ZARZĄDZENIE NR 173. 2021
Wójta Gminy Odrzywół
z dnia 29 stycznia 2021 roku

w sprawie wprowadzenia Polityki bezpieczeństwa informacji w Urzędzie Gminy w Odrzywole

Na podstawie art. 31 oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2020.713 t.j.), w związku z § 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 (Dz. U. z 2017 r. poz. 2247) zarządzam, co następuje:

§ 1.

Wprowadza się w Urzędzie Gminy w Odrzywole Politykę bezpieczeństwa informacji stanowiącą załącznik Nr 1 do niniejszego zarządzenia.

§ 2.

Zobowiązuję pracowników Urzędu Gminy w Odrzywole do stosowania zasad określonych w Polityce.

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
mgr Mariola Kmieciak

Załącznik nr 1 do **Zarządzenia Nr 173 Wójta Gminy Odrzywół z dnia 29 stycznia 2021r.**

Polityka Bezpieczeństwa Informacji

Nazwa i dane kontaktowe Administratora danych	
Nazwa	URZĄD GMINY W ODRZYWOLE
Adres	26-425 Odrzywół, ul. Warszawska53
Email	sektretariat@odrzywol.eu
Telefon	48 6716057

Wersja:	Pierwsza wersja dokumentu
Data wersji:	19 stycznia 2021r.
Utworzony przez:	Ilona Głogowska-Kowalczyk
Historia zmian	
Data:	12.02.2021r.
Wersja:	0.1
Utworzona przez:	Ilona Głogowska-Kowalczyk Inspektor ochrony danych
Zatwierdzona przez:	Pan Marian Kmieciak-Wójt Gminy Odrzywół

Spis treści

Wstęp

O skuteczności działania i rozwoju każdej organizacji świadczy stopień osiągania zamierzonego celu. W procesie tym kluczowe jest stosowanie współczesnych technik i technologii, narzędzi i systemów informatycznych oraz przetwarzania i zarządzania informacją. Informacja jest jednym z najważniejszych zasobów Urzędu, dlatego powinna być chroniona na każdym szczeblu organizacji. Urząd Gminy w Odrzywole chroni zarówno informacje własne, jak i powierzone. Poufność, dostępność i integralność informacji ma kluczowe znaczenie dla utrzymania zgodności z przepisami prawa oraz wizerunku Urzędu wobec stron zainteresowanych.

Polityka Bezpieczeństwa Informacji w Urzędzie stanowi zestawienie zasad, praw i reguł oraz doświadczeń i dobrych praktyk w zakresie zarządzania i ochrony danych i informacji w naszej organizacji. Polityka określa techniczne i organizacyjne środki służące do osiągnięcia celów stawianych przed systemem zarządzania bezpieczeństwem informacji, jakimi są: zapewnienie spełnienia wymagań prawnych, właściwe zabezpieczenie aktywów informacyjnych, ochrona przetwarzania danych, niezawodność funkcjonowania systemów, zmniejszenie ryzyka utraty informacji oraz systematyczna edukacja użytkowników, a w efekcie pełne zaangażowanie wszystkich pracowników w ochronę informacji.

Zarządzanie bezpieczeństwem informacji jest pojęciem obejmującym zasady zarządzania systemem chroniącym istotne aktywa oraz sposoby reagowania na zagrożenia dla tych aktywów. Zapewnienie odpowiedniej wiedzy zarządzających jednostką oraz siecią informatyczną w zakresie pojawiających się nowych zagrożeń oraz metod ochrony jest kolejnym elementem zapewnienia bezpieczeństwa. Pracownicy obsługujący systemy przetwarzające informacje są ogniwem zabezpieczeń, na którego skuteczność wpływa również zapewnienie rzetelnej informacji w zakresie sposobu bezpiecznego użytkowania aktywów instytucji. Niniejszy dokument Polityki Bezpieczeństwa Informacji Urzędu Gminy w Odrzywole jest jednym z elementów Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Polityka Bezpieczeństwa Informacji jest aktem wewnętrznego stosowania wprowadzanym przez Wójta Odrzywołu. Polityka Bezpieczeństwa Informacji opisuje ogólne zasady ochrony informacji obowiązujące w Urzędzie, zasady zarządzania ryzykiem, role i zadania osób uczestniczących w procesie przetwarzania informacji oraz zarządzania bezpieczeństwem informacji. Polityka określa również warunki, jakie muszą spełniać systemy informatyczne przetwarzające informacje w UG w Odrzywole. Konkretne i szczegółowe polityki, instrukcje, procedury i inne regulacje wewnętrzne, wynikające zarówno z przepisów prawa jak i przyjętych przez urząd standardów w obszarze bezpieczeństwa, stanowią dokumenty wewnętrzne urzędu związane z niniejszą Polityką Bezpieczeństwa Informacji i składają się na całość dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji UG w Odrzywole.

Dokumenty referencyjne:

1. Polityka ochrony danych osobowych;
2. Procedura postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Gminy w Odrzywole;
3. Instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń i budynku UG;
4. Instrukcja zarządzania systemami informatycznymi;
5. Polityka czystego biurka i czystego ekranu;
6. Procedura nadawania uprawnień do przetwarzania danych osobowych;
7. Rejestr czynności przetwarzania;
8. Rejestr umów powierzenia przetwarzania danych osobowych;
9. Szacowanie ryzyka;
10. DPIA;
11. Regulamin wykonywania zadań przez Inspektora ochrony danych;
12. Procedura realizacji praw osób, których dane dotyczą;
13. Procedura przetwarzania szczególnych kategorii danych;
14. Regulamin ochrony danych osobowych;
15. Ewidencja uprawnień do przetwarzania danych osobowych.

Deklaracja zaangażowania Najwyższego Kierownictwa

Zgodnie z treścią § 20 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjnosci, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, w Urzędzie Gminy w Odrzywole realizującym zadania publiczne, ustanawia się, wdraża, eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali System Zarządzania Bezpieczeństwem Informacji zapewniający poufność, dostępność, integralność informacji z uwzględnieniem takich atrybutów jak autentyczność, rozliczalność, niezaprzeczalneność i niezawodność. System zarządzanie bezpieczeństwem informacji (SZBI) oparty został na podejściu wynikającym z ryzyka i odnosi się do ustanawiania wdrażania, eksploatacji monitorowania utrzymywania doskonalenia bezpieczeństwa informacji to jest ochrony informacji w każdym punkcie jej przetwarzania. Wymagania (SZBI) mają charakter zintegrowany z innymi procesami realizowanymi w UG w Odrzywole.

Kierownictwo urzędu przywiązuje szczególną wagę do ochrony informacji przetwarzanej w UG w Odrzywole, a także do ochrony informacji powierzonych urzędowi przez inne podmioty celem przetwarzania. Gwarancją odpowiedniej i skutecznej ochrony informacji jest zapewnienie właściwego poziomu bezpieczeństwa oraz zastosowanie adekwatnych do istniejących lub potencjalnych zagrożeń rozwiązań organizacyjnych i technicznych.
Najwyższe Kierownictwo urzędu deklaruje w szczególności:

1. Zapewnienie dostępności zasobów potrzebnych do utrzymywania rozwoju i ciągłego doskonalenia SZBI;

Zaangażowanie w odniesieniu do SZBI w tym w kompleksową ochronę informacji i aktywów wspierających ich przetwarzanie w UG w Odrzywole.

2. oraz promowanie ciągłego doskonalenia ustanowionego systemu;

3. Kierowanie i aktywne wspieranie osób przyczyniających się do osiągnięcia skuteczności SZBI oraz stałe podnoszenie świadomości pracowników Urzędu w zakresie bezpieczeństwa informacji

pełne zaangażowanie wciągłe planowanie, tworzenie, aktualizowanie, sprawdzanie i doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji w UG w Odrzywole.

4. w celu utrzymania go na jak najwyższym poziomie zapewniającym bezpieczeństwo informacjom, w tym danym osobowym przetwarzanym w UG w Odrzywole

Podstawy prawne

Zasady zarządzania bezpieczeństwem informacji w Ministerstwie zostały opracowane zgodnie z obowiązującymi przepisami oraz w oparciu o wymagania Polskich Norm i standardów w obszarze bezpieczeństwa informacji, określonych w szczególności w:

1. ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2019, poz. 700 ze zmianami);
2. ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2019, poz. 1781);
3. ustawie z dnia 06 września 2001 r. o dostępie do informacji publicznej (Dz.U. 2019, poz. 1429);
4. ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. 2019, poz. 162 ze zmianami);
5. ustawie z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. 2019, poz. 848);
6. ustawie z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (Dz.U. 2019, poz. 1696 ze zmianami);
7. rozporządzeniu 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 (Dz.U. 2017, poz. 2247);
8. rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2018.119.1); 10) normie PN-ISO/IEC 27001:2017-06.
9. ustawie z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego (Dz.U.2019.1446 t.j.);
10. ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U.2019.742 t.j.);
11. ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U.2020.1369 t.j.);
12. rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007r. w sprawie Biuletynu Informacji Publicznej (Dz.U.2007.10.68);
13. normach:

a. PN-ISO/IEC 27001,

b. PN-ISO/IEC 27002,
c. PN-ISO/IEC 27005,
d. PN-ISO/IEC 24762.

Definicje

Użyte w Polityce pojęcia oznaczają:
aktywa (zasoby) - wszystko, co stanowi wartość dla UG w Odrzywole.

1. i w związku z tym wymaga ochrony, w szczególności:
    a. aktywa informacyjne (informacje) rozumiane jako wiedza, dane oraz wszelkie informacje wpływające na wartość urzędu, w tym informacje udokumentowane,
    b. zasoby ludzkie - pracownicy, wiedza, umiejętności, doświadczenie i kwalifikacje,
    c. usługi i licencje,
    d. wartości niematerialne, w tym wizerunek, kultura organizacyjna, wartości etyczne,
    e. systemy teleinformatyczne,
    f. urządzenia dostępowe i oprogramowanie,
    g. zabezpieczenia fizyczne, środowiskowe, techniczne i organizacyjne,
    h. siedziba i nieruchomości oraz poszczególne pomieszczenia użytkowane przez urząd;
2. bezpieczeństwo informacji - zabezpieczenie i zachowanie informacji w zakresie integralności, dostępności i poufności przed nieautoryzowanym dostępem lub zmianą; dodatkowo mogą być brane pod uwagę inne atrybuty - rozliczalność, autentyczność, niezaprzeczalność oraz niezawodność;
3. dostępność - właściwość polegająca na tym, że informacja jest dostępna i użyteczna na żądanie upoważnionego podmiotu;
4. incydent związany z bezpieczeństwem informacji - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które zagrażają bezpieczeństwu informacji oraz stwarzają znaczne prawdopodobieństwo utraty aktywów lub zakłócenia realizacji zadań;
5. integralność - właściwość polegająca na zapewnieniu dokładności i kompletności informacji;
6. podatność - słabość lub wrażliwość aktywa lub grupy aktywów w zakresie funkcjonowania urzędu, która może wpłynąć na wystąpienie zagrożenia i jego ewentualne skutki; podatność może dotyczyć, w szczególności sposobu zarządzania lub postępowania, personelu, zależności, relacji, kontaktów wewnętrznych i zewnętrznych, czynnika technologicznego, niedoskonałości zabezpieczeń;
7. poufność - właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
8. ryzyko - potencjalna sytuacja, w której określone zagrożenie wykorzysta podatność aktywa lub grupy aktywów, powodując w ten sposób naruszenie poufności, integralności, dostępności lub innych atrybutów bezpieczeństwa informacji;

użytkownik - pracownik, stażysta, wolontariusz, praktykant lub inna osoba wykonująca pracę bądź świadcząca usługi na podstawie umów cywilnoprawnych na rzecz UG w Odrzywole, zwanego dalej "urzędem/UG", która uzyskała uprawnienie albo upoważnienie do przetwarzania danych osobowych w danym zakresie, w tym do przetwarzania informacji w systemach teleinformatycznych;

9. zabezpieczenie - działanie lub rozwiązanie, które ogranicza prawdopodobieństwo wystąpienia zagrożenia lub minimalizuje jego negatywne skutki oraz wpływa na osiągnięcie celów; wyróżnia się trzy rodzaje zabezpieczeń funkcjonujących w UG:
   a. organizacyjne (struktury organizacyjne, polityki, procedury postępowania, zarządzenia, regulaminy, klauzule w umowach, zakresy obowiązków pracowników, szkolenia, audyty, kontrole itp.),
   b. techniczne (systemy bezpieczeństwa teleinformatycznego, systemy kontroli dostępu, depozytory kluczy, urządzenia alarmowe lub monitoringu, oprogramowanie antywirusowe itp.),
   c. fizyczne (ogrodzenie, drzwi, zamykane szafy, sejfy, strefy ochronne itp.);

10. dane osobowe – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Osoba fizyczna możliwa do zidentyfikowania 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;
11. administrator – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania. Administratorem jest Wójt Gminy Odrzywół;
12. inspektor Ochrony Danych (IOD) – osoba wyznaczona przez Administratora do zadań której należy zapewnienie przestrzegania przepisów o ochronie danych osobowych.

Terminologia

Ilekroć w Polityce Bezpieczeństwa Informacji jest mowa o:

„Polityce" - należy przez to rozumieć Politykę Bezpieczeństwa Informacji w Urzędzie Gminy w Odrzywole.

„Mieście" – należy przez to rozumieć Gminę – Gminę Odrzywół;

„Wójt Gminy" – należy przez to rozumieć Wójt Gminy Odrzywół;

„Urzędzie" - należy przez to rozumieć ;

„UG" - należy przez to rozumieć Urząd Gminy w Odrzywole;

„Systemie informatycznym" - należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur, narzędzi programowych zastosowanych do przetwarzania informacji i danych;

„**SZBI**" - należy przez to rozumieć System Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy w Odrzywole.

Organizacja bezpieczeństwa informacji

1. Polityka jest podstawowym elementem w dokumentacji SZBI.
2. Polityką objęte są wszystkie informacje wykorzystywane przez UG, niezależnie od formy i nośnika przetwarzania lub dystrybucji (ustne, pisemne, nagrania audio i video), utrwalone na nośnikach elektronicznych, systemach komputerowych oraz wytworzone w dokumentach, będące własnością urzędu oraz powierzone w ramach umów lub porozumień z kontrahentami lub wykonawcami.
3. Polityka ma zastosowanie do wszystkich komórek organizacyjnych UG i obejmuje zakresem nie tylko obszar urzędu, ale także miejsca i sytuacje, w których informacje związane z działalnością urzędu są przetwarzane poza jego siedzibą, w szczególności w kontekście pracy zdalnej.
4. Do przestrzegania Polityki zobowiązane są wszystkie osoby korzystające z zasobów urzędu, w szczególności:

a. pracownicy;
b. osoby świadczące usługi na podstawie umów cywilnoprawnych, w tym umów zlecenia lub umów o dzieło;
c. osoby odbywające praktykę, staż lub wolontariat, w zakresie określonym odpowiednio w umowie o odbywaniu praktyki lub stażu, programie praktyki lub stażu, porozumieniu o świadczeniu wolontariatu;
d. eksperci oraz pracownicy podmiotów zewnętrznych realizujący inne, niż określone w pkt 1-3 zadania.

5. Każdy pracownik Urzędu jest zapoznawany z zasadami bezpieczeństwa oraz z aktualnymi procedurami ochrony informacji w swojej komórce organizacyjnej oraz w UG. Stażyści oraz praktykanci również są zapoznawani z tymi zasadami. Kierownik komórki organizacyjnej jest odpowiedzialny za ochronę bezpieczeństwa informacji w podległej komórce, a w szczególności za monitorowanie integralności i dostępności posiadanych zasobów informacji, nadzorowanie przestrzegania zasad bezpieczeństwa przez podległych pracowników oraz podejmowanie stosownych działań w razie stwierdzenia wystąpienia incydentu lub sytuacji mogącej prowadzić do wystąpienia incydentu bezpieczeństwa.
6. Właściciel aktywu odpowiada za bieżące nadzorowanie oraz zarządzanie aktywem.
7. Odpowiedzialność za realizację ochrony informacji w Urzędzie ponoszą wszyscy pracownicy Urzędu – proporcjonalnie do wykonywanych obowiązków i posiadanych uprawnień.

Zakres Systemu Zarządzania Bezpieczeństwem Informacji

Zakres SZBI dotyczy obsługi administracyjnej ludności i podmiotów gospodarczych oraz zarządzania przestrzenią miejską.
Zakresy określone przez dokument Polityki Bezpieczeństwa Informacji mają zastosowanie do całego systemu informacyjnego Urzędu Gminy w Odrzywole, obejmującego w szczególności:

1. wszystkie istniejące, wdrażane obecnie lub w przyszłości systemy informatyczne oraz papierowe, w których przetwarzane są informacje podlegające ochronie;
2. informacje będące własnością Urzędu przetwarzane w ramach realizowanych procesów i zadań, w tym:

a. przetwarzane w formie tradycyjnej (m.in. informacje wydrukowane lub zapisane na papierze),
b. przetwarzane w formie elektronicznej (min. przesyłane za pośrednictwem poczty elektronicznej lub urządzeń elektronicznych, elektronicznych nośników informacji),

3. będące własnością urzędu lub stron zainteresowanych, o ile zostały przekazane na podstawie obowiązujących przepisów prawnych lub umów.

4. informacje będące własnością klientów Urzędu, uzyskane na podstawie zawartych umów;
5. wszystkie lokalizacje Urzędu, czyli budynki i pomieszczenia, w których są lub będą przetwarzane informacje podlegające ochronie;
6. wszyscy pracownicy w rozumieniu przepisów Kodeksu Pracy, konsultanci, stażyści i inne osoby mające dostęp do informacji podlegających ochronie;
7. aktywa wspierające przetwarzanie informacji w ramach procesów oraz realizowanych w Urzędzie działań i zadań, w tym:

a. sprzęt, w tym sprzęt komputerowy, urządzenia mobilne oraz inne nośniki danych, na których znajdują się informacje podlegające ochronie, oprogramowanie, infrastruktura sieciowa,
b. technologie służące pozyskiwaniu, selekcjonowaniu, analizowaniu, przetwarzaniu, zarządzaniu i udostępnianiu informacji, do których zalicza się zarówno systemy papierowe jak i elektroniczne wspomagające realizację zadań publicznych,
c. struktura organizacyjna (wszystkie komórki organizacyjne wskazane w Regulaminie Organizacyjnym UG w Odrzywole).

8. Z uwagi na szczególny charakter informacji niejawnych wynikający z obowiązujących przepisów prawa, ochrona informacji niejawnych i aktywów wspierających ich przetwarzanie podlega wyłączeniu z ustanowionego SZBI. Zasady i tryb ochrony informacji niejawnych w urzędzie określone zostały w treści odrębnych uregulowań wewnętrznych.

Struktura dokumentacji SZBI

W ramach ustanowionego SZBI wprowadza się dokumentację bezpieczeństwa określającą zasady i tryb zarządzania bezpieczeństwem informacji oraz aktywów wspierających przedmiotowe przetwarzanie w UG. W ramach SZBI wyróżnia się:

1. Politykę Bezpieczeństwa Informacji Urzędu Gminy w Odrzywole– dokument główny, nadrzędny w stosunku do pozostałych wewnętrznych aktów prawnych dotyczących bezpieczeństwa informacji obowiązujących w Urzędzie, tworzących wspólnie

dokumentację bezpieczeństwa, określającą ogólne ramy, kierunki, zasady i wymogi bezpieczeństwa informacji w UG;

2. dokumenty dedykowane i udostępniane wszystkim pracownikom UG, praktykantom, stażystom, wolontariuszom, w uzasadnionych przypadkach wybranym osobom i podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz UG i/lub mającym dostęp do aktywów informacyjnych Urzędu, wśród nich wyróżnia się dedykowane polityki i procedury tematyczne oraz instrukcje wykonawcze:
   - polityka kluczy,
   - Polityka ochrony danych osobowych;
   - Procedura postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Gminy w Odrzywole;
   - Instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń i budynków UG w Odrzywole;
   - Polityka czystego biurka i czystego ekranu;
   - Procedura nadawania uprawnień do przetwarzania danych osobowych;
   - Rejestr czynności przetwarzania;
   - Procedura nadawania uprawnień;
   - Rejestr umów powierzenia przetwarzania danych osobowych;
   - Szacowanie ryzyka;
   - DPIA;
   - Regulamin wykonywania zadań przez Inspektora ochrony danych;
   - Procedura realizacji praw osób, których dane dotyczą;
   - Procedura przetwarzania szczególnych kategorii danych;
   - Regulamin ochrony danych osobowych;
   - Ewidencja uprawnień do przetwarzania danych osobowych,

wprowadzane i aktualizowane w formie odrębnych dokumentów na mocy zarządzeń Wójta Gminy Odrzywół. Dokumenty uzupełniają się wzajemnie, tworząc kompleksową dokumentację Systemu Informacji w UG dokumentację bezpieczeństwa. Celem zapewnienia właściwości, adekwatności i skuteczności obowiązujących przepisów wewnętrznych w zakresie bezpieczeństwa, prowadzone są okresowe przeglądy i aktualizacja ww. dokumentacji.

Zasady dotyczące bezpieczeństwa informacji

Polityka SZBI realizowana jest poprzez:

1. Zapewnienie odpowiedniej jakości procesów przetwarzania informacji w szczególności skuteczności i adekwatności działania zabezpieczeń (lub ich grup) i środków chroniących przed nieuprawnionym ujawnieniem, odpowiednich warunków do ich użytkowania oraz sprawności i efektywności ich wykorzystywania;

2. pracowników posiadających odpowiednią wiedzę, umiejętności i doświadczenie adekwatne do powierzonych zadań;
3. ochronę fizyczną, techniczną i organizacyjną aktywów przed dostępem osób nieupoważnionych, w szczególności przed nieuprawnionym wykorzystaniem, kradzieżą, uszkodzeniem, nieuprawnioną modyfikacją lub zniszczeniem;
4. zabezpieczenie systemów teleinformatycznych eksploatowanych w Urzędzie przed zagrożeniami;
5. zabezpieczenie aktywów Urzędu przed ich uszkodzeniem lub zniszczeniem w wyniku pożaru, zalania, ataku terrorystycznego, zjawisk naturalnych lub innych zagrożeń;
6. zapewnienie ciągłości działania procesów przetwarzania informacji;
7. zapewnienie możliwości sprawnego odtworzenia aktywów w przypadku ich zniszczenia;
8. zapewnienie gotowości do reakcji na sytuację awaryjną lub kryzysową;
9. zapewnienie rozwiązań organizacyjnych i systemowych regulujących zasady i sposób zarządzania bezpieczeństwem informacji;
10. zapewnienie pracownikom szkoleń i innych akcji promocyjno-edukacyjnych z zakresu bezpieczeństwa informacji;
11. zapewnienie działań kontrolnych w zakresie przestrzegania zasad określonych w Polityce;
12. przestrzeganie zasad bezpieczeństwa informacji, o których mowa poniżej.

Stosowanie zabezpieczeń powinno uwzględniać następujące zasady:

1. zabezpieczenia powinny być adekwatne do wymogów prawnych oraz wyników audytów i analiz ryzyka bezpieczeństwa informacji;
2. zabezpieczenia fizyczne, techniczne i organizacyjne powinny uzupełniać się wzajemnie, zapewniając wymagany poziom bezpieczeństwa informacji;
3. w doborze zabezpieczeń należy kierować się w szczególności:

a. adekwatnością,
b. zaleceniami Polskiej Normy PN-ISO 27002,
c. uwzględnieniem wyników szacowania ryzyka;

4. świadomość pracowników w zakresie bezpieczeństwa informacji powinna być doskonalona w szczególności poprzez różne formy podnoszenia kwalifikacji;
5. należy podejmować działania na rzecz utrzymania standardów współpracy Urzędu z osobami i podmiotami zewnętrznymi, poprzez stosowanie zasad regulujących kwestie poufności w ramach realizacji umów, porozumień i innych form relacji, obowiązujących Strony również po ustaniu współpracy.

Skuteczność SZBI zachowuje się przy jednoczesnym zastosowaniu i uzupełnianiu się elementów regulujących obszary bezpieczeństwa fizycznego i środowiskowego, technicznego, organizacyjnego.

Poziom bezpieczeństwa informacji jest odpowiedni wówczas, gdy spełnione są następujące warunki:

a. dokonano szacowania ryzyka w odniesieniu do bezpieczeństwa informacji;
b. wdrożono skuteczne zabezpieczenia wymagane przepisami prawa i Polityką.

W Urzędzie stosuje się następujące zasady dotyczące bezpieczeństwa informacji:

1. wiedzy koniecznej (ograniczonego dostępu do informacji) - pracownicy posiadają dostęp tylko do tych informacji, które są konieczne do realizacji powierzonych im zadań; zasada ta dotyczy głównie informacji wrażliwych; zasada ta ma ograniczone

znaczenie dla pewnych grup informacji, w szczególności informacji dostępnych publicznie;

2. indywidualnej odpowiedzialności - za utrzymanie odpowiedniego poziomu bezpieczeństwa poszczególnych aktywów lub ich elementów odpowiadają konkretne osoby, w zakresie nałożonych obowiązków i nadanych uprawnień;
3. czystego biurka i czystego ekranu:

a. podczas dłuższej nieobecności pracownika na stanowisku pracy dokumenty i informatyczne nośniki danych przechowywane - w miarę możliwości organizacyjno-technicznych - należy przechowywać w odpowiednio zabezpieczonych meblach biurowych lub szafach metalowych/sejfach,

b. na czas nieobecności pracownika dostęp do komputera jest blokowany, a po zakończeniu pracy komputer jest wyłączany, chyba że dany komputer musi pracować w trybie ciągłym - np. serwer obsługujący systemy alarmowe; w czasie obecności pracownika monitor powinien być tak ustawiony, aby nie pozwalał na zapoznawanie się z wyświetlanymi treściami przez osoby postronne, nieupoważnione;

4. dyskrecji (ograniczonego zaufania i odpowiedzialnej konwersacji) - wszelkie informacje służbowe mogą być przekazywane wyłącznie w celu wykonywania zadań w zakresie do tego niezbędnym oraz osobom uprawnionym do pozyskania tych informacji; zasada ta ma ograniczone znaczenie dla pewnych grup informacji, np. informacji dostępnych publicznie;
5. obecności koniecznej - prawo przebywania w określonych miejscach - istotnych dla bezpieczeństwa informacji - powinny mieć tylko osoby upoważnione;
6. zamykania pomieszczeń - niedopuszczalne jest pozostawienie pod nieobecność pracownika niezabezpieczonego pomieszczenia służbowego, zarówno w godzinach pracy, jak i po jej zakończeniu; na zakończenie dnia pracy ostatnia wychodząca z pomieszczenia osoba powinna zamknąć wszystkie okna i drzwi oraz zabezpieczyć klucze do pomieszczenia;
7. nadzorowania dokumentów - po godzinach pracy wszystkie dokumenty zawierające informacje podlegające ochronie powinny być przechowywane w miejscach zabezpieczonych przed dostępem osób nieuprawnionych;
8. zachowania prywatności kont w systemach - każdy pracownik zobowiązany jest do pracy w systemach teleinformatycznych na przypisanych lub udostępnionych mu kontach; zabronione jest udostępnianie własnych kont osobom trzecim;
9. poufności haseł - każdy pracownik zobowiązany jest do zachowania poufności udostępnionych mu haseł i kodów dostępu, w szczególności do systemów teleinformatycznych;
10. legalnego oprogramowania - na stacjach roboczych zainstalowane jest wyłącznie legalne oprogramowanie umożliwiające automatyczne aktualizacje;
11. zgłaszania incydentów bezpieczeństwa informacji - każdy użytkownik ma obowiązek niezwłocznie zgłosić wystąpienie lub podejrzenie wystąpienia incydentu bezpieczeństwa informacji;
12. automatyzacji backupu - procesy tworzenia kopii zapasowych powinny być zautomatyzowane oraz niemożliwe do przerwania przez pracownika;
13. ochrony nośników danych - dane kopiowane na nośniki i wynoszone poza Urząd powinny być odpowiednio zabezpieczone w czasie transportu i przechowywania, co najmniej poprzez szyfrowanie;
14. adekwatności zabezpieczeń - używane mechanizmy zabezpieczeń powinny być adekwatne do zagrożeń, podatności, wartości aktywów oraz innych istotnych okoliczności;

15. kompleksowości ochrony (asekuracji zabezpieczeń) - ochrona aktywów systemu przetwarzania informacji powinna opierać się na stosowaniu różnych mechanizmów ochrony, w tym ochrony: prawnej, fizycznej, technicznej oraz organizacyjnej;
16. bezpiecznej współpracy z podmiotami zewnętrznymi - dokumenty regulujące współpracę powinny zawierać stosowne klauzule bezpieczeństwa, w tym o zachowaniu poufności, zasadach postępowania z pozyskaną informacją, niszczenia lub zwrotu dokumentacji po ich wykorzystaniu;
17. doskonalenia - SZBI jest stale monitorowany i dostosowywany do zmieniających się warunków wewnętrznych i zewnętrznych;
18. czystego kosza - dokumenty papierowe, z wyjątkiem materiałów promocyjnych, marketingowych i innych publicznie dostępnych, powinny być niszczone w sposób uniemożliwiający ich odczytanie.

Katalog zasad, o których mowa powyżej jest otwarty i może być rozszerzony lub uszczegółowiony w innych dokumentach stanowiących dokumentację SZBI.

Klasyfikacja informacji i zasady postępowania z informacjami

1. Klasyfikacja została wprowadzona w celu uporządkowania w Urzędzie postępowania z informacjami, które są głównym zasobem organizacji.

Podstawowym elementem klasyfikacji są grupy informacji. W grupach informacji zebrane zostały dokumenty logicznie ze sobą powiązane o podobnych wymaganiach związanych z bezpieczeństwem. Do określenia poziomu bezpieczeństwa danej grupy informacji przyjęto wskaźniki definiujące poufność, integralność oraz dostępność danej grupy informacji, wymagane w Urzędzie.

Przez poufność rozumiemy zapewnienie, iż dostęp do informacji mają tylko i wyłącznie osoby uprawnione. Przez integralność rozumiemy zapewnienie, iż informacje nie zostały zmienione lub zniszczone w nieautoryzowany sposób (niezgodny z wewnętrznymi regulacjami Urzędu).

Przez dostępność rozumiemy możliwość dostępu do informacji w takim czasie, jaki jest oczekiwany przez użytkownika. Ze względu na charakter pracy Urzędu i cel jego funkcjonowania do określenia wskaźników bezpieczeństwa największy nacisk położono na parametr integralności.

Struktura informacji w Urzędzie opiera się na klasyfikacji następujących grup:

Grupa informacji	Opis
Dane osobowe	W rozumieniu przepisów dot. ochrony danych osobowych informacje stanowiące dane osobowe podlegające ochronie na mocy przepisów o ochronie danych osobowych. Dane osobowe to informacje, które RODO definiuje jako: "wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej". Ochrona danych osobowych oparta jest m.in. na zapisach RODO, ustawy o ochronie danych osobowych, Polityce Bezpieczeństwa Danych Osobowych, przyjętych dobrych

	praktykach z tego obszaru. Za organizację systemu ochrony danych osobowych odpowiada ADO, za przestrzeganie przyjętych zasad ich ochrony odpowiada ASI oraz IOD. Dane osobowe przetwarzane w UG dotyczą m.in. klientów, mieszkańców, pracowników, rodzin pracowników, kontrahentów, i in.
Informacje jawne	Informacje, których obowiązek udostępniania wynika z przepisów prawa, w szczególności informacje publiczne w rozumieniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej. Informacje udostępniane w szczególności na stronach internetowych Urzędu.
Informacje prawnie chronione	Informacje przekazane Urzędowi przez przedsiębiorcę, co do których podjął on działania w celu zachowania ich w poufności, w szczególności nieujawnione do wiadomości publicznej informacje organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą (tajemnica przedsiębiorstwa). Informacje chronione na mocy ustawy o ochronie informacji niejawnych (uregulowane odrębnymi przepisami). Inne informacje chronione z mocy prawa tajemnice powołane na mocy ustaw, których obowiązek ochrony wynika z tychże ustaw)
Informacje wrażliwe	Informacje wewnętrzne UG, wytworzone w Urzędzie lub na jego rzecz, niewchodzące w zakres informacji zaklasyfikowanych do pozostałych grup. Są to informacje ogólnie dostępne wewnątrz Urzędu oraz przeznaczone do użytku wewnętrznego.
Informacje wewnętrzne	Informacje, których ewentualne udostępnienie poza Urząd wymaga złożenia stosownego wniosku oraz analizy prawnej dotyczącej możliwości udostępnienia informacji wskazanej we wniosku oraz analizy ewentualnych konsekwencji związanych z jej udostępnieniem.

2. Wprowadzenie klasyfikacji informacji, o której mowa w ust. 1 nie powoduje konieczności specjalnego fizycznego oznaczania informacji udokumentowanych, dokonuje się w nich jedynie odwzorowania literowo-cyfrowego zgodnie z Instrukcją kancelaryjną lub oznaczenia identyfikujące dokument w systemie Elektronicznego Zarządzania Dokumentacją (EZD).

3. W Urzędzie przyjmuje się następujące zasady postępowania z informacjami:

Grupa informacji	Zasady

Dane osobowe	Przetwarzanie, przechowywanie, przekazywanie: w sposób gwarantujący zachowanie bezpieczeństwa, integralności, poufności i dostępności informacji. Niszczenie: zgodnie z wymogami określonymi w przepisach prawa lub zawartych przez urząd umowach oraz instrukcją kancelaryjną.
Informacje jawne	Przetwarzanie, przechowywanie, przekazywanie: w sposób gwarantujący zachowanie integralności i dostępności informacji. Udostępnianie: na zasadach i w trybie przewidzianym przepisami prawa. Niszczenie: zgodnie z wymogami określonymi w przepisach prawa lub zawartych przez Urząd umowach oraz Instrukcją kancelaryjną.
Informacje prawnie chronione	Przetwarzanie: w sposób gwarantujący zapewnienie bezpieczeństwa informacji ze szczególnym uwzględnieniem atrybutów integralności, dostępności i poufności oraz innych atrybutów bezpieczeństwa, które są wymagane dla danej informacji chronionej na podstawie właściwej ustawy. Przechowywanie: w sposób gwarantujący zapewnienie bezpieczeństwa informacji. Przekazywanie: wyłącznie osobom uprawnionym, w sposób gwarantujący zachowanie integralności i poufności oraz zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych przez Urząd umowach. Udostępnianie: wyłącznie uprawnionym osobom lub podmiotom po uzyskaniu zgody kierownictwa Urzędu lub kierownika właściwej komórki organizacyjnej. Niszczenie: zgodnie z wymogami określonymi w przepisach prawa lub zawartych przez Urząd umowach oraz Instrukcją kancelaryjną.
Informacje wrażliwe	Przetwarzanie: w sposób gwarantujący zapewnienie bezpieczeństwa informacji, ze szczególnym uwzględnieniem atrybutów integralności, dostępności i poufności. Zgodnie z przyjętą Procedurą przetwarzania szczególnych kategorii danych. Przechowywanie: w sposób gwarantujący zapewnienie bezpieczeństwa informacji.

	Przekazywanie: wyłącznie osobom uprawnionym (pracownikom Urzędu, osobom/pracownikom podmiotów z którymi Urząd zawarł stosowne umowy) w sposób gwarantujący zachowanie integralności i dostępności informacji oraz zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych umowach. Zmiana klasyfikacji: możliwa po podjęciu decyzji przez uprawnione osoby oraz zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych przez umowach. Udostępnianie: wyłącznie po uzyskaniu zgody kierownika właściwej komórki organizacyjnej. Niszczenie: zgodnie z wymogami określonymi w przepisach prawa lub zawartych przez umowach oraz Instrukcją kancelaryjną.
Informacje wewnętrzne	Przetwarzanie: w sposób gwarantujący zachowanie integralności, dostępności i poufności informacji. Przechowywanie: w sposób gwarantujący zapewnienie bezpieczeństwa informacji. Przekazywanie: możliwe wysyłanie adresatom zewnętrznym po dokonaniu analizy prawnej dotyczącej możliwości udostępnienia informacji oraz analizy ewentualnych konsekwencji z tym związanych. Przekazywanie wewnątrz Urzędu na zasadach określonych przez kierownika właściwej komórki organizacyjnej. Udostępnianie: wyłącznie po uzyskaniu zgody kierownika właściwej komórki organizacyjnej. Niszczenie: zgodnie z Instrukcją kancelaryjną.

Zarządzanie aktywami

Urząd zarządza swoimi aktywami informacyjnymi poprzez zapewnienie im wymaganego poziomu bezpieczeństwa. Identyfikowane są aktywa informacyjne i klasyfikowane zgodnie ze stawianymi im wymaganiami w zakresie ochrony. Właścicielem aktywów informacyjnych w Urzędzie są kierownicy jednostek organizacyjnych, osoby obejmujące samodzielne

stanowiska jak również w szczególnych przypadkach mogą nimi być wskazani, konkretni pracownicy, w zależności od przydzielonych im zadań. Własność w rozumieniu systemu zarządzania bezpieczeństwem informacji nie oznacza prawa własności w rozumieniu zapisów kodeksu cywilnego, ale odnosi się do szczególnej odpowiedzialności za prawidłowe zarządzanie aktywem.

Zarządzanie ryzykiem w bezpieczeństwie informacji

1. Skuteczne zarządzanie bezpieczeństwem informacji wymaga podejmowania okresowych działań w obszarze zarządzania ryzykiem, w szczególności w zakresie szacowania tj. identyfikowania, analizy i oceny ryzyka w bezpieczeństwie informacji, zmierzających do ograniczenia oraz eliminacji przedmiotowego ryzyka. W obszarze bezpieczeństwa informacji identyfikacja i analiza ryzyka jest obligatoryjna i przeprowadza się ją cykliczne. Identyfikację i analizę ryzyka przeprowadza się w oparciu o dostępne metodyki.
2. Działania związane z zarządzaniem ryzykiem mającym wpływ na bezpieczeństwo informacji obejmują w szczególności:
   a. przygotowanie oraz okresową aktualizację dokumentów dot. zarządzania ryzykiem,
   b. prowadzenie okresowego szacowania ryzyka,
   c. postępowanie z ryzykiem,
   d. podejmowanie działań korygujących.

3. Szczegółowe zasady dot. zarządzania ryzykiem w bezpieczeństwie informacji zostały uregulowane w *dedykowanej Procedurze szacowania i postępowania z ryzykiem* oraz w *Procedurze ocena skutków dla ochrony danych (DPIA).*

Bezpieczeństwo fizyczne i środowiskowe

W celu zapobieżenia nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w przetwarzaniu informacji i środkach przetwarzania informacji należących do UG oraz utracie, zniszczeniu, uszkodzeniu, kradzieży aktywów informacyjnych, wykorzystywane są wdrożone mechanizmy ochrony w obszarze bezpieczeństwa fizycznego i środowiskowego. m.in. system zamków i kontroli dostępu do pomieszczeń, system monitoringu wizyjnego. W celu zabezpieczenia przed zagrożeniami zewnętrznymi i środowiskowymi kluczowe systemy techniczne i teleinformatyczne zostały wyposażone w systemy utrzymujące optymalne warunki środowiskowe oraz podtrzymujące zasilanie (UPS), a także opracowano praktyki i procedury postępowania w razie wystąpienia potencjalnych zagrożeń.

Zabezpieczenia kryptograficzne

W celu zapewnienia poufności, autentyczności i integralności informacji w UG stosowane są zabezpieczenia kryptograficzne wszędzie tam, gdzie istnieje konieczność ich stosowania. Zastosowanie konkretnego narzędzia kryptograficznego jest poprzedzone oszacowaniem ryzyka pod kątem wyboru typu zabezpieczenia.

Zarządzanie systemami i sieciami

Urząd Gminy w Odrzywole przykłada dużą wagę do przestrzegania zasad bezpieczeństwa związanych z utrzymywaniem i użytkowaniem systemów informatycznych oraz sieci. Celem takiego postępowania jest zapewnienie poufności, integralności i dostępności przetwarzanej przez ww. systemy informacji.
Skuteczna realizacja tego celu możliwa jest dzięki:
1. kompetencjom i świadomości pracowników oraz podpisanym umowom ze specjalistycznymi firmami;
2. obowiązującym zasadom konserwacji urządzeń w celu zapewnienia ich ciągłej pracy;
3. kontrolowaniu wprowadzania zmian do infrastruktury technicznej;
4. nadzorowaniu usług dostarczanych przez strony trzecie a w szczególności wszelkim wprowadzanym do nich zmianom. Plany zakupu lub wprowadzenia zmian do systemu uwzględniają wpływ nowych procesów na istniejący system bezpieczeństwa;
5. kontroli systemów - przed dopuszczeniem do użytkowania - pod kątem spełnienia standardów obowiązujących w UG;
6. wdrożonym zabezpieczeniom chroniącym przed złośliwym oprogramowaniem i złośliwym kodem mobilnym;
7. usystematyzowanemu tworzeniu i testowaniu kopii bezpieczeństwa;
8. przestrzeganiu opracowanych zasad postępowania z nośnikami;
9. bieżącemu monitorowaniu aktywów informacyjnych, w tym informatycznych, pod kątem wcześniejszego wykrycia wszelkich niebezpieczeństw mogących zagrozić bezpieczeństwu systemów;
10. monitorowaniu poziomu incydentów w systemach informatycznych i odpowiedniej reakcji w przypadku ich wystąpienia.
Szczegółowe zasady bezpieczeństwa związane z utrzymywaniem i użytkowaniem systemów informatycznych oraz sieci zostały opisane w *Instrukcji zarządzania systemami informatycznymi*.

Zasady nadawania uprawnień

Szczegółowa procedura opisująca obieg wniosku o nadanie upoważnienia i uprawnień do systemów teleinformatycznych stanowi załącznik do *Procedury nadawania uprawnień*.

Kontrola dostępu

W celu skutecznej realizacji zasady uprawnionego dostępu w UG, dostęp do miejsc, urządzeń, systemów, w których informacje są przetwarzane jak i samej informacji jest kontrolowany.

1. Kontrola dostępu do pomieszczeń służbowych.

Wszystkie pomieszczenia służbowe są zabezpieczane przed dostępem osób nieuprawnionych np. zamykane na klucz, alarmem. Każdy pracownik odpowiada za powierzony mu klucz i nie może udostępniać go osobom trzecim. Niedopuszczalne jest pozostawienie bez nadzoru w pomieszczeniu służbowym osób nieuprawnionych. Niedopuszczalne jest także pozostawienie niezabezpieczonego pomieszczenia służbowego w sytuacji, gdy nie znajdują się w nim osoby uprawnione. W UG wdrożona została *Polityka kluczy*, która zawiera szczegółowe zasady dostępu do pomieszczeń i postępowania z kluczami.

2. Kontrola dostępu do sieci i systemów teleinformatycznych.

W UG sprawowany jest nadzór nad wszystkimi urządzeniami i systemami podłączanymi do sieci. Aby zapewnić dostateczną ochronę usług sieciowych przed nieautoryzowanym dostępem, każde urządzenie lub system podłączane do sieci musi spełniać określone wymagania. Przed uzyskaniem dostępu do systemów teleinformatycznych wszystkie osoby wykonujące zadania na rzecz UG podpisują stosowne oświadczenie, w którym są zobowiązane do zachowania w tajemnicy informacji chronionych, natomiast pracownicy firm zewnętrznych zobowiązani są do zachowania poufności stosownymi oświadczeniami zawartymi w umowach podpisywanych z podmiotami zewnętrznymi.

Bezpieczeństwo zasobów ludzkich

Urząd Gminy w Odrzywole przykłada szczególną wagę, aby wyznaczone zadania realizowali kompetentni, świadomi swoich ról i odpowiedzialności pracownicy. Takie podejście ma na celu zminimalizowanie ryzyka błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania zasobów informacyjnych. Podstawowym i skutecznym sposobem realizacji tego celu jest przyjęcie zgodnych z obowiązującym prawem praktyk uwzględniających obszar bezpieczeństwa informacji m.in. związanych z weryfikacją kandydatów do pracy podczas naboru, zasadom zatrudniania pracowników oraz ustalonym procedurom rozwiązywania umów o pracę (przed zatrudnieniem – na etapie rekrutacji, podczas trwania umowy związanej z zatrudnieniem oraz po zakończeniu zatrudnienia). Niezwykle ważny jest też element szkoleń i ciągłego uświadamiania, rozwiązany systemowo i skierowany do wszystkich pracowników UG na każdym etapie zatrudnienia. Dodatkowo Urząd zapewnia osobom mającym przypisane role w SZBI lub zajmującym stanowisko związane z bezpieczeństwem informacji specjalistyczne szkolenia z zakresu bezpieczeństwa informacji i ochrony danych osobowych w celu zapewnienia, podnoszenia i utrzymania kompetencji.

Relacje z podmiotami zewnętrznymi

1. Celem zapewnienia ochrony aktywów informacyjnych udostępnianych usługodawcom, dostawcą i innym osobom i podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz UG lub mającym dostęp do aktywów Urzędu, wprowadza się zasady postępowania w przypadku współpracy związanej z dostępem do aktywów informacyjnych UG i korzystania z usług ww. osób i podmiotów.
2. W przypadku wykonywania zadań delegowanych i/lub korzystania z aktywów, w tym przetwarzania informacji powierzonych przez podmioty zewnętrzne w drodze stosownej umowy i/lub porozumienia, poza wymogami określonymi w obowiązującej w UG dokumentacji bezpieczeństwa dopuszcza się stosowanie wymogów i zaleceń bezpieczeństwa określonych przez ww. podmioty zewnętrzne, o ile wskazane wymogi i zalecenia „zewnętrzne" nie obniżają poziomu bezpieczeństwa pozostałych informacji przetwarzanych w Urzędzie.

Zarzadzanie ciągłością działania

Urząd dba o zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem danych. Celem takiego postępowania jest przeciwdziałanie przerwom w działalności oraz ochrona krytycznych procesów przed rozległymi awariami lub katastrofami. Realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z zarządzeniem ciągłością działania tak, aby ograniczyć do akceptowalnego poziomu skutki wypadków i awarii. UG podejmuje działania w zakresie planowania, weryfikowania, zapewnienia, przeglądu i oceny ciągłości działania i postępowania w przypadku wystąpienia sytuacji kryzysowych. Zasady reagowania na zdarzenia mogące prowadzić do zaburzenia procesów przetwarzania informacji są przedmiotem instrukcji i planów awaryjnych. Plany awaryjne podlegają systematycznemu testowaniu.

Zgodność z przepisami prawa i zapisami umownymi

1. W celu uniknięcia naruszenia obowiązujących przepisów prawa, zobowiązań ustawowych, zapisów zawartych umów i porozumień w UG prowadzona jest bieżąca kontrola zgodności regulacji wewnętrznych, przyjętych zasad bezpieczeństwa i ich stosowania z ww. przepisami w tym identyfikowanie, dokumentowanie i aktualizowanie wszystkich istotnych wymagań prawnych, regulacyjnych, umownych oraz podejścia organizacji do ich przestrzegania.

2. Kierownicy komórek organizacyjnych, w zakresie zadań realizowanych zgodnie z *Regulaminem Organizacyjnym* prowadzą bieżący nadzór w swoich komórkach w zakresie zgodności z przepisami prawa i zapisami umownymi.
3. Inspektor Ochrony Danych w UG odpowiedzialny jest za zapewnienia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
4. Kierownicy poszczególnych komórek organizacyjnych UG dokonują okresowych przeglądów regulacji wewnętrznych dotyczących bezpieczeństwa informacji w zakresie ich zgodności z przepisami prawa i zapisami umownymi.
5. Audytor Wewnętrzny zapewnia okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
6. *Polityka Bezpieczeństwa Informacji Urzędu Gminy w Odrzywole jest* zgodna z obowiązującymi przepisami prawa oraz wybranymi standardami międzynarodowymi dot. bezpieczeństwa informacji.

Postanowienia końcowe

Najwyższe kierownictwo Urzędu zapoznaje pracowników Urzędu, stażystów i praktykantów z dokumentem Polityki Bezpieczeństwa Informacji oraz Instrukcją podstawowych zasad bezpieczeństwa dla pracowników Urzędu. Kierownik każdej komórki organizacyjnej Urzędu jest odpowiedzialny za zebranie od podległych pracowników oświadczeń o zapoznaniu się z instrukcją i przyjęciu jej do stosowania. Naruszenia świadome bądź przypadkowe niniejszej Polityki Bezpieczeństwa Informacji (wraz z wszystkimi dokumentami operacyjnymi) powodują skutki prawne zgodnie z Regulaminem Pracy, a w przypadkach zastrzeżonych przez ustawodawcę – karne wynikające z odpowiedzialności określonej przez przepisy prawa.

Wykaz załączników

1. Załącznik nr 1 Oświadczenie o zapoznaniu się z Polityką Bezpieczeństwa Informacji w Urzędzie Gminy
2. Załącznik nr 2 Instrukcja Zarządzania Systemami Informatycznymi

WÓJT
mgr Marian Kmieciak
.....
Podpis Wójta

Załącznik nr 1

Oświadczenie o zapoznaniu się z Polityką Bezpieczeństwa Informacji w Urzędzie Gminy w Odrzywole

Niniejszym oświadczam, że zapoznałem/am się z Polityką Bezpieczeństwa Informacji w ***Urzędzie Gminy w Odrzywole*** i zobowiązuję się do przestrzegania zawartych w niej zasad.

Ponadto mam na uwadze zachowanie w tajemnicy informacji prawnie chronionych, do których mam lub będę miał/a dostęp w związku z wykonywaniem przeze mnie obowiązków pracowniczych lub innych wykonywanych na rzecz Urzędu, a także sposobów zabezpieczenia tych informacji, zarówno w trakcie wykonywania zadań, jak i po ich zakończeniu.

Mam świadomość, że celem Polityki Bezpieczeństwa Informacji jest zapewnienie odpowiedniego poziomu bezpieczeństwa informacji przetwarzanych w ***Urzędzie Gminy w Odrzywole***, a naruszenia związane z bezpieczeństwem informacji mogą skutkować odpowiedzialnością karną lub dyscyplinarną na zasadach i w trybie przewidzianym w przepisach prawa, w tym w ustawie z dnia z dnia 26 czerwca 1974 r. - Kodeks pracy.

.....

Data i podpis czytelny

Załącznik nr 2

Instrukcja Zarządzania Systemami Informatycznymi

w Urzędzie Gminy w Odrzywole

1. Cel, zakres i użytkownicy

Realizując postanowienia:

Art. 24 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), wprowadza się „Instrukcję Zarządzania Systemami Informatycznymi w Urzędzie Gminy w Odrzywole" (zwaną dalej Polityką Instrukcja).

Niniejsza instrukcja określa zasady eksploatacji i zarządzania systemami informatycznymi służącymi do przetwarzania danych.

Użytkownikami niniejszego dokumentu są wszyscy pracownicy Urzędu Gminy w Odrzywole jak również odnośne podmioty zewnętrzne.

2. Dokumenty referencyjne
   - Polityka Bezpieczeństwa Informacji w Urzędzie Gminy w Odrzywole
   - Polityka kluczy
   - Procedura nadawania uprawnień

3. Określenia i skróty użyte w Instrukcji Zarządzania Systemami Informatycznymi

Poufność – właściwość informacji zapewniająca jej dostęp wyłącznie dla osób uprawnionych;

Integralność – właściwość informacji zapewniająca możliwość dokonywania w niej zmian tylko przez uprawnione osoby lub procesy, w dozwolony sposób;

Dostępność – właściwość informacji zapewniająca możliwość dostępu do tej informacji przez uprawnione osoby w każdym czasie, gdy dana informacja jest potrzebna;

Bezpieczeństwo informacji – zapewnienie poufności, integralności oraz dostępności informacji;

Polityka - rozumie się przez to Politykę Bezpieczeństwa Danych Osobowych w Urzędzie Gminy w Odrzywole;

Instrukcja - rozumie się przez to Instrukcję Zarządzania Systemami Informatycznymi w Urzędzie Gminy w Odrzywole;

Administrator Danych/AD – Urząd Gminy w Odrzywole reprezentowany przez Wójt Gminy Odrzywół, decydującego o celach i środkach przetwarzania danych osobowych;

Inspektor Ochrony Danych - osoba powołana przez AD w Urzędzie, wpisana do prowadzonego przez organ nadzorczy rejestru inspektorów ochrony danych, zwaną dalej „IOD";

Administrator Systemów Informatycznych (ASI) – osobę wyznaczoną przez AD, odpowiedzialny za infrastrukturę techniczną systemów;

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

Dane osobowe (dane) - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

Zbiór danych - zestaw danych osobowych posiadający określoną strukturę, prowadzony w/g określonych kryteriów oraz celów;

Usuwanie danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

Zgoda osoby, której dane dotyczą - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści;

Baza danych osobowych - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe;

Przetwarzanie danych - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

System informatyczny (system) - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

Administrator systemu - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień;

Użytkownik – pracownik Urzędu Gminy Odrzywół posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych;

Zabezpieczenie systemu informatycznego - należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;

Nośnik komputerowy (wymienny) - nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde, dysku flash, pendrive;

Hasło - ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;

Identyfikator - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie;

Urząd - rozumie się przez Urząd Gminy w Odrzywole

4. Bezpieczna eksploatacja sprzętu i oprogramowania

a. Sprzęt służący do przetwarzania zbioru danych osobowych składa się z: komputerów stacjonarnych klasy PC, notebooków oraz serwerów.
b. Sieć komputerowa służąca do przetwarzania danych osobowych posiada zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu komputerowego.
c. Główne węzły są podtrzymywane przez UPS zapewniający odpowiedni czas pracy systemu.
d. Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają licencje.
e. Administrator Systemu odpowiada za wyposażenie systemu informatycznego w mechanizmy uwierzytelniania użytkownika oraz za sprawowanie kontroli dostępu do danych osobowych jedynie osób upoważnionych.
f. Ekrany monitorów są wyposażone w wygaszacze zabezpieczone hasłem, które aktywują się automatycznie po upływie określonego czasu od ostatniego użycia komputera.
g. Ekrany monitorów, są ustawione w taki sposób, żeby w miarę możliwości uniemożliwić odczyt wyświetlanych informacji osobom nieupoważnionym.

5. Procedura nadawania uprawnień do systemu informatycznego

a. Podstawą do nadania uprawnień do przetwarzania danych osobowych w systemie informatycznym Urzędu jest upoważnienie do przetwarzania danych osobowych;
b. Upoważnienie wydawane jest przez Administratora Danych Osobowych;

c. Upoważnienie wydawane jest na wniosek przełożonego danego pracownika, a w przypadku osoby niebędącej pracownikiem Urzędu na wniosek pracownika koordynującego działania osoby, dla której upoważnienie jest wydawane;
d. Za nadanie uprawnień w systemie informatycznym odpowiada ASI. Uprawnienia nie mogą być nadane w przypadku, jeżeli dana osoba nie posiada upoważnienia do przetwarzania danych osobowych w wymaganym zakresie;
e. Użytkownikom w systemie informatycznym, przyznawane są indywidualne identyfikatory z hasłem inicjującym;
f. Kierownik komórki organizacyjnej składa do Administratora Systemu Informatycznego wniosek o przyznanie uprawnień, określony w *Procedurze nadawania uprawnień;*
g. Administrator Systemu rejestruje użytkownika w systemie oraz nadaje mu identyfikator;
h. Identyfikator użytkownika wraz z jego imieniem i nazwiskiem, Administrator Systemu wpisuje do Ewidencji osób upoważnionych do przetwarzania danych osobowych;
i. Inspektor ochrony danych prowadzi, w imieniu i z upoważnienia Administratora Danych Osobowych, ewidencję osób upoważnionych do przetwarzania danych osobowych. Każda zmiana w zakresie informacji zawartych w ewidencji podlega niezwłocznemu odnotowaniu przez IOD;
j. W przypadku zmiany przez użytkownika uprawnień do obsługi danego systemu, kierownik komórki organizacyjnej występuje z wnioskiem do Administratora Systemu o modyfikację uprawnień, wzór wniosku określa *Procedura nadawania uprawnień;*
k. W przypadku utraty przez użytkownika uprawnień do obsługi danego systemu informatycznego (np. rozwiązanie stosunku pracy, nieobsługiwanie systemu z powodu zmiany stanowiska pracy) kierownik komórki organizacyjnej występuje do Administratora Systemu z wnioskiem o anulowanie upoważnienia do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych;
l. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.

6. Weryfikacja uprawnień

1. Administrator Bezpieczeństwa Informacji co najmniej raz do roku prowadzi przegląd uprawnień użytkowników w systemach informatycznych.
2. Weryfikacja dokonywana jest na podstawie zestawień przygotowanych przez Administratora Systemu Informatycznego.
3. IOD w porozumieniu z przełożonymi użytkowników ustala prawidłowość uprawnień.
4. Weryfikacja uprawnień kończy się sporządzeniem raportu.

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

- Pierwsze hasło dla użytkownika systemu przydziela Administrator Systemu Informatycznego przy wprowadzaniu identyfikatora użytkownika do systemu;
- Użytkownik systemu podczas pierwszego logowania niezwłocznie ustala swoje, znane tylko jemu hasło;

- Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło dostępu.
- Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów itp.;
- Właścicielem hasła jest użytkownik systemu;
- Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom;
- Osobą odpowiedzialną za przydział haseł i częstotliwość ich zmiany, a także w zakresie rejestrowania i wyrejestrowania użytkowników jest Administrator Systemu Informatycznego;
- Hasło powinno różnić się od poprzednio używanych;
- W przypadku zapomnienia hasła użytkownik powinien zwrócić się do ASI o wygenerowanie nowego hasła;
- W przypadku podejrzenia zapoznania się z hasłem przez osobę nieuprawnioną, użytkownik jest zobowiązany do natychmiastowej zmiany hasła oraz powiadomienia ASI o zaistniałym fakcie;
- Za wszelkie operacje w systemie wykonywane z wykorzystaniem indywidualnego identyfikatora oraz hasła odpowiada właściciel identyfikatora.

Hasła administratora systemu.

- Administrator Systemu zobowiązany jest zmienić swoje hasło nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne;
- Hasła administratora wymienione powinny być spisanie oraz umieszczenie w zamkniętych kopertach, odrębnych dla każdego z systemów, w miejscu uniemożliwiającym dostęp do nich osób nieupoważnionych, chroniącym przed utratą lub zniszczeniem oraz gwarantującym ich odczytanie upoważnionemu użytkownikowi, a także kierownikowi komórki organizacyjnej w przypadkach nadzwyczajnych;
- Zarejestrowane hasła administratora, oprócz treści hasła winny posiadać adnotację o dacie ich wprowadzenia do systemu;
- W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

Uwierzytelnianie na poziomie systemu operacyjnego.

- Hasło na poziomie dostępu do systemu operacyjnego może składać się z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne;
- Za systematyczną, terminową zmianę hasła odpowiada użytkownik;
- Zmiana hasła do systemu operacyjnego następuje nie rzadziej, niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.

Uwierzytelnianie na poziomie dostępu do aplikacji.

- Hasło na poziomie dostępu do programu może składać się z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne;
- Za systematyczną, terminową zmianę hasła odpowiada użytkownik;
- Zmiana hasła następuje nie rzadziej, niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.

8. Procedura rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników systemu.

- Rozpoczynając pracę na komputerze użytkownik loguje się do systemu informatycznego;
- Dostęp do danych osobowych możliwy jest jedynie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia użytkownika;
- Jeśli system to umożliwia, po przekroczeniu 3 prób logowania system blokuje dostęp do systemu informatycznego na poziomie danego użytkownika;
- Administrator Systemu ustala przyczyny zablokowania systemu oraz w zależności od zaistniałej sytuacji podejmuje odpowiednie działania. O zaistniałym incydencie powiadamia Inspektora ochrony danych;
- Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest:
  - wylogować się z systemu informatycznego lub,
  - wywołać blokowany hasłem wygaszacz ekranu.
- Kontynuacja pracy po powrocie powinna być możliwa jedynie po ponownym uwierzytelnieniu (w przypadku wylogowania) lub odblokowaniu systemu komputerowego przez wprowadzenie hasła;
- Zakończenie pracy w systemie informatycznym polega na przeprowadzeniu operacji wylogowania z systemu oraz wyłączenia systemu komputerowego;
- Opuszczając pomieszczenie, w którym przetwarzane są dane osobowe, pracownik zobowiązany jest do zamknięcia pomieszczenia na klucz, jeżeli w pomieszczeniu tym nie przebywa inna osoba upoważniona do przebywania w tym pomieszczeniu. Zabronione jest pozostawianie bez nadzoru w pomieszczeniach, w których przetwarzane są dane osobowe, osób nieupoważnionych;
- Kończąc pracę w systemie informatycznym pracownik wyloguje się ze wszystkich aplikacji, z których korzystał, wyłącza stację roboczą i zabezpiecza nośniki danych. W przypadku, gdy pracownik jest ostatnią osobą opuszczającą pomieszczenie, sprawdza zamknięcie okien, zamyka na klucz drzwi do pomieszczenia oraz zdaje klucz.

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

- Zbiory danych osobowych przetwarzanych w systemie informatycznym, są dodatkowo zabezpieczane poprzez przechowywanie ich w postaci kopii zapasowych w sposób określony ustawą i rozporządzeniem;
- Za tworzenie kopii zapasowych systemu informatycznego odpowiedzialny jest Administrator Systemu Informatycznego;
- Kopie są wykonywane przy pomocy wbudowanych funkcji systemu;
- Kopie zapasowe:
  - sporządza się raz dziennie po zakończeniu dziennej obsługi systemu przez użytkowników systemu;
  - przechowuje się przez minimum 1 miesiąc;
  - przechowuje się w zamkniętych szafach, przy czym kopie te nie mogą być przechowywane w pomieszczeniu, w którym eksploatowany jest system komputerowy, z którego one pochodzą.
- Kopie zapasowe wykonuje się na nośniku zewnętrznym w cyklu miesięcznym. Kopie te są wykonywane na nośnikach optycznych jednokrotnego użytku;
- Kopie zapasowe są odpowiednio oznakowane;
- Utworzone kopie zapasowe podlegają weryfikacji ze względu na sprawdzenie możliwości odczytu danych;

- ASI odpowiada za prowadzenie ewidencji wykonania kopii zapasowych;
- IOD określa czas przechowywania poszczególnych kopii zapasowych ze względu na cel przetwarzania zapisanych danych;
- ASI odpowiedzialny jest za realizację działań odtworzeniowych w przypadku konieczności podjęcia takich działań w związku z awarią systemu informatycznego Urzędu. Po odtworzeniu systemu informatycznego ASI odpowiedzialny jest za przeprowadzenie testów poprawności działania systemu przed jego oddaniem do użytkowania;
- ASI przeprowadza weryfikację możliwości odtworzenia danych zapisanych na kopiach zapasowych. Weryfikacja taka powinna być przeprowadzana nie rzadziej niż raz na pół roku.

10. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji, kopii zapasowych i wydruków.

- Wydruki oraz elektroniczne nośniki informacji z danymi osobowymi pochodzącymi z systemu informatycznego, przechowuje się w zamykanych szafach i pomieszczeniach, do których dostęp mogą mieć wyłącznie uprawnieni użytkownicy systemu;
- Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, nośnik niszczy się trwale w sposób uniemożliwiający odczytanie danych;
- Decyzję o likwidacji danych osobowych przetwarzanych bezpośrednio w systemie informatycznym oraz danych osobowych przechowywanych w kopiach zapasowych podejmuje osoba nadzorująca pracę na określonym zbiorze danych osobowych w porozumieniu z IOD;
- Dla udokumentowania likwidacji danych, o których mowa powyżej, likwidujący sporządza protokół zawierający niezbędne informacje o usuniętych danych;
- Fakt niszczenia kopii zapasowych, Administrator Systemu odnotowuje w rejestrze kopii zapasowych;
- Przechowywane w systemie informatycznym, na kopiach zapasowych lub w postaci wydruków dane osobowe, które przestały być użyteczne, podlegają usunięciu lub zniszczeniu w sposób trwały uniemożliwiający ich odczytanie;
- Kopie zapasowe przechowuje się przez okres określony dla poszczególnych danych osobowych zgodnie z ustalonymi przepisami;
- Dane osobowe w systemie informatycznym przechowywane są przez czas wymagany do spełnienia celu, dla którego są one przetwarzane. Po jego upływie dane podlegają skasowaniu lub anonimizacji;
- Przenośne elektroniczne nośniki informacji zawierające dane osobowe są przechowywane przez pracowników w sposób minimalizujący ryzyko ich uszkodzenia lub zniszczenia, w szczególności w zamykanych szafach i meblach biurowych. IOD wyznacza pomieszczenia, w których mogą być przechowywane takie nośniki;
- Dane przechowywane są na nośnikach jedynie w przypadkach, gdy jest to konieczne, przez czas niezbędny do spełnienia celu, w jakim zostały one na nośniku zapisane. Po ustaniu czasu przechowywania zawartość nośnika podlega skasowaniu przy użyciu narzędzi zaakceptowanych do użycia w Urzędzie, a w przypadku nośników optycznych stosuje się niszczenie w niszczarkach umożliwiających niszczenie tego typu nośników;
- Kopie zapasowe zbioru danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w kasie pancernej;

- Zbędne wydruki zawierające dane osobowe, należy niszczyć w niszczarce;
- Dopuszcza się powierzenie niszczenia nośników danych wyspecjalizowanym podmiotom zewnętrznym, pod warunkiem:

❖ Zawarcia umowy określającej obowiązki podmiotu przetwarzającego, o których mowa w art. 28 Rozporządzenia;
❖ Zagwarantowania poufności danych przez usługodawcę;
❖ Umożliwienia prowadzenia nadzoru nad procesem niszczenia nośników przez IOD lub upoważnionego przez niego pracownika Urzędu;
❖ Udokumentowania faktu zniszczenia nośników protokołem.

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

W celu zabezpieczenia systemu informatycznego przed działaniem niebezpiecznego oprogramowania zabrania się:
❖ Uruchamiania jakiegokolwiek oprogramowania, które nie zostało zatwierdzone do użytku w Urzędzie;
❖ Samowolnego korzystania z nośników przenośnych;
❖ Otwierania poczty elektronicznej, której tytuł nie sugeruje związku z pełnionymi obowiązkami służbowymi; w przypadkach wątpliwych należy skonsultować się z ASI.

W przypadku zauważenia objawów mogących wskazywać na obecność niebezpiecznego oprogramowania użytkownik jest zobowiązany powiadomić ASI. Do objawów powyższych można zaliczyć:
❖ Istotne spowolnienie działania systemu informatycznego;
❖ Nietypowe działanie aplikacji;
❖ Nietypowe komunikaty;
❖ Utratę danych lub modyfikację danych.

System informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:
❖ Oprogramowanie antywirusowe;
❖ Zaporę sieciową;
❖ Aktualizację oprogramowania systemowego;
❖ Konfigurację oprogramowania minimalizującą ryzyko naruszenia bezpieczeństwa.

ASI jest odpowiedzialny za nadzór nad działaniem powyższych zabezpieczeń, a w szczególności za:
❖ Weryfikację aktualności sygnatur systemu antywirusowego i podejmowanie ewentualnych działań korekcyjnych;
❖ Weryfikację logów systemu antywirusowego i podejmowanie działań korekcyjnych;
❖ Przegląd logów zapory sieciowej oraz podejmowanie działań mających na celu zablokowanie ataków sieciowych;
❖ Weryfikację poprawności aktualizacji oprogramowania systemowego.

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

- Przegląd i konserwacja sprzętu informatycznego realizowany jest przez upoważnionych pracowników Urzędu oraz przez podmioty zewnętrzne.
- Prace serwisowe wykonywane na terenie Urzędu przez podmioty zewnętrzne podlegają bezpośredniemu nadzorowi ASI;
- Przeglądy i konserwacja systemu informatycznego powinny być wykonywane w terminach określonym przez producentów systemu oraz zgodnie z harmonogramem Administratora Systemu;
- Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada Administrator Systemu;
- Nieprawidłowości w działaniach systemu informatycznego oraz oprogramowania powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane.

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

- Sprzęt przekazywany jest bez nośników zawierających dane osobowe, zaś fakt usunięcia nośników danych lub stwierdzenia braku nośników danych jest potwierdzany protokołem;
- Przekazanie sprzętu potwierdzane jest protokołem, pozwalającym na jednoznaczne wskazanie osoby przekazującej i osoby odbierającej sprzęt;
- Protokoły, o których mowa lub ich kopie przechowywane są przez IOD.

Wszelkie prace serwisowe wykonywane przez podmioty zewnętrzne wymagają sporządzenia protokołu serwisowego, zawierającego, co najmniej poniższe informacje:

- Wskazanie osoby przeprowadzającej prace serwisowe oraz podmiotu, którego osoba ta jest pracownikiem;
- Wskazanie osoby nadzorującej przebieg prac serwisowych (dotyczy sytuacji, gdy prace realizowane są w siedzibie Urzędu);
- Przedmiot prac serwisowych (w szczególności identyfikator sprzętu w przypadku prac serwisowych dotyczących sprzętu);
- Zakres prac serwisowych i ich wynik;
- Czas przeprowadzania prac serwisowych.

13. Postanowienia końcowe.

Stwierdza się ważność niniejszego dokumentu na dzień 19.01.2021r.
ASI jest odpowiedzialny za weryfikację oraz w razie konieczności aktualizację niniejszego dokumentu.