ZARZĄDZENIE NR 30/2024
WÓJTA GMINY ŻELAZKÓW
z dnia 14 marca 2024 r.

w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji
w Urzędzie Gminy Żelazków

Na podstawie § 20 ust. 1 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

W Urzędzie Gminy Żelazków ustanawia się System Zarządzania Bezpieczeństwem Informacji (dalej SZBI), który stanowi załącznik nr 1 zarządzenia. Celem wprowadzenia SZBI jest zapewnienie poufności, dostępności oraz integralności informacji przetwarzanych we wszystkich komórkach organizacyjnych.

§ 2

Wprowadza się niżej wymienione dokumenty:
- Polityka Bezpieczeństwa Informacji , stanowiąca załącznik nr 2
- Polityka Bezpieczeństwa Teleinformatycznego, stanowiąca załącznik nr 3;
- Polityka Prywatności Strony Internetowej, stanowiąca załącznik nr 4, niniejszego zarządzenia.

Pozostałe dokumenty SZBI na podstawie wcześniejszych Zarządzeń Wójta Gminy w zakresie:
- Ochrona Informacji Niejawnych (Zarządzenie nr 113 /2019 z dnia 7 października 2019 r);
- Polityka Ochrony Danych Osobowych (Zarządzenie nr 81/2019 z dnia 2 lipca 2019 r);
- Plan Ciągłości Działania (Zarządzenie 117/2023 z dnia 5 października 2023 r)

pozostają w mocy.

§ 3

Wprowadza się w Polityce Bezpieczeństwa Teleinformatycznego Formularz dostępu do systemu teleinformatycznego stanowiący załącznik do Upoważnienia do przetwarzania danych osobowych. W związku z powyższym tracą ważność z dniem 14 marca 2024 roku dotychczasowe Upoważnienia do przetwarzania danych osobowych wydane w latach 2018 – 2023. Dla pracowników Urzędu Gminy Żelazków wydane zostaną nowe Upoważnienia.

§ 4

W Urzędzie Gminy Żelazków powołuje się Zespół ds. Systemu Zarządzenia Bezpieczeństwem Informacji (dalej Zespół ds. SZBI), który odpowiedzialny jest za monitorowanie funkcjonowania mechanizmów bezpieczeństwa informacji, właściwe postępowanie z incydentami i naruszeniami, dokonywanie corocznych przeglądów Systemu Zarządzania Bezpieczeństwem Informacji, oraz opracowywanie zmian we wprowadzanych dokumentach, procedurach i infrastrukturze technicznej.

§ 6

W skład Zespołu ds. Systemu Zarządzania Bezpieczeństwem Informacji wchodzą:

a. Sekretarz Gminy Żelazków,
b. Administrator Systemów Informatycznych,
c. Inspektor Ochrony Danych,
d. Pełnomocnik Ochrony Informacji Niejawnych,
e. Inspektor ds. obrony cywilnej, obronności, wojskowości, pożarnictwa i stanów nadzwyczajnych.

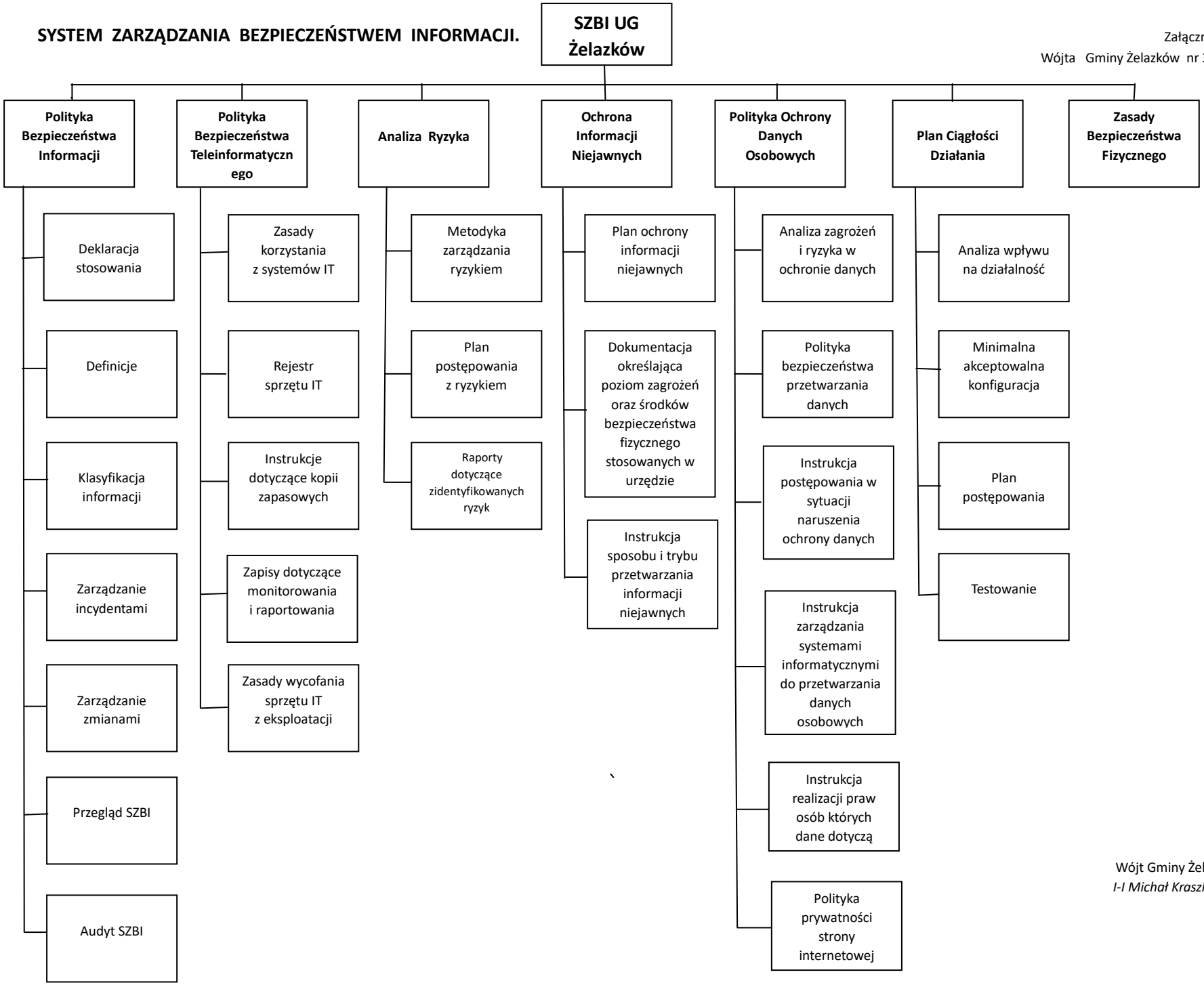
§ 7

Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Żelazków
I-I Michał Kraszkiewicz

SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI.

Załącznik nr 1 do Zarządzenia
Wójta Gminy Żelazków nr 30 z dnia 14.03. 2024 r



Wójt Gminy Żelazków
I-I Michał Kraszkiewicz

Załącznik nr 2 do Zarządzenia
Wójta Gminy Żelazków nr 30/2024
z dnia 14.03. 2024 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

W URZĘDZIE GMINY ŻELAZKÓW

Żelazków 14.03.2024 rok

Spis treści

1. 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 Gminy Żelazków, dlatego powinna być chroniona na każdym szczeblu organizacji. Urząd Gminy Żelazków 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 Gminy Żelazków 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. Polityka Bezpieczeństwa Informacji została wdrożona i jest stale doskonalona w celu:

1) zapewnienia poufności, integralności i dostępności danych;

2) zapewnienia identyfikowalności czynności i zasobów podczas przetwarzania danych;

3) zapewnienia niezawodności działań;

4) podejmowania wysiłków prowadzących do poprawy poziomu bezpieczeństwa zasobów informacyjnych w Urzędzie. Polityka Bezpieczeństwa Informacji jest dokumentem nadrzędnym w stosunku do wszystkich dokumentów systemowych z zakresu zarządzania bezpieczeństwem informacji.

2. Terminologia

Ilekroć w Polityce Bezpieczeństwa Informacji jest mowa o:

– „Polityce” - należy przez to rozumieć Politykę Bezpieczeństwa Informacji w Urzędzie Gminy Żelazków ;

– „Gminie” – należy przez to rozumieć Gminę Żelazków;

– „Wójcie” – należy przez to rozumieć Wójta Gminy Żelazków;

– „Urzędzie” - należy przez to rozumieć Urząd Gminy Żelazków ;

– „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 Żelazków ;

– „Użytkowniku” - należy przez to rozumieć osobę korzystającą z zasobów teleinformatycznych Urzędu.

3. Podstawy prawne:

Polityka Bezpieczeństwa Informacji oraz pozostałe dokumenty SZBI dotyczące zarządzania bezpieczeństwem informacji w Urzędzie spełniają wymagania prawne i regulacyjne, zawarte w:

1) ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2023, poz.57);

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. 2022 poz. 902);

4) ustawie z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. 2021, poz. 1641 ze zm.);

5) ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. 2021, poz. 1797);

6) ustawie z dnia 5 sierpnia 2010 r o ochronie informacji niejawnych (t. j. Dz. U. z 2020 r poz. 756);

7) ustawie z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. 2023, poz. 82 ze zm.);

8) ustawie z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (Dz.U. 2022, poz. 2240);

9) ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2022, poz. 1863 ze zm.)

10) ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. 2021, poz. 1797);

11) ustawie z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz.U.2023, poz.285);

12) 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);

13) rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28 sierpnia 2014, str.73);

14) 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);

15) normie PN-ISO/IEC 27001:2017-06.

4. Definicje:

1)Informacja – wszelkie zapisy w formie papierowej, w systemach komputerowych oraz na innych nośnikach przetwarzane w systemach tradycyjnych, elektronicznych i komunikacyjnych będących własnością Miasta, funkcjonujących w Urzędzie lub tylko administrowanych przez Urząd;

2) Bezpieczeństwo informacji – zachowanie poufności, integralności i dostępności informacji w wyniku stosowania procesu zarządzania ryzykiem;

3) Aktyw/zasób – wszystko to, co ma wartość dla organizacji w zakresie informacji (zarówno informacje, jak i środki techniczne oraz organizacyjne do ich przetwarzania);

4) Poufność – zapewnienie dostępu do informacji tylko osobom upoważnionym;

5) Integralność – zapewnienie że dokument nie zostanie zmieniony w sposób nieuprawniony;

6) Dostępność – zapewnienie, że osoby upoważnione będą miały dostęp do informacji zawsze gdy jest to im niezbędne;

7) Ryzyko – prawdopodobieństwo wystąpienia zagrożenia, które wykorzystując podatność(ci) aktywu, może doprowadzić do jego uszkodzenia lub zniszczenia;

8) Szacowanie ryzyka – całościowy proces analizy i oceny ryzyka;

9) Postępowanie z ryzykiem – proces wyboru i wdrażania środków modyfikujących ryzyko;

10) Zarządzanie ryzykiem – proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych przy zachowaniu akceptowalnego poziomu kosztów;

11) Zdarzenie związane z bezpieczeństwem informacji – określony stan systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem;

12) Incydent bezpieczeństwa informacji – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji;

13) 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;

14) 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 Gmina Żelazków;

15) Inspektor Ochrony Danych (IOD) – wyznaczony przez Administratora pracownik Urzędu, do zadań którego należy zapewnienie przestrzegania przepisów o ochronie danych osobowych.

5. Zakres Systemu Bezpieczeństwa Informacji

SZBI w Urzędzie stanowi część Systemu Zarządzania, odnoszącą się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa

informacji. SZBI został opracowany, wdrożony i jest utrzymywany w oparciu o normę PN-ISO/IEC 27001:2017-06. Zakres SZBI dotyczy obsługi administracyjnej ludności i podmiotów gospodarczych oraz zarządzania przestrzenią administracyjną. Zakresy określone przez dokument Polityki Bezpieczeństwa Informacji mają zastosowanie do całego systemu informacyjnego Urzędu Gminy Żelazków, w szczególności do:

1)wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie;

2) informacji będących własnością Urzędu Gminy Żelazków;

3) informacji będących własnością klientów Urzędu Gminy Żelazków, uzyskanych na podstawie zawartych umów;

4) wszystkich lokalizacji Urzędu Gminy Żelazków, czyli budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;

5) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

6. Deklaracja Kierownictwa w zakresie bezpieczeństwa informacji w Urzędzie Gminy Żelazków.

Wójt Gminy Żelazków , stojąc na stanowisku, że informacja jest newralgicznym zasobem Urzędu, wdrożył w ramach Zintegrowanego Systemu Zarządzania w Urzędzie Gminy Żelazków system zarządzania bezpieczeństwem informacji i zobowiązuje się do podejmowania wszelkich działań prowadzących do kompleksowego zabezpieczenia informacji oraz zapewnienia środków niezbędnych do realizacji niniejszej Polityki.

7. Organizacja bezpieczeństwa informacji w Urzędzie Gminy Żelazków

Odpowiedzialność za realizację ochrony informacji w Urzędzie ponoszą wszyscy

pracownicy Urzędu – proporcjonalnie do wykonywanych obowiązków i posiadanych uprawnień. Zakres uprawnień i odpowiedzialności związany z zarządzaniem bezpieczeństwem informacji określony został w procedurach i instrukcji „Bezpieczeństwa Informacji w Urzędzie Gminy Żelazków".

Zarządzeniem nr 105/2019 z dnia 29 sierpnia 2019 r. Wójt Gminy Żelazków wyznaczył Inspektora Ochrony Danych.

Każdy pracownik Urzędu jest zapoznawany z zasadami bezpieczeństwa oraz z aktualnymi procedurami ochrony informacji w swojej komórce organizacyjnej oraz w Urzędzie Gminy Żelazków zawartymi w Instrukcji podstawowych zasad bezpieczeństwa dla pracowników Urzędu. 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. Właściciel aktywu odpowiada za bieżące nadzorowanie oraz zarządzanie aktywem.

8. Dokumentacja systemu zarządzania bezpieczeństwem informacji

Dokumentacja SZBI składa się z następujących głównych elementów. Są nimi:

- Polityka Bezpieczeństwa Informacji ;
- Polityka Bezpieczeństwa Teleinformatycznego;
- Analiza Ryzyka;
- Ochrona Informacji Niejawnych;
- Polityka Ochrony Danych Osobowych;

- Plan Ciągłości Działania;

- Zasady Bezpieczeństwa Fizycznego.

9. Zasady współpracy ze stronami zainteresowanymi

W Urzędzie Gminy Żelazków wdrożono standard bezpieczeństwa fizycznego w odniesieniu do klientów i podmiotów wykonujących prace zlecone na terenie Urzędu. Ponadto instrukcja ogólna w zakresie wymagań dla umów przygotowywanych w Urzędzie Gminy Żelazków określa klauzule poufności różnego stopnia szczegółowości, niezbędne przy zawieraniu umów. Celem takiego postępowania jest zapewnienie bezpieczeństwa informacji przed dostępem osób niepowołanych, uszkodzeniem lub innymi zakłóceniami w obiektach oraz systemach Urzędu Gminy Żelazków. Wyodrębnione zostały również obszary niedostępne dla klientów i osób trzecich z uwagi na przetwarzane informacje bądź funkcje techniczne. Pomieszczenia komórek organizacyjnych przetwarzających dane osobowe wyposażono w fizyczne bariery (lady) umożliwiające obsługę klientów przy jednoczesnym odseparowaniu ich od zasobów informacyjnych. Ponadto znaczna część klientów jest obsługiwana na stanowisku obsługi klienta, co sprawia, że nie mają oni uzasadnionej potrzeby poruszania się po innych obszarach Urzędu Gminy Żelazków. Ciągi komunikacyjny wejścia do budynku jest pod stałą obserwacją systemu monitoringu.

10. Polityka kontroli dostępu do informacji

Dostęp do informacji przechowywanych i przetwarzanych w Urzędzie jest poddany kontroli wynikającej z obowiązujących przepisów prawa powszechnego oraz dodatkowych wymagań bezpieczeństwa, przyjętych w normie PN-ISO/IEC 27001:2017-06. Kontrola polega na:

1) wydzieleniu obszarów przeznaczonych do przechowywania oraz przetwarzania poszczególnych zbiorów danych i zapewnieniu odpowiednich barier fizycznych przeciwdziałających nieuprawnionemu dostępowi;

2) zarządzaniu uprawnieniami poszczególnych użytkowników w sposób zapewniający dostęp wyłącznie do danych wymaganych do wykonywania obowiązków służbowych, jeśli dane te podlegają ochronie z jakiejkolwiek przyczyny;

3) stosowaniu bezpiecznych systemów przetwarzania informacji;

4) nadzorowaniu działalności stron trzecich, mogących wpłynąć na bezpieczeństwo informacji;

5) bieżącym informowaniu pracowników o wszelkich zmianach w zakresie regulacji dotyczących przechowywania, przetwarzania i udostępniania informacji.

Adekwatność i skuteczność stosowanych w Urzędzie środków kontroli dostępu do informacji podlega bieżącej weryfikacji w ramach audytów wewnętrznych, zmian dokumentacji i metod postępowania wynikających z ewolucji uregulowań prawnych oraz systemów przetwarzania danych a także reagowania na zagrożenia ujawnione przez inne strony.

11. Klasyfikacja informacji

Klasyfikacja została wprowadzona w celu uporządkowania w Urzędzie postępowania z różnymi rodzajami informacji, które są głównym zasobem naszej organizacji.

W szczególny sposób potraktowano informację, której ujawnienie może narazić pracodawcę na szkodę.

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. Zdefiniowano trzy poziomy dla każdego z powyższych wskaźników po to, aby możliwe było powiązanie danej grupy informacji z określonym poziomem zdefiniowanego wskaźnika w skali 1-3.

Struktura klasyfikacji informacji w Urzędzie Gminy Żelazków opiera się na założeniu istnienia trzech poziomów postrzegania informacji:

1) informacje jawne – informacje publicznie dostępne,

2) informacje wewnętrzne – informacje, których przetwarzanie i udostępnianie podlega restrykcjom z uwagi na szczególne znaczenie dla pracodawcy (właściciela informacji):

a) informacje wewnętrzne dostępne – informacje dostępne dla wszystkich pracowników Urzędu Gminy Żelazków,

b) informacje wewnętrzne wrażliwe – informacje dostępne dla grupy pracowników upoważnionych z uwagi na realizowane zadania regulaminowe,

c) informacje stanowiące tajemnicę pracodawcy – informacje, których przetwarzanie i udostępnianie może narazić pracodawcę na szkodę;

3) informacje ustawowo chronione – tajemnice określone w odrębnych przepisach.

12. Zarządzanie aktywami i ryzykami

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. Ważnym elementem zarządzania aktywami i bezpieczeństwem informacji jest przeprowadzanie okresowej analizy ryzyka i opracowywanie planów postępowania z ryzykiem. Analiza wyników stanowi podstawę podejmowania wszelkich działań w zakresie doskonalenia ochrony zasobów Urzędu. Na podstawie wyników analizy ryzyka opracowywane są plany postępowania z ryzykiem dla aktywów o ryzykach większych niż ustalony poziom ryzyka

akceptowalnego. Ryzyka są przeglądane na przeglądach kierownictwa oraz po zmianach mających wpływ na system bezpieczeństwa informacji.

13. Autoryzacja nowych urządzeń

Każde nowe lub zmienione urządzenie służące do przetwarzania informacji lub mogące w jakikolwiek inny sposób wpływać na bezpieczeństwo informacji jest weryfikowane na zgodność z wymaganiami systemu bezpieczeństwa informacji i zaakceptowane przez uprawnioną osobę. Urządzenia służące do przetwarzania informacji nie będące własnością Urzędu mogą być używane (po sprawdzeniu sprzętu pod względem kryteriów bezpieczeństwa) wyłącznie za zgodą osoby upoważnionej.

14. Zarządzanie systemami i sieciami

Urząd dba o przestrzeganie zasad związanych z utrzymywaniem i użytkowaniem systemów informatycznych i sieci. Celem takiego postępowania jest zapewnienie poufności, integralności i dostępności przetwarzanej przez nie informacji własnych. Skuteczna realizacja postawionego celu możliwa jest dzięki:

1) kompetencjom i świadomości pracowników oraz podpisanym umowom ze specjalistycznymi firmami administrującymi zasobami informatycznymi;

2) opracowanym zasadom konserwacji urządzeń w celu zapewnienia ich ciągłej pracy;

3) kontrolowaniu wprowadzania wszelkich zmian do infrastruktury technicznej,

4) prowadzeniu prac rozwojowych i testowych na oddzielnych urządzeniach lub środowiskach w celu zapewnienia bezpieczeństwa systemów produkcyjnych;

5) nadzorowaniu usług dostarczanych przez strony trzecie, w szczególności odbieraniu ich i akceptowaniu w sposób świadomy uwzględniający jego wpływ na istniejący system bezpieczeństwa;

6) wdrożeniu zabezpieczeń chroniących przed oprogramowaniem złośliwym i mobilnym;

7) systematycznemu tworzeniu i testowaniu kopii bezpieczeństwa;

8) przestrzeganiu opracowanych zasad postępowania z nośnikami;

9) bieżącemu monitorowaniu aktywów informacyjnych.

Urząd monitoruje możliwość wystąpienia incydentów bezpieczeństwa i posiada mechanizmy reagowania w przypadkach ich wystąpienia.

15. Bezpieczeństwo zasobów ludzkich

Urząd zapewnia kompetentną kadrę pracowniczą do realizacji wyznaczonych zadań. Celem takiego postępowania jest ograniczenie ryzyka błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania zasobów. Realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z weryfikacją kandydatów do pracy podczas naboru, zasadom zatrudniania pracowników oraz ustalonej procedurze rozwiązywania umów o pracę.

16. Bezpieczeństwo fizyczne, sprzętu i infrastruktury technicznej

W Urzędzie określono następujące kierunkowe standardy:

– standard bezpieczeństwa fizycznego;

– standard bezpieczeństwa sprzętu i okablowania;

– standard konfiguracji i eksploatacji sieci.

Z uwagi na to, że standardy zawierają informacje, których ujawnienie nieuprawnionym stronom trzecim mogłoby w istotnym stopniu obniżyć poziom bezpieczeństwa informacji, są udostępnione tylko pracownikom Urzędu wykonującym zadania określone w standardach.

Przedmiot poszczególnych standardów:

1) standard bezpieczeństwa fizycznego: parametr bezpieczeństwa fizycznego, kontrola fizycznych wejść, zabezpieczenie biur, pokoi i urządzeń, ochrona przed zagrożeniami zewnętrznymi i środowiskowymi, praca w obszarach zabezpieczonych, obszary ogólnie dostępne, obszary dostaw i załadunku;

2) standard bezpieczeństwa sprzętu i okablowania: rozmieszczenie i ochrona sprzętu, urządzenia wspomagające, bezpieczeństwo okablowania, utrzymanie sprzętu, bezpieczeństwo sprzętu znajdującego się poza terenem organizacji, bezpieczne usuwanie sprzętu, wynoszenie majątku;

3) standard konfiguracji i eksploatacji sieci: środki kontroli przeciwko kodowi złośliwemu i mobilnemu, środki kontroli sieci, bezpieczeństwo usług sieciowych, polityki i procedury dotyczące wymiany informacji, przesyłanie wiadomości drogą elektroniczną, korzystanie z usług sieciowych, identyfikacja sprzętu w sieciach, ochrona portu służącego do zdalnego diagnozowania i konfiguracji, segregacja w sieciach, kontrola połączeń sieci, routing, nadzorowanie słabości technicznych.

17. Zarządzanie 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. Zasady reagowania na zdarzenia mogące prowadzić do zaburzenia procesów przetwarzania informacji są przedmiotem „Planu ciągłości działania w Urzędzie Gminy Żelazków ” oraz instrukcji i planów awaryjnych. Plany awaryjne podlegają systematycznemu testowaniu.

18. Zarządzanie zmianami

Urząd, mając na uwadze konieczność szybkiego dostosowywania się do wymagań stron zainteresowanych, ciągłe zmiany przepisów prawnych oraz dążenie do wzrostu efektywności i wydajności pracy, zapewnia metody postępowania dla skutecznej i terminowej obsługi zmian w infrastrukturze teleinformatycznej przy utrzymaniu pożądanego poziomu bezpieczeństwa przetwarzanych danych i ograniczeniu ryzyka

negatywnego wpływu zmiany na obsługę teleinformatyczną organizacji.

Proces zarządzania zmianą w Urzędzie Gminy Żelazków przebiega w następujących etapach:

1) ustalenie celu zmiany;

2) rozważenie wielkości i ważności zmiany dla organizacji;

3) określenie momentów krytycznych we wdrożeniu zmiany;

4) zainicjowanie zmiany, przeprowadzenie testów, wdrożenie w systemie produkcyjnym;

5) aktywne włączenie pracowników Urzędu w proces zmiany;

6) monitorowanie i raportowanie kolejnych kroków wdrożenia zmiany

19. Polityka wymiany informacji pomiędzy Urzędem Gminy i podległymi jednostkami organizacyjnymi .

Urząd oraz gminne jednostki organizacyjne posiadają własne rozłączne zasoby informacyjne, którymi administrują. Zasoby przechowywane są na rozdzielonych logicznie własnych serwerach. Wzajemna wymiana informacji następuje na ogólnych zasadach z wykorzystaniem służbowej poczty elektronicznej.

20. Zgodność z wymaganiami prawnymi i regulacyjnymi

Urząd dba o zapewnienie zgodności postępowania z przepisami obowiązującego prawa, przyjętych uwarunkowań umownych i normatywnych oraz wypracowanych własnych standardów. Celem takiego postępowania jest unikanie naruszania jakichkolwiek przepisów prawnych, zobowiązań wynikających z ustaw, zarządzeń lub umów oraz wymagań bezpieczeństwa. Realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z identyfikacją wymagań prawnych w zakresie bezpieczeństwa informacji. Prowadzone są audyty wewnętrzne i zewnętrzne funkcjonowania systemu.

21. Deklaracja ochrony własności intelektualnej

W Urzędzie Gminy Żelazków zostały wdrożone w ramach SZBI mechanizmy zapobiegające naruszeniom przepisów prawa powszechnego związanych z ochroną własności intelektualnej. Przede wszystkim zabezpieczono stacje robocze przed możliwością instalacji oprogramowania z naruszeniem właściwej licencji. Sieć podlega ciągłemu monitorowaniu, a dostęp do stron oraz usług internetowych, co do których zachodzi podejrzenie naruszania własności intelektualnej lub ryzyko infekcji systemu złośliwym oprogramowaniem, może zostać zablokowany. W ramach usług domeny wprowadzono filtrowanie plików użytkownika, blokując te z formatów, które nie będąc z założenia wynikającego z funkcjonalności przydatnymi w pracy zawodowej, mogłyby zarazem być nośnikami treści naruszających prawa autorskie i pokrewne. Prowadzona jest bieżąca ewidencja licencji oprogramowania, co zapewnia, że pracownicy upoważnieni do instalacji oprogramowania działają w granicach praw nabytych przez Gminę Żelazków. Nadzorowana jest także własność intelektualna powierzona lub przekazana przez osoby trzecie, zarówno klientów, jak i kontrahentów.

22. Postanowienia końcowe

Kierownictwo Urzędu zapoznaje pracowników Urzędu, stażystów i praktykantów z dokumentem Polityki Bezpieczeństwa Informacji oraz Instrukcją podstawowych zasad bezpieczeństwa dla pracowników Urzędu Gminy Żelazków . 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.

Kierownictwo Urzędu zapoznaje pracowników Urzędu, stażystów i praktykantów z

dokumentem Polityki Bezpieczeństwa Informacji oraz Instrukcją podstawowych zasad bezpieczeństwa dla pracowników Urzędu Gminy Żelazków . 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.

Wójt Gminy Żelazków
I-I Michał Kraszkiewicz

Załącznik nr 3 do Zarządzenia
Wójta Gminy Żelazków nr 30/2024
z dnia 14.03.2024 r.

POLITYKA BEZPIECZEŃSTWA TELEINFORMATYCZNEGO URZĘDU GMINY ŻELAZKÓW

Żelazków 14.03.2024 rok

Spis treści

1. Definicje pojęć

1) Atrybuty bezpieczeństwa informacji – poufność, dostępność, integralność, autentyczność, rozliczalność, niezawodność, niezaprzeczalność.
2) Autentyczność – właściwość gwarantująca, że pochodzenie lub zawartość informacji są takie, jak deklarowane.
3) Bezpieczeństwo informacji – stan zapewniający zachowanie atrybutów bezpieczeństwa informacji.
4) Dostępność – właściwość gwarantująca, że określone informacje mogą być wykorzystywane w określonym czasie.
5) Incydent – pojedyncze zdarzenie lub seria zdarzeń, związanych z bezpieczeństwem informacji, naruszające ich atrybuty.
6) Integralność – właściwość wykluczająca modyfikację informacji w nieautoryzowany sposób.
7) Niezaprzeczalność – brak możliwości zanegowania uczestnictwa w całości lub w części wymiany informacji przez jeden z podmiotów uczestniczących w tej wymianie.
8) Niezawodność – właściwość oznaczająca spójne, zamierzone zachowanie i skutki.
9) Polityka – Polityka Bezpieczeństwa Teleinformatycznego.
10) Poufność – właściwość gwarantująca, że tylko osoby upoważnione, mają dostęp do informacji.
11) Rozliczalność – właściwość systemu pozwalająca przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie.
12) System – system teleinformatyczny Urzędu Gminy Żelazków.

2. Regulacje prawne dla bezpieczeństwa teleinformatycznego

2.1 Zewnętrzne

1) Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2021 r. poz. 2070);

- Rozporządzenie 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 (t. j. Dz.U. 2017 poz. 2247);

2) Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (tj. Dz.U. z 2021 r., poz. 2234);

- Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP (t .j. Dz. U. z 2016 r. poz. 1101);

3) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781);

- 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 iw sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 2016.119.1);

4) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. z 2020 r. poz. 1369 ze zm.);

- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 2016.194.1);

5) Ustawa z dnia 29 września 1994 r. o rachunkowości (t.j. Dz. U. 2021 r. poz. 217 ze zm.);

6) Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz. U. z 2021 r. poz. 305 ze zm.);

- Komunikat Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych (Dz. Urz. MF z 2009 r. Nr 15 poz. 84).

2.2 Wewnętrzne

1) Polityka bezpieczeństwa – schemat Systemu Zarzadzania Bezpieczeństwem Informacji w Urzędzie;
2) Polityka ochrony danych osobowych w Urzędzie;
3) Ochrona informacji niejawnych w Urzędzie;
4) Analiza Ryzyka;
5) Plan ciągłości działania;
6) Zasady bezpieczeństwo fizycznego.

3. Cel i zakres stosowania

1) Celem Polityki jest zdefiniowanie zasad stosowania zabezpieczeń na poziomie organizacyjnym oraz technicznym umożliwiających redukcję ryzyka związanego z bezpieczeństwem informacji przetwarzanych w UG Żelazków.
2) Niniejszy dokument uwzględnia wymagania określone zarówno w zewnętrznych, jak i wewnętrznych regulacjach prawnych dotyczących bezpieczeństwa teleinformatycznego.

4. Bezpieczeństwo fizyczne

4.1 Ochrona fizyczna pomieszczeń szczególnych.

1) Szczególna funkcja pomieszczenia typu serwerownia oraz węzły teleinformatyczne determinuje zapewnienie im zwiększonych środków bezpieczeństwa.
2) Informatyk prowadzi rejestr wejść do serwerowni.
3) Pomieszczenia te powinny być objęte kontrolą dostępu zapewniającą możliwość dostępu wyłącznie osobom upoważnionym.
4) Dostęp do wskazanych pomieszczeń realizowany jest wyłącznie w obecności informatyka.

4.2 Prace serwisowe

1) W przypadku prac serwisowych, w których uczestniczą osoby trzecie, prace nadzorowane są przez Informatyka.
2) Informatyk nadzorujący wykonywane prace przez osoby trzecie odpowiada za działania wykraczające poza zleconą pracę.
3) Sprzęt wydawany do serwisu, świadczonego przez firmę zewnętrzną, należy pozbawić nośników pamięci masowej zawierających informacje podlegające ochronie (dane osobowe, informacje księgowe, informacje niejawne, itp.)

4) W przypadku braku możliwości spełnienia ww. punktu niezbędne jest podpisanie umowy powierzenia danych osobowych pomiędzy stronami.

5. Zarządzanie uprawnieniami dostępu.

1) Domyślnym poziomem uprawnień do system jest brak dostępu.
2) Uprawnienia do systemów przetwarzających dane osobowe nadawane są zgodnie z Polityką ochrony danych w UG Żelazków.
3) Uprawnienia nadawane są pracownikom na czas realizacji powierzonych zadań.
4) Każdy pracownik musi posiadać indywidualne i unikalne konto, jednoznacznie identyfikujące go w systemie.
5) Identyfikator systemowy, który został wcześniej przyznany, nie może być nadany innemu użytkownikowi.
6) Administrator systemu odpowiada za poprawne utworzenie konta użytkownika i nadanie uprawnień w systemie.
7) Dostęp do systemów przetwarzających dane osobowe mogą posiadać wyłącznie osoby, które zostały przeszkolone w zakresie ochrony danych osobowych.
8) Uprawnienia dostępu powinny być nadane wyłącznie na poziomie niezbędnym do pracy.
9) Zmiana uprawnień dla pracownika zatwierdzana jest każdorazowo przez bezpośredniego przełożonego, który odpowiada za przypisanie właściwych uprawnień przyznanych podległym pracownikom w ramach zasobów informacyjnych wykorzystywanych w kierowanej komórce organizacyjnej.
10) Uprawnienia mogą być odebrane lub zmienione na wniosek przełożonego, który zobowiązany jest każdorazowo do określenia niezbędnego zakresu uprawnień, do wykonywania pracy na danym stanowisku.
11) Wnioskowanie o nadanie lub zmianę uprawnień do systemów służących do przetwarzania danych osobowych odbywa się na zasadach opisanych w Polityce ochrony danych osobowych.
12) W przypadku zmiany komórki organizacyjnej, poprzedni przełożony pracownika zobowiązany jest do wnioskowania o odebranie uprawnień do systemów i zasobów, do których dostęp powinni mieć wyłącznie pracownicy wewnątrz danej komórki organizacyjnej.
13) W przypadku ustania stosunku pracy lub zwolnienia z niego, dostęp do systemów jest blokowany.
14) W przypadku ustania zatrudnienia pracownika, w uzasadnionych przypadkach, przełożony może wyrazić zgodę na czasowe korzystanie z poczty służbowej po ustaniu zatrudnienia. W przypadku zaistnienia sytuacji wyjątkowej, bezpośredni przełożony dokonuje oceny zaistniałej sytuacji, na podstawie której podejmowana jest decyzja w sprawie odebrania lub ograniczenia uprawnień.
15) Wprowadza się Formularz dostępu do systemu teleinformatycznego dla pracownika stanowiący załącznik do Polityki bezpieczeństwa teleinformatycznego.

5.1 Dostęp administracyjny

1) Każdy system musi posiadać zdefiniowane role użytkowników i niezależne od nich konto administratora.
2) Uprawnienia administracyjne do systemów może posiadać wyłącznie ASI UG Żelazków.

3) Konto administratora powinno być wykorzystywane, wyłącznie, gdy istnieje wyraźna potrzeba skorzystania z tych uprawnień.

5.2 Przegląd uprawnień

1) Każdy system musi posiadać mechanizmy umożliwiające kontrolę dostępu do poszczególnych informacji.
2) Przełożony ma obowiązek weryfikacji uprawnień podległych mu pracowników przynajmniej raz na rok.
3) Administrator systemu w ramach przeprowadzanego przeglądu uprawnień porównuje dane dotyczące przyznanych rzeczywistych dostępów z danymi zawartymi w Formularzu dostępu do systemu teleinformatycznego.
4) Kontrola dostępu do systemów realizowana jest na zlecenie Wójta Gminy Żelazków.
5) Każdy przegląd uprawnień musi być udokumentowany protokołem.

5.3 Kontrola dostępu

1) Każdy system posiada wbudowane mechanizmy zabezpieczeń pozwalające na identyfikację użytkownika, kontrolę dostępu i zakresu uprawnień.
2) Każda operacja rozpoczęcia pracy, końca pracy, nieudanego logowania w systemie musi zostać odnotowana w dzienniku zdarzeń.

6. Zasady tworzenia haseł

1) Hasło konta użytkownika musi spełniać poniższe wymagania:
   a) nie może być krótsze niż 8 znaków,
   b) musi posiadać odpowiednią złożoność, składającą się z dużych oraz małych liter, cyfr oraz znaków specjalnych,
   c) nie może zawierać w ciągu znaków elementów bezpośrednio powiązanych z identyfikatorem w systemie bądź w jednoznaczny sposób powiązanych z użytkownikiem (imię, nazwisko, PESEL, itp.). Wyjątek stanowią hasła tymczasowe, przekazywane użytkownikowi,
   d) nie powinno zawierać ciągów słownikowych,
   e) musi być zmieniane nie rzadziej niż co 30 dni,
   f) tam, gdzie to możliwe powinny zostać wdrożone mechanizmy wymuszania zmiany hasła przez użytkownika,
   g) konieczne jest, aby różniło się od hasła zmienianego, tzn. jego części nie powinny zawierać się w nowym,
   h) zalecane jest wdrożenie konfiguracji umożliwiającej zapamiętywanie 5 ostatnich haseł,
2) Hasło konta z uprawnieniami administracyjnymi musi spełniać poniższe wymagania:
   a) nie może być krótsze niż 10 znaków,
   b) hasło przechowywane jest w karcie stanowiskowej,
   c) pozostałe wymagania jak dla haseł użytkowników.
3) Pod żadnym pozorem nie można udostępniać nikomu swoich haseł.
4) W razie podejrzenia ujawnienia danych uwierzytelniających należy bezzwłocznie zmienić hasło.
5) Należy bezzwłocznie, tuż po pierwszym logowaniu zmienić tymczasowe hasło dostępowe.
6) Należy stosować różne hasła do każdego systemu.
7) Zabrania się zapisywania haseł w łatwo dostępnych miejscach, a przede wszystkim tuż obok stanowiska pracy.

7. Praca zdalna

1) Zdalny dostęp do zasobów sieciowych może być nadawany wyłącznie do zasobów, do których użytkownik posiada uprawnienia w obrębie sieci wewnętrznej.
2) Zdalny dostęp odbywa się za pośrednictwem dedykowanego łącza VPN.

3) Połączenie i transmisja danych pomiędzy komputerem znajdującym się poza siedzibą UG Żelazków, a jej siecią musi odbywać się zgodnie ze standardami zapewniającymi bezpieczną transmisję danych.
4) Zabronione jest:
   a) podłączanie się do sieci bez posiadania aktywnego i aktualnego oprogramowania antywirusowego,
   b) udostępnianie połączenia nieuprawnionym osobom,
   c) udostępnianie poświadczeń do zdalnego logowania do sieci (loginu i hasła) osobom trzecim,
   d) korzystanie z połączenia przy użyciu ogólnodostępnych sieci bezprzewodowych,
   e) generowanie nadmiernego ruchu w sieci podczas zdalnego połączenia (np.: połączenia peer2peer, skanowanie sieci, itp.).

8. Zdarzenia związane z bezpieczeństwem teleinformatycznym

1) Pracownicy UG Żelazków, wykonawcy i użytkownicy reprezentujący stronę trzecią, korzystających z systemów informacyjnych i usług, mają możliwość zgłaszania zaobserwowanych naruszeń bezpieczeństwa lub podejrzewanych słabości bezpieczeństwa w systemach lub usługach przez utworzone do tego kanały (telefonicznie, mailowo lub bezpośrednio do Informatyka) w ramach systemu zarządzania zgłoszeniami.
2) Działania mające na celu zapobieganie, wykrywanie oraz usuwanie skutków incydentów oraz podatności mogących zagrażać bezpieczeństwu informacji przetwarzanych w systemach informatycznych realizowane są zgodnie z procedurą zarządzania incydentem teleinformatycznym.
3) W sytuacji, kiedy zdarzenie związane z naruszeniem bezpieczeństwa doprowadzi do awarii systemu należy postępować zgodnie z przyjętymi procedurami awaryjnymi.

9. Zarządzanie kopiami zapasowymi

1) Kopie zapasowe powinny być wykonywane w sposób umożliwiający przywrócenie dostępności i funkcjonalności systemów informatycznych. Częstotliwość wykonywania kopii zapasowych określana jest na 2 tygodnie.
2) Czas przechowywania kopii zapasowych musi być zgodny z wymaganiami wynikającymi z obowiązujących przepisów prawa, określających wymagany minimalny czas przechowywania danych.
3) Systemy wspierające zarządzanie kopiami zapasowymi muszą zapewniać odnotowywanie w logach historii działań związanych z zarządzaniem kopiami zapasowymi, wraz ze wskazaniem ich rezultatów. W przypadku nieudanego wykonania kopii zapasowej system powinien wysyłać informację do administratora systemu informatycznego.
4) Kopie zapasowe konfiguracji urządzeń sieci informatycznej oraz urządzeń zabezpieczającej styk sieci informatycznej uczelni z sieciami zewnętrznymi wykonywane są każdorazowo po zmianie konfiguracji urządzeń. Konieczne jest przechowywanie co najmniej bieżącej i poprzedniej konfiguracji urządzenia sieciowego.
5) Kopie zapasowe powinny podlegać okresowej weryfikacji prowadzonej przez administratora systemu informatycznego, w celu sprawdzenia ich przydatności do odtworzenia funkcjonalności systemu informatycznego w przypadku jego awarii. Testy odtworzenia powinny być wykonywane na wydzielonych do tego celu środowiskach testowych, a ich wyniki dokumentowane.
6) Kopie zapasowe systemów powinny być fizycznie zlokalizowane w innym środowisku niż produkcyjne.

10. Bezpieczeństwo komputerów

1) ASI odpowiada za określenie standardu bezpieczeństwa stanowisk komputerowych.
2) Standard bezpieczeństwa stanowisk komputerowych obejmuje co najmniej:
   a) brak uprawnień administratora lokalnego przez użytkownika (z wyjątkiem uzasadnionych przypadków),
   b) posiadanie oprogramowania antywirusowego (z wyjątkiem uzasadnionych przypadków),
   e) posiadanie zainstalowanego i użytkowanie oprogramowania, zgodnie z jego licencją,
   f) ograniczenie użytkownikom dostępu do narzędzi systemowych umożliwiających ingerencję w konfigurację systemu bądź aplikacji, które mogłoby mieć wpływ na obniżenie poziomu bezpieczeństwa.
3) Użytkownik odpowiada za zapewnienie bezpieczeństwa fizycznego przekazanego mu sprzętu komputerowego.
4) Zakazane jest uruchamianie nośników niewiadomego pochodzenia, pochodzących z nieznanych źródeł.
5) Zabrania się uruchamiania załączników poczty elektronicznej oraz linków do stron internetowych wzbudzających podejrzenie lub pochodzących od nieznanego nadawcy.
6) Przekazany sprzęt komputerowy, będący własnością UG Żelazków może być wykorzystywany wyłącznie w celach służbowych.
7) Praca na komputerze odbywa się z wykorzystaniem indywidualnego konta założonego przez pracownika obsługi informatycznej.
8) Użytkownik nie może samodzielnie instalować ani usuwać oprogramowania na przydzielonym mu komputerze.
9) Użytkownik nie może dokonywać żadnych zmian w konfiguracji sprzętowej komputera.
10) Zakazane jest usuwanie oznaczeń licencyjnych oraz ewidencyjnych znajdujących się na obudowie udostępnionych urządzeń.
11) Zabrania się przechowywania na dyskach lokalnych plików naruszających prawo.
12) Zabrania się udostępniania komputerów osobom nieuprawnionym.
13) W przypadku konieczności opuszczenia miejsca pracy i pozostawienia komputera bez nadzoru, użytkownik zobowiązany jest zabezpieczyć dostęp do uruchomionych aplikacji i systemów co najmniej na poziomie dostępu do systemu operacyjnego, przez zablokowanie komputera.
14) Użytkownicy komputerów zobowiązani są do ustawienia monitorów w sposób uniemożliwiający podejrzenie informacji przez osoby nieuprawnione.
16) W przypadku zaistnienia uzasadnionych okoliczności związanych ze zwolnieniem dyscyplinarnym pracownika, długotrwałą nieobecnością lub innymi zdarzeniami losowymi, przełożony może uzyskać dostęp do danych służbowych użytkownika oraz prowadzonej korespondencji.

11. Bezpieczeństwo komputerów przenośnych

1) Dopuszczalne jest wykorzystywanie służbowego sprzętu przenośnego poza siedzibą UG Żelazków oraz pracy zdalnej, zgodnie z określonymi zasadami.
2) Użytkownik służbowego komputera przenośnego, należącego do UG Żelazków, jest zobowiązany do użytkowania go w sposób minimalizujący ryzyko kradzieży, uszkodzenia bądź zniszczenia, w tym również podczas transportu.
3) Komputer nie powinien być pozostawiany bez nadzoru w miejscach, w których istnieje ryzyko przejęcia go przez osoby trzecie.

4) Ze względu na bezpieczeństwo systemów informatycznych Uczelni zabrania się pozostawiania bez nadzoru komputera z nawiązanym zdalnym połączeniem (VPN) oraz umożliwiania dostępu do takiego komputera osobom nieupoważnionym.
5) Podczas korzystania z komputera przenośnego w miejscach publicznych użytkownik powinien zwrócić szczególną uwagę na uniemożliwienie podejrzenia informacji wyświetlanych na ekranie komputera, zarówno bezpośrednio przez osobę nieupoważnioną, jak i z wykorzystaniem systemu dozoru wizyjnego.
6) Stanowisko pracy poza biurem powinno być zorganizowane w sposób uniemożliwiający dostęp do informacji służbowych nieupoważnionym osobom trzecim oraz zapewniać fizyczną ochronę sprzętu i nośników danych przed utratą, zniszczeniem oraz nieuprawnionym dostępem osób trzecich.
7) Zapewnienie właściwej konfiguracji służbowych komputerów przenośnych odbywa się na ogólnie przyjętych zasadach, dotyczących stanowisk komputerowych.

12. Wykorzystywanie komputerów prywatnych do celów służbowych

1) Dopuszczane jest wykorzystywanie do pracy służbowej sprzętu prywatnego, który nie stanowi własności UG Żelazków.
2) Właściciel komputera odpowiedzialny jest za:
   a) posiadanie zainstalowanego oprogramowania zapewniającego odpowiednią ochronę przed złośliwym oprogramowaniem,
   b) prawidłowe działanie komputera,
   c) legalne źródło pochodzenia zainstalowanego oprogramowania,
   d) zapewnienie należytej ochrony powierzonych danych służbowych, przetwarzanych na prywatnym komputerze,
   e) działania osób trzecich korzystających z komputera,
   f) usunięcie wszystkich służbowych danych z komputera po zakończeniu realizacji zadań na rzecz Uczelni.

13. Bezpieczne korzystanie z poczty elektronicznej

1) W celu zwiększenia ochrony informacji przesyłanych drogą pocztową należy upewnić się, że podany został właściwy adresat wiadomości.
2) Załączniki z informacjami podlegającymi ochronie (w tym zawierające dane szczególne oraz PESEL, datę urodzenia, miejsce zamieszkania/zameldowania) należy wysyłać, o ile jest to możliwe, w formie zaszyfrowanej, przesyłając hasło do pliku innym kanałem informacyjnym (np. MS Teams). W uzasadnionych przypadkach można odstąpić od przesyłania danych w postaci zaszyfrowanej.
3) Niedozwolone jest wykorzystywanie służbowej skrzynki pocztowej do celów prywatnych oraz wykorzystywanie prywatnej skrzynki pocztowej do celów służbowych.
4) Niedozwolone jest wykorzystywanie prywatnej poczty do celów służbowych.
5) Nie należy otwierać odnośników do stron internetowych oraz załączonych plików w wiadomościach niewiadomego pochodzenia, a w przypadku wątpliwości należy skontaktować się z pracownikami obsługi informatycznej.
6) W przypadku, kiedy istnieje podejrzenie lub doszło do nieuprawnionego przejęcia konta pocztowego, należy bezzwłocznie skontaktować się z ASI.

14. Zarządzanie licencjami

1) Użytkownicy powinni wykorzystywać wyłącznie licencjonowane oprogramowanie, na które UG Żelazków posiada licencję, które zostało zainstalowane przez pracownika obsługi informatycznej na służbowym komputerze
2) Niedopuszczalne jest korzystanie z licencjonowanego oprogramowania bez posiadania licencji.

15. Monitorowanie systemów i sieci

1) Wszystkie systemy i sieci informatyczne podlegają monitorowaniu pod względem bezpieczeństwa i wykrywania potencjalnych zagrożeń.
2) Wykorzystanie zasobów jest monitorowane, co pozwala na określenie pojemności systemów, w celu zapewnienia odpowiedniej wydajności.
3) Działania administratora i użytkowników systemów są rejestrowane.
4) Zegary urządzeń sieciowych, serwery, stacje robocze oraz pozostałe urządzenia końcowe są synchronizowane z uzgodnionym, dokładnym źródłem czasu.
5) W celu umożliwienia sprawnego monitorowania systemów i sieci niezbędne jest prowadzenie spisu systemów i sieci wchodzących w skład infrastruktury UG Żelazków.
6) Spis powinien być prowadzony na bieżąco, natomiast inwentaryzacja powinna być przeprowadzana okresowo nie rzadziej niż raz na rok.
7) Monitorowanie systemów i sieci odbywa się na bieżąco przez ASI.
8) Administrator systemów zapewnia dostęp do logów i dzienników zdarzeń.
9) Bezwarunkowemu zapisowi w systemie logów podlegają zdarzenia generowane przez administratora systemu, od momentu zalogowania do chwili wylogowania w danym systemie lub na tyle ile dany system pozwala.
10) Zdarzenia związane z bezpieczeństwem informacji przetwarzanych w systemach informatycznych powinny być rejestrowane i przechowywane nie krócej niż 12 miesięcy.
11) Każde zaobserwowane zdarzenie zagrażające bezpieczeństwu systemu powinno zostać poddane analizie.
12) W przypadku zakwalifikowania zdarzenia jako incydent, niezbędne jest postępowanie jak w przypadku incydentu naruszenia bezpieczeństwa.

16. Ciągłość działania systemów informatycznych

1) Zarządzanie ciągłością działania systemów i sieci obejmuje analizę zagrożeń, ich prawdopodobieństwo wystąpienia i wpływ na funkcjonowanie systemów i sieci.
2) Wdrożenie zarządzania ciągłością działania systemów i sieci powinno zagwarantować zwiększenie świadomości na możliwość wystąpienia sytuacji kryzysowych.
3) Zasady testowania i aktualizacji procedur awaryjnych dla systemów i sieci opisane są w Planie ciągłości działania.

17. Ochrona danych osobowych

1) Dostęp do systemów przetwarzających dane osobowe uzyskują wyłącznie użytkownicy posiadający upoważnienie do ich przetwarzania i odbywa się on na zasadach opisanych w Polityce Ochrony Danych Osobowych.
2) Uprawnienia do systemów nadawane są zgodnie z obowiązującą Polityką ochrony danych osobowych.
3) Przed przekazaniem lub udostępnieniem urządzeń i nośników zawierających dane osobowe osobie nieupoważnionej do ich przetwarzania należy skutecznie zabezpieczyć lub usunąć te dane, w sposób uniemożliwiający ich odzyskanie.

18. Usuwanie danych osobowych z systemów informatycznych

1) Usuwanie danych osobowych z systemów informatycznych świadczonych przez UG Żelazków odbywa się na poniżej opisanych zasadach:

a) W przypadku wpłynięcia wniosku o usunięcie danych przetwarzanych w systemie informatycznym, kierownik komórki merytorycznie odpowiedzialnej za ich przetwarzanie, dokonuje oceny wniosku pod kątem zasadności oraz zgodności przedmiotu wniosku z przepisami przyjętymi w UG Żelazków.
b) Kierownik jednostki merytorycznie odpowiedzialnej za przetwarzane dane osobowe wnioskuje do Centrum Informatycznego o przeprowadzenie usunięcia danych osobowych wskazując jednocześnie termin, w którym dane osobowe wnioskującego powinny zostać usunięte.
c) Administrator Systemu Informatycznego (ASI) dokonuje usunięcia lub w przypadku, kiedy z przyczyn technicznych jest to niemożliwe, podejmuje działania mające na celu anonimizację danych osobowych, polegającą na pozbawieniu danych osobowych cech pozwalających na identyfikację osoby, której dotyczą.

19. Audyty i kontrole

Audyty i kontrole są prowadzone na polecenie Wójta przez uprawnione jednostki organizacyjne.

20. Procedura zarządzania incydentami teleinformatycznymi

Procedura zarządzania incydentami teleinformatycznymi opisana jest w Planie ciągłości działania na wypadek awarii systemu informatycznego, braku energii elektrycznej oraz zaistnienia innych zdarzeń losowych w UG Żelazków wprowadzona na podstawie Zarządzenia Wójta Gminy Żelazków nr 117/2023 z dnia 5.10.2023 rok. Ponadto wyznaczono ASI UG Żelazków do nawiązania i utrzymywania kontaktów z podmiotem krajowego systemu cyberbezpieczeństwa CSIRT NASK w zakresie zadań publicznych zależnych od systemów informatycznych, użytkowanych przez Urząd Gminy Żelazków na podstawie zarządzenia Wójta Gminy Żelazków nr 4/2022 z dnia10 stycznia 2022 roku.

Formularz dostępu do systemu teleinformatycznego

1. Dostęp do stanowiska komputerowego…….

Nazwa komputera	Nr pokoju	Login do domeny

2. Dostęp do programu

Program	TAK (login)	NIE
Płace		
Budżet		
Podatki		
KSGZOB		
Egzekucje		
Środki Trwałe		
JGU		
Auta		
Kasa		
GOMIG – Odpady		
Moduł wymiarowy – Odpady		
PB_EWID		
CEIDG		
EMUiA		
Płatnik		
Besti@		
Portal UZP		
BANK Spółdzielczy Ziemi Kal.		
SIO		
Portal PZU		
EGB		
Edap – legislator		
Arcus		
ŹRÓDŁO		
Pfron		
Platforma Kuratorium Oświaty		
Shrimp(pomoc de minimis)		

Program	TAK (login)	NIE
Platforma wyborcza		
PARPA - sprawozdania		

3. Czy dla pracownika należy wyrobić podpis elektroniczny

TAK	NIE

4. Czy pracownik posiada indywidualny adres e-mail

5. Czy pracownik posiada katalog na Import – Export

……...
Podpis ASI

…….
Podpis Administratora lub osoby
upoważnionej do wystawiania upoważnień

……
Podpis osoby upoważnionej

Żelazków, dnia ….....

Wójt Gminy Żelazków
I-I Michał Kraszkiewicz

Załącznik nr 4 do Zarządzenia
Wójta Gminy Żelazków nr 30 /2024
z dnia 14.03. 2024 r

Polityka Prywatności Strony Internetowej Urzędu Gminy Żelazków

1. Niniejsza Polityka Prywatności określa zasady gromadzenia, przetwarzania i wykorzystywania danych osobowych oraz ich ochrony przez Stronę Internetową przekazanych przez Użytkowników w związku z korzystaniem przez nich z Formularza Kontaktowego na stronie.

2. Administratorem danych osobowych jest: **Urząd Gminy w Żelazkowie, 62-817 Żelazków, Żelazków 137, 62 769 10 08, email: ug@zelazkow.pl , NIP: 9680371259, REGON: 000552030.**

3. Wyznaczono Inspektora Ochrony Danych, z którym kontaktować można się w sprawach dotyczących przetwarzania danych osobowych poprzez e-mail: **obronacywilna@zelazkow.pl** lub pisemnie na adres naszej siedziby, wskazany w pkt. 1.

4. W trosce o bezpieczeństwo powierzonych nam danych opracowaliśmy wewnętrzne procedury i zalecenia, które mają zapobiec udostępnieniu danych osobom nieupoważnionym. Kontrolujemy ich wykonywanie i stale sprawdzamy ich zgodność z odpowiednimi aktami prawnymi - ustawą o ochronie danych osobowych, ustawą o świadczeniu usług drogą elektroniczną, a także wszelkiego rodzaju aktach wykonawczych i aktach prawa W trosce o bezpieczeństwo powierzonych nam danych opracowaliśmy wewnętrzne procedury i zalecenia wspólnotowego.

5. Dane Osobowe przetwarzane są na podstawie zgody wyrażanej przez Użytkownika oraz w przypadkach, w których przepisy prawa upoważniają Administratora do przetwarzania danych osobowych na podstawie przepisów prawa lub w celu realizacji zawartej pomiędzy stronami zamówienia (art. 6ust. 1 lit. b RODO).

6. Administrator zapewnia przetwarzanie danych osobowych zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE)2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) („RODO") oraz godnie z obowiązującymi przepisami prawa powszechnie obowiązującego w Polsce w zakresie danych osobowych, oraz ustawą z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2016 r. poz. 1030 tj.)

7. Serwis Strony Internetowej Urzędu Gminy Żelazków, realizuje funkcje pozyskiwania informacji o użytkownikach i ich zachowaniach w następujący sposób:

   1) poprzez dobrowolnie wprowadzone w formularzach informacje;
   2) poprzez gromadzenie plików "cookies" której zasady przedstawione są poniżej:

Polityka plików „Cookies"

1. W trakcie odwiedzin witryny zapisywane są i przechowywane tzw. pliki "cookies". Są to małe pliki tekstowe wysyłane z serwerów odwiedzanych stron internetowych oraz aplikacji i przechowywane przez przeglądarkę internetową i inne rozwiązania technologiczne na urządzeniu użytkownika. Pliki te identyfikują internautę przy ponownych odwiedzinach lub

w ramach jednej wizyty, umożliwiając mu między innymi zalogowanie się do serwisu czy dodanie produktów do koszyka. Pozwalają również zbierać anonimowe statystyki, które informują, w jaki sposób użytkownik korzysta z serwisu, co z kolei pomaga administratorom usprawniać serwis i jego funkcje.

2. Do prawidłowego działania serwisu, tworzone są i wykorzystywane pliki sesyjne oraz pliki stałe. Pliki sesyjne są plikami tymczasowymi, przechowywanymi na urządzeniu użytkownika do czasu wylogowania się ze strony internetowej lub zamknięcia przeglądarki internetowej. Pliki stałe pozostają na urządzeniu na określony czas lub bez okresu ważności, w zależności od ustawień administratora witryny. Plik stały może być usunięty wcześniej z przeglądarki internetowej przez użytkownika.

3. Korzystając z serwisu, użytkownik może otrzymać pliki "cookies" współpracujących podmiotów trzecich. Są to pliki wykorzystywane przez usługi interaktywne portali społecznościowych oraz systemy analityczne gromadzące anonimowe dane o popularności serwisu.

4. Użytkownik posiada możliwość skonfigurowania przeglądarki internetowej w taki sposób, aby całkowicie lub częściowo wyłączyć przechowywanie plików "cookies", jednakże efektem tego może być utrata możliwości korzystania z niektórych funkcjonalności serwisu.

7. Serwis Strony Internetowej Urzędu Gminy Żelazków zbiera informacje dobrowolnie podane przez użytkownika.

8. Dane podane w formularzu są przetwarzane w celu wynikającym z funkcji Formularza Kontaktowego np. w celu dokonania procesu obsługi kontaktu informacyjnego.

9. Dane osobowe pozostawione w serwisie nie zostaną sprzedane ani udostępnioneosobom trzecim, zgodnie z przepisami Ustawy o ochronie danych osobowych.

10. Do danych zawartych w formularzu przysługuje wgląd osobie fizycznej, która je tam umieściła. Osoba ta ma również praw do modyfikacji i zaprzestania przetwarzania swoich danych w dowolnym momencie.

11. Zastrzegamy sobie prawo do zmiany w polityce ochrony prywatności serwisu, na które może wpłynąć rozwój technologii internetowej, ewentualne zmiany prawa w zakresie ochrony danych osobowych oraz rozwój naszego serwisu internetowego. O wszelkich zmianach będziemy informować w sposób widoczny i zrozumiały.

W razie wątpliwości co któregokolwiek z zapisów niniejszej polityki prywatności jesteśmy do dyspozycji - nasze dane znaleźć można w zakładce - KONTAKT.

Wójt Gminy Żelazków
I-I Michał Kraszkiewicz