnej lokalizacji lub obiektu, w którym dane osobowe są przetwarzane (w tym przechowywane, co obejmuje również kopie zapasowe danych osobowych) oraz uzyskania dostępu do dokumentów, oprogramowania i sprzętu komputerowego oraz pozostałych informacji dotyczących danych osobowych będących przedmiotem Umowy w celu analizy i zbadania tych dokumentów, oprogramowania i sprzętu komputerowego oraz pozostałych informacji. Administrator lub osoba trzecia działająca w imieniu Administratora są upoważnieni do weryfikacji wdrożenia i skuteczności środków technicznych i organizacyjnych stosowanych przez Zleceniobiorcę w celu zabezpieczenia danych osobowych. Zleceniobiorcy nie przysługuje zwrot kosztów poniesionych w związku z kontorlą przeprowadzą przez Administratora danych lub podmiot trzeci na mocy Umowy.
3. Administrator danych może dokonać kontroli po uprzednim pisemnym powiadomieniu Zleceniobiorcy o zamiarze przeprowadzenia kontroli z 7-dniowym wyprzedzeniem. Kontrole będą przeprowadzane w dni robocze (dni inne niż soboty oraz dni wolne od pracy w rozumieniu ustawy z dnia 18 stycznia 1951 roku o dniach wolnych od pracy) w godzinach pracy obowiązujących u Zleceniobiorcy, przy czym Zleceniobiorca dołożyć wszelkich starań, aby było to najbliższy możliwy termin.
4. Zleceniobiorca udostępnia Administratorowi danych wszelkie informacje niezbędne do wykazania spełnienia przez Zleceniobiorcę obowiązków określonych w art. 28 RODO.
5. W przypadku stwierdzenia uchybień w przetwarzaniu czy zabezpieczaniu danych Zleceniobiorca zobowiązuje się do ich usunięcia w terminie uzgodnionym z Administratorem danych jednak nie dłuższym niż 7 dni roboczych, przy uwzględnieniu wiążących dla Zleceniobiorcy zaleceń Administratora danych.

§ 5
Dalsze powierzenie danych do przetwarzania

1. Zleceniobiorca może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych określającej warunki przetwarzania danych osobowych przez podwykonawcę.
2. Zleceniobiorca ponosi pełną odpowiedzialność wobec Administratora danych, jak za własne działania lub zaniechania, za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych zgodnych z niniejszą umową i RODO.

§ 6
Odpowiedzialność Zleceniobiorcy

1. Zleceniobiorca jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Zleceniobiorca zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Zleceniobiorcę danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Zleceniobiorcy, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania u Zleceniobiorcy danych osobowych powierzonych niniejszą umową, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych.

§ 7
Zasady zachowania poufności

1. Zleceniobiorca zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej, a dotyczących danych osobowych podlegających niniejszej umowie.
2. Zleceniobiorca oświadcza, że wymienione w ustępie 1 dane mogą zostać ujawnione podmiotom trzecim tylko w celu realizacji niniejszej umowy lub za zgodę Administratora danych albo zgodnie z wymogami obowiązującego prawa i jednoczesnym poinformowaniu Administratora danych zgodnie z § 6 ust. 2.

§ 8
Czas obowiązywania umowy

Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas trwania umowy głównej.

§ 9
Rozwiązanie umowy

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Zleceniobiorca:

   a) przetwarza dane osobowe w sposób niezgodny z umową,
   b) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych,
   c) nie usunął zgłoszonych uchybień w przetwarzaniu danych osobowych powierzonych przez Administratora danych w uzgodnionym terminie.

§ 10
Postanowienia końcowe

1. Wynagrodzenie należne na mocy umowy głównej obejmuje wynagrodzenie za usługi świadczone przez Zleceniobiorcę na rzecz Administratora danych na mocy Umowy.
2. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
3. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz RODO.
4. Strony oświadczają, że forma pisemna niniejszej umowy jest formą pisemną pod rygorem nieważności dla wszystkich jej postanowień. Wszelkie zmiany niniejszej umowy, jak i wszelkie oświadczenia skutkujące wygaśnięciem niniejszej umowy lub poszczególnych obowiązków z niej wynikających wymagają formy pisemnej pod rygorem nieważności.
5. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora danych.

.....	.....
Administrator danych	Zleceniobiorca

ZAŁACZNIK_PBI_07
Do Polityki Bezpieczeństwa Informacji
w UG Świdnica

Rejestr umów powierzenia przetwarzania danych osobowych

Lp.	Nazwa Podmiotu Przetwarzającego	Opis kategorii przetwarzań (zakres usługi)	Kategoria osób których dane dotyczą	Numer umowy powierzenia
1				
2				
3				
4				
5				
6				
7				

ZAŁACZNIK_PBI_08
Do Polityki Bezpieczeństwa Informacji
w UG Świdnica

Rejestr udostępnień

L.p.	Podmiot, któremu udostępniono dane osobowe	Na podstawie wniosku z dnia	Imię i nazwisko osoby udostępniającej dane	Data udostępnienia

ZAŁACZNIK_PBI_09
Do Polityki Bezpieczeństwa Informacji
w UG Świdnica

Ewidencja osób zapoznanych z Polityką Bezpieczeństwa Informacji

L.p.	Imię i Nazwisko	Komórka organizacyjna	Data	Podpis
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Załącznik nr 2
do zarządzenia nr 72/2018
Wójta Gminy Świdnica
z dnia 9 lipca 2018r.

Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

Urząd Gminy Świdnica

SPIS TREŚCI

Wprowadzenie

Instrukcja Zarządzania Systemem Informatycznym wraz z Polityką Bezpieczeństwa stanowi dokumentację przetwarzania danych osobowych w rozumieniu § 5 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. Urz. UE L 119 z 5 kwietnia 2016 r.).

Instrukcja Zarządzania Systemem Informatycznym obowiązuje od dnia 25-05-2018 r. Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów niniejszego dokumentu „Instrukcji Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych" powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych zawartych w systemach informatycznych w Urzędzie Gminy Świdnica. Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę UG Świdnica.

Instrukcja obowiązuje wszystkich pracowników UG ŚWIDNICA Wykonywanie postanowień tego dokumentu zapewnia właściwą ochronę danych oraz ewentualną reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa przetwarzanych danych.

Nadto dokument ten określa tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych UG ŚWIDNICA.

Należy przez powyższe rozumieć w szczególności realizację w niniejszym dokumencie wymogu opisania sposobu przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Zadaniem Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych jest także określenie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz wymagań w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

ROZDZIAŁ I

Zakres informacji objętych Instrukcją Zarządzania Systemem Informatycznym

Dokument Instrukcji Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem. Obejmuje on ogólne informacje o systemie informatycznym i zbiorach danych osobowych, które są przy ich użyciu przetwarzane, o zastosowanych rozwiązaniach technicznych, jak również o procedurach eksploatacji i zasady użytkowania, jakie zastosowano w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych.

Na Instrukcję Zarządzania składają się w szczególności następujące informacje:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
5) sposób, miejsce oraz okres przechowywania:
    a) elektronicznych nośników informacji zawierających dane osobowe,
    b) kopii zapasowych, o których mowa w pkt 4,
6) sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego,
7) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych,
8) opis incydentów naruszenia bezpieczeństwa danych osobowych i procedura zarządzania.

Instrukcję Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych stosuje się do wszelkich czynności, stanowiących w myśl rozporządzenia przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania.

Rygorowi Instrukcji Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych podlegają także dane powierzone przez UG ŚWIDNICA do przetwarzania na podstawie pisemnej umowy powierzenia przetwarzania danych osobowych oraz dane osobowe, których UG ŚWIDNICA jest odbiorcą w rozumieniu rozporządzenia.

ROZDZIAŁ II

Charakterystyka Systemu

1. System informatyczny służący do przetwarzania danych osobowych obejmuje wszystkie pracujące w UG ŚWIDNICA serwery, komputery stacjonarne i przenośne, a także urządzenia peryferyjne i sieciowe.

ROZDZIAŁ III

Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym

1. Użytkowników systemów informatycznych tworzy oraz usuwa Administrator Systemów Informatycznych na podstawie zgody Administratora Danych Osobowych.
2. Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie wydane przez Administratora Danych Osobowych.
3. Upoważnienie do przetwarzania danych osobowych dla pracowników UG ŚWIDNICA wydawane jest po złożeniu wniosku przez kierownika działu. Wzór wniosku o upoważnienie do przetwarzania danych osobowych określa załącznik nr 1 do Instrukcji.
4. Upoważnienie sporządza Inspektor Ochrony Danych, zgodnie ze wzorem stanowiącym załącznik nr 2 do Instrukcji. Upoważnienie do przetwarzania danych osobowych sporządzane jest w 3 egzemplarzach, jeden otrzymuje pracownik, drugi przechowywany jest w aktach osobowych pracownika, trzeci u Inspektora Ochrony Danych.
5. Upoważnienie do przetwarzania danych osobowych jest rejestrowane przez Inspektora Ochrony Danych.
6. Upoważnienie osobie upoważnionej wydawane jest po podpisaniu przez nią oświadczenia o zapoznaniu się z obowiązującymi przepisami w zakresie ochrony danych osobowych oraz zobowiązaniu się do zachowania w tajemnicy, także po ustaniu realizacji zadań oraz po ustaniu stosunku pracy, poznanych danych osobowych oraz informacji związanych z funkcjonowaniem systemu ochrony danych osobowych. Wzór oświadczenia określa załącznik nr 3 do Instrukcji. Oświadczenie sporządzane jest w 2 egzemplarzach, jeden przechowywany jest w aktach osobowych pracownika, drugi otrzymuje Inspektor Ochrony Danych.
7. Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta w przypadku:
   a) nieobecności pracownika w pracy trwającej dłużej niż 30 dni kalendarzowych,
   b) zawieszenia w pełnieniu obowiązków służbowych.
8. ĄCEJ nienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy.

ROZDZIAŁ IV

Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła jako narzędzi umożliwiających bezpieczne uwierzytelnienie.
2. Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.
3. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego przechowywanie.
4. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu hasła, które jest związane z jego identyfikatorem.
5. Każdy użytkownik posiadający dostęp do systemów teleinformatycznych UG ŚWIDNICA zobowiązany jest do:
    1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie informatycznym UG ŚWIDNICA,
    2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia,
    3) niezwłocznej zmiany hasła tymczasowego, przekazanego przez Administratora Systemów Informatycznych,
    4) poinformowania Administratora Systemów Informatycznych oraz Administratora Bezpieczeństwa Informacji o podejrzeniu lub rzeczywistym ujawnieniu hasła i natychmiastowej zmiany hasła,
    5) stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację małych i wielkich liter, cyfr i znaków specjalnych,
    6) zmiany wykorzystywanych haseł nie rzadziej niż co 30 dni.
6. Zabronione jest:
    1) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób,
    2) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.,
    3) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach,
    4) udostępnianie haseł innym użytkownikom,
    5) przeprowadzanie prób łamania haseł,
    6) wpisywanie haseł w postaci jawnej.
7. Hasłami najwyższego poziomu dysponuje Administrator Systemów Informatycznych i przechowuje je w zamkniętej kopercie w sejfie.

ROZDZIAŁ V

Ogólne zasady pracy w systemie informatycznym

1. Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez dopuszczone przez Administratora Danych do eksploatacji licencjonowane oprogramowanie.
2. Do eksploatacji dopuszcza się systemy informatyczne wyposażone w:
   a) mechanizmy kontroli dostępu umożliwiające autoryzację pracownika wykorzystującego system informatyczny na indywidualnym komputerowym stanowisku pracy zwanego dalej użytkownikiem, z pominięciem narzędzi do edycji tekstu,
   b) mechanizmy ochrony poufności, dostępności i integralności informacji, z uwzględnieniem potrzeby ochrony kryptograficznej,
   c) mechanizmy umożliwiające wykonanie kopii bezpieczeństwa oraz archiwizację danych, niezbędne do przywrócenia prawidłowego działania systemu po awarii,
   d) urządzenia niwelujące zakłócenia i podtrzymujące zasilanie,
   e) mechanizmy monitorowania w celu identyfikacji i zapobiegania zagrożeniom, w szczególności pozwalające na wykrycie prób nieautoryzowanego dostępu do informacji lub przekroczenia przyznanych uprawnień w systemie,
   f) mechanizmy zarządzania zmianami.
3. Użytkownikom zabrania się:
   a) korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami i dniami pracy UG ŚWIDNICA bez zgody na pracę w godzinach nadliczbowych lub odpracowanie czasu nieprzepracowanego w związku z załatwianiem spraw osobistych w godzinach pracy,
   b) udostępniania stanowisk roboczych osobom nieuprawnionym,
   c) wykorzystywania sieci komputerowej UG ŚWIDNICA w celach innych niż wyznaczone przez Administratora Danych Osobowych ,
   d) samowolnego instalowania i używania programów komputerowych,
   e) korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich,
   □) umożliwiania dostępu do zasobów wewnętrznej sieci informatycznej UG ŚWIDNICA oraz sieci Internetowej osobom nieuprawnionym,
   g) używania komputera bez zainstalowanego oprogramowania antywirusowego.
   h) korzystania z urządzeń nie będących własnością UG ŚWIDNICA.
4. Regulamin korzystania z przeglądarek internetowych stanowi załącznik nr 4 do Instrukcji.
5. Regulamin korzystania z poczty elektronicznej stanowi załącznik nr 5 do Instrukcji.

ROZDZIAŁ VI

Procedury rozpoczęcia, zawieszenie i zakończenia pracy

1. Każdy pracownik korzystający z systemu informatycznego przystępując do pracy powinien podać swoje dane dostępu do komputera i systemu, tj. identyfikator i hasło.

2. Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu. Użytkownik jest zobowiązany w takiej sytuacji do włączenia wygaszacza ekranu odblokowywanego hasłem.

3. Zakończenie pracy w systemie następuje poprzez prawidłowe, wymagane przez daną aplikację oraz system operacyjny, wykonanie czynności kończących. Niedopuszczalne jest zakończenie pracy poprzez wyłączenie napięcia zasilającego bez pełnej procedury zamknięcia komputera.

4. Ekrany monitorów stanowisk komputerowych, na których odbywa się przetwarzanie danych osobowych powinny być w miarę możliwości tak umieszczone, aby uniemożliwić wgląd w dane osobom postronnym przebywającym w pomieszczeniu oraz powinny automatycznie się wyłączać poprzez stosowanie wygaszaczy ekranowych uruchamiających blokadę pracy na komputerze.

5. Osoba przetwarzająca dane osobowe w przypadku konieczności opuszczenia pomieszczenia, obowiązana jest prawidłowo, zgodnie z instrukcją obsługi systemu, zakończyć pracę w systemie.

6. Czas rozpoczynania i kończenia pracy w systemach sieciowych, w tym systemach przetwarzających dane osobowe, określa Regulamin Pracy.

7. Administrator Systemów Informatycznych monitoruje logowanie oraz wylogowania się użytkowników oraz nadzoruje zakres przetwarzanych przez nich zbiorów danych.

ROZDZIAŁ VII

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania

1. Dla wszystkich aktywów informatycznych określa się zasady archiwizacji i tworzenia kopii zapasowych. Przy określaniu zasad bierze się pod uwagę:
    1) Kategoryzację aktywu,
    2) Zagrożenia i ryzyka związane z utratą integralności i dostępności danych,
    3) Możliwości techniczne,
    4) Wymogi prawne
2. Archiwizacja zasobów i wykonywanie kopii zapasowych odbywa się według planu archiwizacji i wykonywania kopii zapasowych.
3. Plan archiwizacji i wykonywania kopii zapasowych stanowi załącznik nr 6 do Instrukcji.
4. Dane osobowe zabezpiecza się poprzez wykonywanie kopii zapasowych.
5. Ochronie poprzez wykonanie kopii podlegają także programy i narzędzia programowe służące przetwarzaniu danych. Kopie programów i narzędzi wykonywane są zaraz po instalacji oraz po każdej aktualizacji na zewnętrznych, elektronicznych nośnikach informacji.

6. Zabezpieczeniu poprzez wykonywanie kopii zapasowych podlegają także dane konfiguracyjne systemu informatycznego przetwarzającego dane osobowe, w tym uprawnienia użytkowników systemu.
7. Za proces tworzenia kopii programów i narzędzi programowych oraz danych konfiguracyjnych systemu odpowiedzialny jest Administrator Systemów Informatycznych. Kopie przechowywane są w zamkniętej szafie w wydzielonym i zabezpieczonym pomieszczeniu.
8. Kopie zapasowe mogą być sporządzane automatycznie lub manualnie z wykorzystaniem specjalistycznych urządzeń do wykonywania kopii lub standardowych narzędzi oferowanych przez stacje robocze.
9. Kopie baz danych gromadzonych na serwerach wykonywane są przez Administratora Systemów Informatycznych co najmniej raz w tygodniu, zapisywane na dysk sieciowy lub zewnętrzne nośniki danych i przechowywane w zamkniętej szafie.
10. Kopie zbiorów danych osobowych zlokalizowanych na komputerach lokalnych wykonywane są przez poszczególnych użytkowników ostatniego dnia każdego miesiąca i zapisywane na dyskach lokalnych w ustalonej z Administratorem Systemów Informatycznych lokalizacji lub zapisywane na nośnikach zewnętrznych, autoryzowanych i dostarczonych przez Administratora Systemów Informatycznych.
11. Pliki edytorów tekstu lub arkuszy kalkulacyjnych traktowane są jak kopie zbiorów, z których pochodzą przetwarzane w nich dane i nie są objęte procedurami wykonywania kopii zapasowych.
12. Nośniki, na których są przechowywane kopie danych osobowych muszą być wyraźnie oznaczone datami.
13. Za bezpieczeństwo kopii zapasowych przetwarzanych lokalnie odpowiadają poszczególni użytkownicy systemu, którzy je wykonali. Kopie usuwa się niezwłocznie po ustaniu ich użyteczności w sposób uniemożliwiający odtworzenie danych.
14. Administrator Systemów Informatycznych zobowiązany jest do okresowego wykonywania testów odtworzeniowych kopii zapasowych.
15. Informację zawierająca dane osobowe, które nie będą wykorzystywane a nie podlegają archiwizacji lub dla której upłynął okres przechowywania należy usunąć.
16. Zewnętrzne nośniki kopii zapasowych, które zostały wycofane z użycia, podlegają zniszczeniu po usunięciu danych osobowych, w odpowiednim urządzeniu niszczącym.
17. Za właściwe usuniecie informacji zawartej na nośniku przenośnym lub w pamięci masowej stacji roboczej odpowiada użytkownik.
18. Za usuwanie informacji z pamięci masowych serwerów oraz nośników kopii archiwalnych i zapasowych odpowiada Administrator Systemów Informatycznych.
19. Użytkownik lub Administrator Systemów Informatycznych usuwający dane osobowe musi uzyskać zgodę Inspektora Ochrony Danych..
20. Użytkownik tworzy wydruki związane z przetwarzaniem danych osobowych wyłącznie w zakresie i ilości niezbędnej dla celów służbowych w uzgodnieniu z przełożonym.
21. Wszystkie dokumenty, zestawienia i wydruki zawierające dane osobowe powinny być chronione przed dostępem osób nieupoważnionych. Użytkownik przechowuje je w zamkniętej szafie w pomieszczeniu zabezpieczonym przed nieuprawnionym dostępem.

ROZDZIAŁ VIII

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji

1. Nośniki danych oraz programy służące do przetwarzania danych osobowych, a także dane konfiguracyjne systemu informatycznego, przechowuje Administrator Systemów Informatycznych w odpowiednio zabezpieczonym pomieszczeniu.
2. Dane osobowe mogą być przetwarzane na serwerach, a także na dyskach lokalnych komputerów w lokalizacji ustalonej z Administratorem Systemów Informatycznych. Zabrania się gromadzenia danych osobowych na innych, nie autoryzowanych przez Administratora Systemów Informatycznych nośnikach danych.
3. W uzasadnionych przypadkach, za zgodą Inspektora Ochrony Danych, dane osobowe można przetwarzać na zewnętrznych nośnikach informacji, autoryzowanych przez Administratora Systemów Informatycznych.
4. Informacje zawierające dane osobowe przechowywane na zewnętrznych nośnikach informacji muszą być szyfrowane.
5. W celu zwiększenia bezpieczeństwa danych i systemu informatycznego ogranicza się w UG ŚWIDNICA obieg dyskietek, pendrive-ów i innych nośników informatycznych poprzez ich oznaczenie i zarejestrowanie w ewidencji wewnętrznej. Wzór ewidencji nośników stanowi załącznik nr 7 do Instrukcji.
6. Ewidencję nośników prowadzi Administrator Systemów Informatycznych.
7. Wprowadza się zakaz obiegu nośników nie oznakowanych w sposób, o którym mowa w pkt 5, a wszystkie nośniki pochodzące od jednostek zewnętrznych mogą być wykorzystane tylko do jednorazowego odczytu ich zawartości po uprzednim sprawdzeniu programem antywirusowym.
8. Serwery oraz komputery, na których odbywa się przetwarzanie danych osobowych, powinny być zabezpieczone przed utratą danych spowodowaną awarią zasilania poprzez stosowanie specjalnych urządzeń podtrzymujących zasilanie i eliminujących zakłócenia sieci zasilającej.
9. Komputery przenośne oraz inne mobilne nośniki danych osobowych muszą być zabezpieczone ochroną kryptograficzną – muszą być zaszyfrowane.

ROZDZIAŁ IX

Zasady ochrony kryptograficznej

1. W celu ochrony poufności danych osobowych stosuje się w UG ŚWIDNICA zabezpieczenia kryptograficzne.
2. Za właściwą ochronę kryptograficzną odpowiedzialny jest Administrator Systemów Informatycznych.
3. Zabezpieczenia kryptograficzne stosuje się przy:
   1) Wymianie danych z podmiotami zewnętrznymi,
   2) Szyfrowaniu informacji na nośnikach zewnętrznych,
   3) Przy korzystaniu z komputerów przenośnych,
   4) Szyfrowaniu wiadomości poczty elektronicznej,

5) Szyfrowaniu baz danych.

4. Do szyfrowania połączeń stosuje się:
    1) Połączenia szyfrowane SSL/TLS,
    2) Tunele VPN.
5. Do szyfrowania informacji na nośnikach zewnętrznych stosuje się:
    1) Szyfrowanie plików technologią PGP,
    2) Szyfrowanie plików w kontenerach,
6. Do szyfrowania informacji na dyskach komputerów przenośnych stosuje się funkcje wbudowane systemu operacyjnego lub produkty firm zewnętrznych.
7. W wypadku przesyłania danych osobowych przez sieć internetową pocztą elektroniczną należy każdy z załączników zabezpieczyć ochroną kryptograficzną poprzez nadanie hasła odczytu. Hasło należy przesłać lub podać odbiorcy w innej przesyłce, a najlepiej z wykorzystaniem innych metod komunikacji (tel., sms, bezpośrednia rozmowa).
8. Do szyfrowania baz danych stosuje się funkcje wbudowane serwera baz danych lub produkty firm zewnętrznych.
9. Zabrania się przekazywania danych przez aplikacje internetowe nie wykorzystujące odpowiedniego protokołu szyfrowania (adres internetowy musi być poprzedzony zapisem „https").
10. Administrator Systemów Informatycznych odpowiedzialny jest za przechowywanie danych związanych z ochroną kryptograficzną w magazynie certyfikatów chronionym hasłem administracyjnym.

ROZDZIAŁ X

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu.

1. Serwery i stacje robocze w UG ŚWIDNICA są objęte ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego oraz zapory (firewall), zapewniających integralność zasobów przechowywanych i przetwarzanych w systemie informatycznym UG ŚWIDNICA.
2. Wymienne nośniki pamięci, przed rozpoczęciem pracy z tymi nośnikami w systemie informatycznym UG ŚWIDNICA, są sprawdzane za pomocą aktualnego oprogramowania antywirusowego.
3. Aktualizacja baz wirusów odbywa się automatycznie.
4. System antywirusowy jest skonfigurowany w sposób zapewniający na bieżąco skanowanie wszystkich informacji przetwarzanych w systemie, a zwłaszcza poczty elektronicznej i stron internetowych.

5. Po każdej naprawie i konserwacji urządzenia a przed ponownym włączeniem do systemu informatycznego UG ŚWIDNICA zawartość stałych nośników informacji jest sprawdzana za pomocą oprogramowania antywirusowego.
6. Wystąpienie infekcji traktowane jest jako incydent bezpieczeństwa i podlega procedurze postępowania w sytuacji naruszenia ochrony danych osobowych.
7. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, Administrator Systemów Informatycznych podejmuje działania zmierzające do usunięcia zagrożenia.

ROZDZIAŁ XI

Informacje o odbiorcach, którym dane osobowe zostały udostępnione.

1. Dla każdej osoby, której dane są przetwarzane w systemie informatycznym powinny być automatycznie odnotowane następujące informacje:
   a) dane o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba, że dane te traktuje się jako dane jawne,
   b) sprzeciwu osoby, której dane dotyczą w przypadku zamierzenia przetwarzania jej danych w celach marketingowych lub zamierzenia przekazania jej danych innemu administratorowi.
2. Zapis pkt 1 nie dotyczy systemów służących do przetwarzania danych ograniczonych do edycji tekstu w celu udostępnienia go na piśmie i niezwłocznym usunięciu z systemu.
3. Dla każdej osoby, której dane są przetwarzane w systemie informatycznym, system powinien zapewniać sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w pkt 1.
4. W uzasadnionych przypadkach uniemożliwiających automatyczne odnotowywanie, o którym mowa w pkt 1, prowadzi się odrębny „rejestr udostępniania", w oparciu o Rzeczowy Wykaz Akt i Instrukcję Kancelaryjną.
5. Za udostępnianie danych zgodnie z przepisami prawa odpowiedzialny jest Administrator Danych Osobowych.

ROZDZIAŁ XII

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

1. Konserwacja sprzętu i urządzeń pracujących w systemie informatycznym UG ŚWIDNICA ma na celu zapewnienie nieprzerwanej i bezpiecznej pracy tego systemu, zapobieganie utraty, uszkodzenia danych lub naruszenie bezpieczeństwa systemu.

2. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

   a) **likwidacji** — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,

   b) **przekazania podmiotowi nieuprawnionemu do przetwarzania danych** — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,

   c) **naprawy** — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem Administratora Systemów Informatycznych.

3. Instalacji, konserwacji oraz napraw sprzętu komputerowego dokonuje Administrator Systemów Informatycznych lub podmiot zewnętrzny świadczący usługi konserwacyjne na podstawie umowy lub w ramach gwarancji.
4. Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez Administratora Danych Osobowych lub posiadające umowy na powierzenie przetwarzania danych w zakresie konserwacji i napraw.
5. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych, w szczególności poprzez bezpośredni nadzór prowadzony przez Administratora Systemów Informatycznych. Jeżeli zaś taki nadzór nie jest możliwy, to informacje zawierające dane osobowe są, po zapewnieniu możliwości ich odtworzenia, skutecznie usuwane z nośnika.
6. Wszelkie konserwacje i naprawy są odnotowywane w dzienniku pracy danego sprzętu.

ROZDZIAŁ XIII

Zdarzenia naruszające bezpieczeństwo informacji

1. Wszyscy pracownicy UG ŚWIDNICA oraz pracownicy reprezentujący podmiot zewnętrzny, którzy mają dostęp do systemów informatycznych UG ŚWIDNICA i zobowiązali się do przestrzegania jej regulacji wewnętrznych związanych z bezpieczeństwem informacji, mają obowiązek zgłaszania wszelkich zdarzeń, które naruszają lub mogą naruszyć przepisy prawa oraz polityki, regulaminy i procedury UG ŚWIDNICA dotyczące bezpieczeństwa informacji.
2. Przed przystąpieniem do pracy użytkownik obowiązany jest sprawdzić stację roboczą i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie lub próbę naruszenia bezpieczeństwa informacji.
3. Podział zagrożeń:

a) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,

b) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora systemu informatycznego, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,

c) zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:

- nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
- nieuprawniony dostęp do systemu z jego wnętrza,
- pogorszenie jakości sprzętu i oprogramowania,
- nieuprawniony przekaz danych,
- bezpośrednie zagrożenie materialnych składników systemu.

4. Do przykładów mogących świadczyć lub świadczących o naruszeniu bezpieczeństwa, niewłaściwym funkcjonowaniu oprogramowania lub podatności systemu informatycznego zalicza się:

1) Naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach (np. zacinające się zamki, naruszone plomby, niedomknięte okno itp.), w których odbywa się przetwarzanie danych osobowych.
2) Utratę usługi, urządzenia lub funkcjonalności aplikacji/systemu,
3) Nieautoryzowaną utratę lub zniszczenie danych,
4) Spowolnienie pracy komputera,
5) Pojawienie się nietypowych komunikatów na ekranie,
6) Niemożność zalogowania się do systemu informatycznego,
7) Objawy niestabilnej pracy systemu informatycznego,
8) Nagłe przyspieszenie lub zwolnienie transmisji danych,
9) Brak reakcji systemu na działania użytkownika,
10) Ponowny start lub zawieszania się komputera,
11) Ograniczenie funkcjonalności komputera.
12) Brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych,
13) Ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika aplikacji (np. brak możliwości wykonywania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji,
14) Wygląd aplikacji inny niż normalnie,
15) Inny zakres danych niż normalnie dostępny dla użytkownika - dużo więcej lub dużo mniej danych,
16) Znaczne spowolnienie działania systemu informatycznego,
17) Zgubienie lub kradzież nośnika danych osobowych,
18) Kradzież sprzętu informatycznego, w którym przechowywane były dane osobowe,

19) Informację z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami,

20) Fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia siły wyższej.

21) Podejrzenie nieautoryzowanej modyfikacji danych osobowych.

5. Za naruszenie ochrony danych osobowych i wystąpienie incydentu bezpieczeństwa uważa się w szczególności:
   1) Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
   2) Awarię sprzętu lub oprogramowania, która wskazuje na umyślne działanie w kierunku naruszenia ochrony danych,
   3) Dopuszczenie do przetwarzania danych osobowych pracowników nie posiadających odpowiednich uprawnień,
   4) Niewłaściwe niszczenie nośników informacji, na których przechowywane są dane osobowe,
   5) Ujawnienie indywidualnych haseł,
   6) Stwierdzenie nieupoważnionego dostępu do systemu informatycznego przetwarzającego dane osobowe,
   7) Niedopełnienie obowiązku ochrony danych osobowych (np. pozostawienie danych osobowych, nie zablokowanie dostępu do systemu, brak nadzoru nad serwisantami itp.),
   8) Wykonanie nieuprawnionych kopii danych osobowych,
   9) Zaniechanie działań zmierzających do eliminacji wirusów komputerowych i innego rodzaju niepożądanego oprogramowania,
   10) Przesyłanie niezabezpieczonych informacji zawierających dane osobowe drogą elektroniczną,
   11) Stwierdzenie próby lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
   12) Ujawnienie istnienia nieautoryzowanych kont dostępu do danych.
   13) Utratę zewnętrznego nośnika pamięci,
   14) Utratę komputera przenośnego,
   15) Dopuszczenie do braku aktualnych kopii bezpieczeństwa danych i ustawień systemu informatycznego,
   16) Korzystanie z nielicencjonowanego oprogramowania,
   17) Dopuszczenie do możliwości korzystania z sieci informatycznej.

6. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie bezpieczeństwa miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp

ROZDZIAŁ XIV

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

1. Osoba, która zauważyła niepokojące zdarzenie, wystąpienie poniżej wymienionych symptomów lub innych objawów, które jej zdaniem mogą spowodować zagrożenie bądź mogą być przyczyną naruszenia ochrony danych osobowych i bezpieczeństwa informacji, zobowiązana jest do natychmiastowego poinformowania: bezpośredniego przełożonego oraz Administratora Systemów Informatycznych.

2. Administrator Systemów Informatycznych dokonuje wstępnej identyfikacji zdarzenia i na podstawie dostępnych informacji oraz analizy okoliczności zdarzenia kwalifikuje zdarzenie (lub serię zdarzeń) jako:

   a) Zdarzenie nie mające cech naruszenia bezpieczeństwa informacji,

   b) Incydent związany z naruszeniem bezpieczeństwa informacji.

3. O potencjalnym wystąpieniu incydentu związanego z naruszeniem bezpieczeństwa informacji Administrator Systemów Informatycznych powiadamia niezwłocznie Inspektora Ochrony Danych.

4. Inspektor Ochrony Danych we współpracy z Administratorem Systemów Informatycznych przeprowadza analizę incydentu.

5. Analiza incydentu uwzględnia następujące kryteria:

   a) Charakter incydentu i jego znaczenie związane z bezpieczeństwem danych,

   b) Miejsce wystąpienia incydentu – identyfikacja punktu, w którym nastąpiło zdarzenie (lokalizacja, serwer, stacja robocza itp.)

   c) Zakres incydentu,

   d) Identyfikację zasobów potrzebnych przy dalszych działaniach w ramach postępowania z incydentem,

   e) Możliwość rozszerzenia się zakresu incydentu,

   f) Szacowany poziom szkód,

   g) Rodzaj ujawnionej informacji,

   h) Skutki organizacyjne i prawne,

6. W przypadku, gdy incydent posiada skutki przekładające się na możliwość zakłócenia działalności ustawowej bądź statutowej UG ŚWIDNICA Administrator Systemów Informatycznych informuje niezwłocznie Administratora Danych Osobowych.

7. W przypadku , gdy zasięg i szacunkowy czas trwania powoduje zakwalifikowanie incydentu jako sytuację kryzysową określaną jako zniszczenie lub poważną awarię kluczowych zasobów teleinformatycznych UG ŚWIDNICA Administrator Systemów Informatycznych niezwłocznie powiadamia Administratora Danych Osobowych.

8. W przypadku, gdy rodzaj i zasięg incydentu zidentyfikowany na którymkolwiek z etapów postępowania uzasadnia potrzebę powiadomienia organów ścigania to decyzje o sposobie i terminie powiadomienia podejmuje Administrator Danych Osobowych.

9. W przypadku, gdy rodzaj i zasięg incydentu zidentyfikowany na którymkolwiek z etapów postępowania uzasadnia podejrzenie utraty danych osobowych Administrator Danych powiadamia w terminie 72 godzin Prezesa Urzędu Ochrony Danych i jeżeli to możliwe osoby, których dane osobowe zostały utracone.

10. Administrator Systemów Informatycznych prowadzi bieżącą dokumentację incydentu. Dokumentacja ta w szczególności obejmuje:

a) Wszystkie zdarzenia zachodzące w systemie informatycznym (zapisy z systemowych dzienników),

b) Wszystkie podejmowane działania (opatrzone datą i czasem),

c) Wszystkie przeprowadzone rozmowy (osoba rozmówcy, data i czas, treść rozmowy).

11. Dokumentacja incydentu podlega rygorom ochrony przez tworzenie autoryzowanych kopii tych elementów systemu, które mają zastosowania przy postepowaniu z incydentem tzn. rejestry urządzeń, systemów operacyjnych i aplikacji, kopie zapasowe, pliki konfiguracyjne i systemowe (zgodnie z rygorami tworzenia materiału dowodowego). Wzór protokołu zabezpieczenia materiału dowodowego stanowi załącznik nr 8 do Instrukcji.

12. Administrator Systemów Informatycznych przeprowadza działania zmierzające do ograniczenia skutków incydentu i zidentyfikowaniu źródła naruszenia bezpieczeństwa.

13. Przy ograniczaniu skutków incydentu Administrator Systemów Informatycznych może korzystać z konsultantów zewnętrznych, jeżeli UG ŚWIDNICA zawarł w umowach z tymi podmiotami stosowne zapisy.

14. Po usunięciu lub zablokowaniu źródła incydentu Administrator Systemów Informatycznych przystępuje do odtworzenia systemu.

15. W przypadku zaistnienia sytuacji, kiedy nastąpiło uruchomienie Planu Zapewnienia Ciągłości Działania UG ŚWIDNICA odtworzenie systemu jest realizowane w oparciu o procedury opisane w tym planie.

16. Odtwarzanie systemu odnosi się do punktu odtworzenia, co do którego Administrator Systemów Informatycznych ma uzasadnioną pewność, że nie zawiera źródła incydentu.

17. System informatyczny, którego prawidłowe działanie zostało odtworzone powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu.

18. Administrator Bezpieczeństwa Informacji prowadzi rejestr incydentów zawierający następujące informacje:

a) datę i godzinę zgłoszenia incydentu,

b) dane identyfikujące osobę zgłaszającą,

c) dane osoby przekazującej informację o incydencie,

d) datę zarejestrowania incydentu,

e) dane identyfikujące osobę rejestrującą incydent,

f) informacje dotyczące sposobu postepowania z incydentem,

g) informacje o zgromadzonych informacjach dowodowych.

19. Z każdego incydentu bezpieczeństwa Administrator Bezpieczeństwa Informacji sporządza raport. Wzór dokumentu raportu opisany jest w załączniku nr 9 niniejszej instrukcji.

20. Administrator Bezpieczeństwa Informacji odpowiedzialny jest za przeprowadzenie przynajmniej raz w roku analizy zaistniałych incydentów w celu:

a) określenia skuteczności podejmowanych działań wyjaśniających i naprawczych,

b) określenia wymaganych działań zwiększających bezpieczeństwo systemu informatycznego i minimalizujących ryzyko zaistnienia incydentów,

c) określenia potrzeb w zakresie szkoleń administratorów systemu i użytkowników systemu informatycznego przetwarzającego dane osobowe.

ROZDZIAŁ XV

Zasady korzystania z komputerów przenośnych, na których są przetwarzane dane osobowe.

1. Przetwarzanie danych osobowych na komputerach przenośnych powinno być ograniczone do niezbędnych przypadków. Przetwarzanie danych osobowych przy użyciu komputerów przenośnych może odbywać się wyłącznie za zgodą Administratora Danych Osobowych i za wiedzą Inspektora Ochrony Danych. Zakres danych przetwarzanych na komputerze przenośnym oraz zakres uprawnień do przetwarzanych danych ustala przełożony pracownika za wiedzą Inspektora Ochrony Danych.

2. Osoba korzystająca z komputera przenośnego w celu przetwarzania danych osobowych zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych danych, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem.

3. Użytkownik komputera przenośnego zobowiązany jest do:

a) transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności:
- transportowania komputera w bagażu podręcznym,
- nie pozostawiania komputera w samochodzie, przechowalni bagażu, itp.,
- zaleca się przenoszenie komputera w torbie przeznaczonej do przenoszenia komputerów przenośnych,

b) korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego,

c) nie zezwalania osobom nieupoważnionym do korzystania z komputera przenośnego, na którym przetwarzane są dane osobowe,

d) zabezpieczania komputera przenośnego hasłem,

e) blokowania dostępu do komputera przenośnego w przypadku, gdy nie jest on wykorzystywany przez

pracownika,

f) kopiowania danych osobowych przetwarzanych na komputerze przenośnym do systemu informatycznego w celu umożliwienia wykonania kopii zapasowej tych danych,

g) umożliwienia, poprzez podłączenie komputera do sieci informatycznej UG ŚWIDNICA do:
- aktualizacji wzorców wirusów w programie antywirusowym,
- utrzymania konfiguracji oprogramowania systemowego w sposób wymuszający korzystanie z haseł,

h) wykorzystywania haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe,

i) zmiany haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe,

j) zabezpieczania danych osobowych przetwarzanych na komputerach przenośnych poprzez zastosowanie oprogramowania szyfrującego te dane, tak by dostęp do tych danych był możliwy wyłącznie po podaniu hasła,

k) dokonania instalacji i konfiguracji oprogramowania antywirusowego na komputerze przenośnym,

l) przeprowadzania aktualizacji wzorców wirusów zgodnie z zasadami zarządzania programem antywirusowym.

4. W razie zgubienia lub kradzieży komputera przenośnego pracownik zobowiązany jest do natychmiastowego powiadomienia Administratora Danych Osobowych lub osoby uprawnionej zgodnie z zasadami informowania o naruszeniu ochrony danych osobowych.

ROZDZIAŁ XVI

Przetwarzanie danych osobowych w systemach informatycznych powierzonych UG ŚWIDNICA przez inne podmioty

1. Możliwe jest przetwarzanie w systemach informatycznych UG ŚWIDNICA danych osobowych powierzonych UG ŚWIDNICA przez inny podmiot (Zleceniodawcę). W takim przypadku, przetwarzanie danych osobowych odbywa się na podstawie umowy pomiędzy UG ŚWIDNICA a Zleceniodawcą zawartej w formie pisemnej. Umowa ta musi zawierać ściśle określony zakres przetwarzanych danych. Przetwarzanie danych możliwe jest tylko w ustalonym przez umowę zakresie.
2. Powierzone dane podlegają ochronie na takich samych zasadach jak dane będące własnością UG ŚWIDNICA , chyba, że umowa określi inne zasady ochrony danych osobowych. W szczególności może dotyczyć to nadawania uprawnień do przetwarzania danych osobowych. Dostęp do powierzonych danych osobowych z sieci zewnętrznej (np. siedziby Zleceniodawcy) musi odbywać się z zachowaniem

odpowiednich zabezpieczeń. Dostęp do danych musi być chroniony identyfikatorem oraz hasłem, a połączenie sieciowe realizujące dostęp do danych musi być odpowiednio szyfrowane.

ROZDZIAŁ XVII

Postanowienia końcowe

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

2. Inspektor Ochrony Danych zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego załącznik nr 10 do niniejszego dokumentu.

3. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Inspektora Ochrony Danych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z rozporządzeniem 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 5 kwietnia 2016 r.) oraz możliwość wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

4. W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy 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 5 kwietnia 2016 r.).

5. Postanowienia Niniejszej instrukcji stosuje się również do stażystów i praktykantów.

6. Wszelkie zmiany Instrukcji mogą być wprowadzane tylko na podstawie zarządzeń Administratora Danych Osobowych.

7. Zmiany wprowadzane w załącznikach do niniejszego dokumentu nie wymagają zmiany zarządzenia, które wprowadziło niniejszą instrukcję w życie.

Załącznik nr 1

do Instrukcji zarządzania systemami informatycznymi
służącymi do przetwarzania danych osobowych
w UG ŚWIDNICA

Świdnica.....

.....

(znak sprawy)

WNIOSEK o
wydanie upoważnienia do
przetwarzania danych osobowych

Proszę o wydanie upoważnienia Pani/Panu

.....

(nazwisko i imię , stanowisko służbowe)

.....

(komórka organizacyjna, budynek, pomieszczenie)

do przetwarzania danych osobowych zawartych w następujących zbiorach:

.....

.....

.....

w zakresie :

zbieranie, wgląd w dane osobowe, wprowadzanie, przechowywanie, opracowywanie, utrwalanie, zmienianie, usuwanie, kopiowanie, udostępnianie*

w formie :

papierowej (kartoteki, ewidencje, rejestry, spisy itp.), elektronicznej*

na okres :

od ..... do .....

bezterminowo*

.....
(podpis)

---

* niepotrzebne skreślić

Załącznik nr 2

do Instrukcji zarządzania systemami informatycznymi
służącymi do przetwarzania danych osobowych
w UG ŚWIDNICA

Świdnica, ...

.....

(znak sprawy)

UPOWAŻNIENIENIE
do przetwarzania danych osobowych

Upoważniam Panią/Pana .....
(imię i nazwisko)

zatrudnioną/zatrudnionego w . .....

.....
(nazwa komórki organizacyjnej)

do przetwarzania danych osobowych zawartych w następujących zbiorach :

1. .....

2. .....

3. .....

w celach związanych z wykonywaniem obowiązków na stanowisku :

.....
(zajmowane stanowisko)

Przetwarzanie danych osobowych może odbywać się przy wykorzystaniu :

.....
(systemu informatycznego, systemu w postaci papierowej)

w zakresie :

.....
(nazwa uprawnień w zakresie przetwarzania danych)

Upoważnienie ważne jest od ..... do .....

.....
(podpis)

Załącznik nr 3

do Instrukcji zarządzania systemami informatycznymi
służącymi do przetwarzania danych osobowych
w UG ŚWIDNICA

Świdnica, ...

.....
(imię i nazwisko pracownika, stażysty, praktykanta)

.....
(stanowisko)

OŚWIADCZENIE

Oświadczam, że:

1) zapoznałam/zapoznałem* się z:

a) Rozporządzeniem 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 5 kwietnia 2016 r.),

c) Polityką bezpieczeństwa w zakresie przetwarzania danych osobowych w UG ŚWIDNICA,

d) Instrukcją zarządzania systemami informatycznymi służącym do przetwarzania danych osobowych w UG ŚWIDNICA i zobowiązuję się do ich przestrzegania.

2) zobowiązuję się :

a) zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia, do których będę miała/miał* dostęp w związku z wykonywaniem zadań wynikających ze stosunku pracy/ z umowy o zorganizowanie stażu/ z umowy- porozumienia o odbycie praktyki*, zarówno w czasie trwania umowy, jak i po jej ustaniu,

b) chronić dane osobowe przed dostępem do nich osób do tego nieupoważnionych, zabezpieczać je przed zniszczeniem i nielegalnym ujawnieniem,

c) zachować szczególną staranność w trakcie przetwarzania danych osobowych w celu ochrony interesów osób, których dane dotyczą.

.....
(podpis)

* niepotrzebne skreślić

Załącznik nr 4

do Instrukcji zarządzania systemami informatycznymi
służącymi do przetwarzania danych osobowych
w UG ŚWIDNICA

Regulamin korzystania z przeglądarek internetowych

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą Administratora Bezpieczeństwa Informacji i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
5. Zabronione jest w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł chyba, że stosuje się hasło główne.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:"
7. Należy zachować szczególną ostrożność w przypadku żądania lub prośby podania kodów, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.
8. Przy korzystaniu z Internetu, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
9. W zakresie dozwolonym przepisami prawa, UG ŚWIDNICA zastrzega sobie prawo kontrolowania sposobu korzystania przez Użytkownika z Internetu pod kątem wyżej opisanych zasad.
10. Ponadto, w uzasadnionym zakresie, UG ŚWIDNICA zastrzega sobie prawo kontroli czasu spędzanego przez Użytkownika w Internecie.

Załącznik nr 5

do Instrukcji zarządzania systemami informatycznymi
służącymi do przetwarzania danych osobowych
w UG ŚWIDNICA

Regulamin korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych z użyciem maila może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania informacji wrażliwych wewnątrz organizacji bądź wszelkich danych osobowych poza organizację należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych plików, podpis elektroniczny).
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. Nie należy otwierać załączników (plików) w mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.
7. Użytkownicy nie powinni rozsyłać (przesyłać dalej) za pośrednictwem maila informacji o zagrożeniach dla systemu informatycznego
8. Użytkownicy nie powinni rozsyłać, maili zawierających załączniki o dużym rozmiarze.
9. Użytkownicy powinni okresowo kasować niepotrzebne maile
10. Podczas wysyłania maili do wielu adresatów (osób prywatnych) jednocześnie, należy użyć metody „Ukryte do wiadomości ".
11. Mail jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
12. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
13. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
14. Użytkownik bez zgody UG ŚWIDNICA nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące UG ŚWIDNICA, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

Załącznik nr 6

do Instrukcji zarządzania systemami informatycznymi
służącymi do przetwarzania danych osobowych
w UG ŚWIDNICA

Rejestr nośników komputerowych zawierających ważne dane w tym dane osobowe

REJESTR NOŚNIKÓW KOMPUTEROWYCH

ZAWIERAJĄCYCH WAŻNE DANE

Oznaczenie nośnika	Data wpisania w rejestr	Opis nośnika	Miejsce przechowywania nośnika	Podpis użytkownika	Uwagi

Oznaczenie nośnika:

Kolejny nr nośnika / symbol nośnika / symbol jednostki lub komórki org.

Przykładowe symbole nośników:

NO – nośnik optyczny

P- Pendrive

Załącznik nr 8

do Instrukcji zarządzania systemami informatycznymi
służącymi do przetwarzania danych osobowych
w UG ŚWIDNICA

PROTOKÓŁ ZABEZPIECZENIA MATERIAŁU DOWODOWEGO

Wykonano w dniu ..... o godzinie ..... w obecności:

Świadek 1: <imię i nazwisko, stanowisko, komórka organizacyjna UG ŚWIDNICA">
Świadek 2: <imię i nazwisko, stanowisko, komórka organizacyjna UG ŚWIDNICA>
Świadek 3: <imię i nazwisko, niezależny ekspert>

4.Rodzaj materiału dowodowego
(zaznaczyć właściwe kwadraty i wpisać odpowiednie nazwy i oznaczenia)

Dokument ☐ Rodzaj i Nazwa dokumentu
papierowy .....

Dokument ☐ Rodzaj i Nazwa dokumentu
elektroniczny .....

Kopia zapasowa

System operacyjny ☐ Aplikacja ☐ .
Nazwa i wersja systemu *Nazwa i wersja aplikacji*
....

Baza Danych ☐ Oznaczenie nośnika .
Nazwa i wersja bazy .....
....

Obraz Dysku ☐ Lokalizacja dysku (adres IP/IPX)..... .
Typ i nr seryjny dysku.....

Pliki konfiguracyjne
i/lub systemowe

System operacyjny ☐ Aplikacja ☐ .
Nazwa i wersja systemu *Nazwa i wersja aplikacji*
....

Baza Danych ☐ Nazwa(y) pliku(ów) .
Nazwa i wersja bazy .....
....

Kopie zawartości dzienników (logów) zdarzeń.....

System operacyjny ☐ Aplikacja ☐ .
Nazwa i wersja systemu *Nazwa i wersja aplikacji*
....

Baza Danych ☐ Nazwa(y) pliku(ów) .
Nazwa i wersja bazy .....
....

Kopia zawartości skrzynki pocztowej

Zewnętrzna ☐ Wewnętrzna ☐
Nazwa skrzynki pocztowej *Nazwa skrzynki pocztowej* .....
.....

5.Opis czynności
(opisać kolejne czynności z zaznaczeniem Wykonawcy(ów))

6.Wytworzony materiał dowodowy

Wykonano kopie materiału dowodowego w 2 egzemplarzach, którym nadano etykiety:

..... Egzemplarz nr 1
..... Egzemplarz nr 2

(wprowadzić krótkie oznaczenie zabezpieczonego materiału dowodowego z data i godziną wykonania)

7.Zabezpieczenie materiału dowodowego
(opisać sposób zabezpieczenia jednego z egzemplarzy)

Protokół sporządził:.....

Podpisano:
Świadek 1 .....
Świadek 2 .....
Świadek 3 .....

Załącznik nr 9

do Instrukcji zarządzania systemami informatycznymi
służącymi do przetwarzania danych osobowych
w UG ŚWIDNICA

Wzór raportu z incydentu

Miejscowość, data

RAPORT O INCYDENCIE BEZPIECZEŃSTWA INFORMACJI

A. ZGŁOSZENIE INCYDENTU *(wypełnia osoba zgłaszająca zdarzenie/incydent)*

DANE OSOBY ZGŁASZAJĄCEJ
Imię i nazwisko.....Stanowisko służbowe .....
Adres .....
Nr telefonu .....e-mail .....
OPIS INCYDENTU:
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Komu zgłoszono: .....

Data i godzina zgłoszenia: .....

Podpis osoby zgłaszającej .....

B. DZIAŁANIA PO ZAISTNIENIU INCYDENTU
(wypełnia osoba rozpatrująca zgłoszenie incydentu)

DANE OSOBY, KTÓRA PRZYJĘŁA ZGŁOSZENIE INCYDENTU/ ADMINISTRATOR SYSTEMU/ ADMINISTRATOR ZABEZPIECZEŃ FIZYCZNYCH

Imię i nazwisko..... Stanowisko .....
Adres .....
Nr telefonu ..... e-mail .....
INFORMACJE O INCYDENCIE
Data i czas zajścia incydentu .....
Data i czas wykrycia incydentu .....
Data i czas zgłoszenia incydentu .....
Czy incydent jest zakończony? TAK □ NIE □
Jeśli tak, to jak długo trwał (dni/godziny/minuty)? .....
Jeśli nie, należy określić jak długo już trwa? .....
Kogo powiadomiono z KIEROWNICTWA? .....

OPIS WSTĘPNY / PODJĘTE DZIAŁANIA / ZABEZPIECZENIE MATERIAŁU DOWODOWEGO
.....
.....
.....
.....
.....
.....
.....
.....
Załączniki (*materiał dowodowy):*
1. .....
2. .....
3. .....

OPIS ROZWIĄZANIA PROBLEMU / KOSZTY ODTWORZENIA
.....
.....
.....
.....
.....
.....
.....
.....
Imię i Nazwisko.....
Data .....
Podpis .....

C. POSTĘPOWANIE WYJAŚNIAJĄCE/ ZAKOŃCZENIE INCYDENTU
(wypełnia osoba prowadząca postępowanie wyjaśniające)

Data rozpoczęcia postępowania ws. incydentu .....
Data zakończenia incydentu (jeśli jest zakończony) .....
Data zamknięcia skutków incydentu .....
Data zakończenia postępowania ws. incydentu .....
Data przedstawienia incydentu na KSBI .....

USTALENIA – OPIS POSTĘPOWANIA - SPRAWCY INCYDENTU
(w tym opis postępowania dyscyplinarnego, jeśli takie ma miejsce)

.....
.....
.....
.....
.....
.....
.....
.....
.....

WNIOSKI I REKOMENDACJE
(w tym zalecenia dotyczące zmian w SZBI)

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

WYKAZ DOŁĄCZONYCH DOKUMENTÓW

.....
.....
.....
.....
.....

DANE OSÓB PROWADZĄCYCH POSTĘPOWANIE WYJAŚNIAJĄCE

Imię i Nazwisko.....
Imię i Nazwisko.....
Imię i Nazwisko.....

Załącznik nr 10

do Instrukcji zarządzania systemami informatycznymi
służącymi do przetwarzania danych osobowych
w UG ŚWIDNICA

Ewidencja osób zapoznanych z Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

L.p.	Imię i Nazwisko	Data	Uwagi