BURMISTRZ
Bystrzycy Kłodzkiej

Zarządzenie Nr 0050.199.2021

Burmistrza Bystrzycy Kłodzkiej z dnia 25 czerwca 2021 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka

Na podstawie art. 31 oraz art.33 ust 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2020, poz. 713), działając w oparciu o przepisy:

Ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U. 2019 poz.1781t.j.); 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. 2016 z roku, poz. 113 ze zm.);

Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. UE L 119 z 4 maja 2016 r., Polskie Wydanie Specjalne 2016 t.59), zarządzam:

§ 1

Wprowadzenie do użytku służbowego *„**Politykę Bezpieczeństwa Urzędu Miasta i Gminy Bystrzyca Kłodzka**”* w brzmieniu stanowiącym załącznik nr 1 do niniejszego zarządzenia. oraz *„**Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka**”* w brzmieniu stanowiącym załącznik nr 2 do niniejszego zarządzenia.

§ 2

Wzór oświadczenia pracowników o zapoznaniu się z ww. dokumentami stanowi załącznik nr 4 do Polityki Bezpieczeństwa. Oświadczenia dołącza się do akt osobowych pracowników.

§ 3

Wykonanie zarządzenia powierzam Inspektorowi Danych Osobowych i Administratorowi Systemu Informatycznego.

§ 4

Wdrożenie systemu zarządzania bezpieczeństwem systemów informatycznych, o którym mowa w § 20 KRI 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 powierzam Administratorowi Systemu Informatycznego.

§ 5

Traci moc Zarządzenie Nr 0050.145.2018 Burmistrza Bystrzycy Kłodzkiej z dnia 23 maja 2018 r. w sprawie wprowadzenia *„**Polityki Bezpieczeństwa Przetwarzania Danych Osobowych**”* *i* *„**Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych osobowych w Urzędzie Miasta i Gminy w Bystrzycy Kłodzkiej**”* oraz Zarządzenie Nr 0050.146.2018 Burmistrza Bystrzycy Kłodzkiej z dnia 23 maja 2018r. w sprawie *„**analizy zagrożeń i ryzyka przy przetwarzaniu danych osobowych w Urzędzie Miasta i Gminy w Bystrzycy Kłodzkiej**”*.

§ 6

Zarządzenie wchodzi w życie z dniem 1 lipca 2021 r.

Burmistrz
Bystrzycy Kłodzkiej
Renata Surma

Załącznik nr 1 do Zarządzenia Nr 0050.199.2021 Burmistrza Bystrzycy Kłodzkiej z dnia 25 czerwca 2021 r w sprawie wprowadzenia Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka

POLITYKA BEZPIECZEŃSTWA URZĘDU MIASTA i GMINY BYSTRZYCA KŁODZKA

Spis treści

ROZDZIAŁ I - POSTANOWIENIA OGÓLNE

§ 1

Podstawy prawne:

1. Ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U. 2019 poz.1781t.j.);
2. 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. 2016 z roku, poz. 113 ze zm.);
3. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. UE L 119 z 4 maja 2016 r., Polskie Wydanie Specjalne 2016 t.59).

§ 2

Celem Polityki Bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka dalej nazywaną Polityką Bezpieczeństwa (PB), jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe, a przede wszystkim zapewnienie ochrony przetwarzanych danych osobowych przed wszelkiego rodzaju zagrożeniami, tak zewnętrznymi jak i wewnętrznymi.

§ 3

Słownik pojęć i skrótów stosowanych w niniejszej Polityce Bezpieczeństwa:

1. **Bezpieczeństwo Informacji** - zachowanie poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności;
2. **Urząd** - Urząd Miasta i Gminy Bystrzyca Kłodzka;
3. **Administrator Danych Osobowych** - Burmistrz Bystrzycy Kłodzkiej, zwany dalej Administratorem lub **ADO**;
4. **Inspektor Ochrony Danych**, zwany dalej **IOD**;
5. **Administrator Systemu Informatycznego**, zwany dalej **ASI** - osoba wyznaczona przez Administratora, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach oraz odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń system w informatycznych, w których przetwarzane są dane osobowe;
6. **Pracownik** - każda osoba zatrudniona w Urzędzie Miasta i Gminy Bystrzyca Kłodzka na podstawie: stosunku pracy (umowa o pracę, powołanie), umowy cywilnoprawnej, stażu absolwenckiego, praktyki zawodowej, a także pracownicy podmiotów

świadczących usługi na jej rzecz w związku z realizacją celów i zadań (prace doraźne o charakterze serwisowym lub innym);

7. **Osoba upoważniona lub użytkownik systemu, zwany dalej użytkownikiem** - osoba posiadająca upoważnienie wydane przez Administratora lub osobę wyznaczoną przez niego i dopuszczona, w zakresie w nim wskazanym, jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej.
8. **Przełożony użytkownika, zwany dalej przełożonym** - kierownik wydziału lub osoba kierująca wydziałem lub referatem w Urzędzie Miasta i Gminy Bystrzyca Kłodzka, a w przypadku stanowisk samodzielnych - Burmistrz Bystrzycy Kłodzkiej;
9. **Osoba trzecia** - to każda osoba nieupoważniona i przez to nieuprawniona do dostępu do danych osobowych zbiorów będących w posiadaniu Administratora. Osobą trzecią jest również osoba posiadająca upoważnienie wydane przez Administratora podejmująca czynności w zakresie przekraczającym ramy jego upoważnienia;
10. **Baza danych osobowych** - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisywane dane osobowe;
11. **Dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;
12. **Działanie korygujące** - działanie przeprowadzane w celu wyeliminowania przyczyny wykrytej niezgodności/incydentu lub innej niepożądanej sytuacji;
13. **Działanie zapobiegawcze** - działanie, które należy przedsięwziąć, aby wyeliminować przyczyny potencjalnej niezgodności/incydentu lub innej potencjalnej sytuacji niepożądanej;
14. **Przetwarzanie danych** - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, udostępnianie i ich usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
15. **System informatyczny**, zwany dalej systemem to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
16. **Hasło** - ciąg znaków literowych, cyfrowych lub innych, uwierzytelniający osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym
17. **Identyfikator Użytkownika (login)** - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
18. **Incydent** - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji lub zmniejszeniem poziomu usług systemowych, które stwarzają znaczne prawdopodobieństwo zakłócenia działania systemu informatycznego i zagrażają bezpieczeństwu informacji; naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność;
19. **Korekcja** - działanie w celu wyeliminowania wykrytej niezgodności lub incydentu;

20. **Kontrola (Audyt)** - systematyczny, niezależny i udokumentowany proces oceny skuteczności systemu ochrony danych osobowych, na podstawie określonych kryteriów, wymagań polityk i procedur;
21. **Niezgodność** - niespełnienie wymagania, czyli potrzeby lub oczekiwania, które zostało ustalone, przyjęte zwyczajowo lub jest obowiązkowe;
22. **Nośniki danych** - płyty CD lub DVD, pamięć Flash, dyski twarde lub inne urządzenia/materiały służące do przechowywania plików z danymi;
23. **Odbiorca danych** - każdy, komu udostępniane są dane osobowe, z wyłączeniem osoby, której dane dotyczą;
    a) osoby upoważnionej do przetwarzania danych osobowych;
    b) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;
24. **Podatność** - luka (słabość), która może być wykorzystana przez co najmniej jedno zagrożenie, rozumiane jako potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę;
25. **Polityka Bezpieczeństwa (PB)** - dokument o nazwie Polityka Bezpieczeństwa w Urzędzie Miasta i Gminy Bystrzyca Kłodzka;
26. **Zabezpieczenie danych w systemie informatycznym** - wdrożenie przez Administratora stosownych środków organizacyjnych i technicznych w celu zabezpieczenia zasobów oraz ochrony danych przed dostępem, modyfikacją ujawnieniem, pozyskaniem lub zniszczeniem przez osobę trzecią;
27. **RODO** - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE;
28. **Serwisant** - firma lub pracownik firmy zajmujący się instalacją, naprawą oraz konserwacją sprzętu komputerowego;
29. **Sieć publiczna** - sieć telekomunikacyjna wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;
30. **Słabość systemu** - zdarzenie, stan rzeczy zwiększający ryzyko wystąpienia incydentu;
31. **Usuwanie danych** - zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dotyczą;
32. **Uwierzytelnianie** - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
33. **Profilowanie** - polega na dowolnym zautomatyzowanym przetwarzaniu danych osobowych pozwalającym ocenić czynniki osobowe osoby fizycznej, a w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą - o ile wywołuje skutki prawne względem tej osoby lub w podobny sposób znacząco na nią wpływa;
34. **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
35. **Zdarzenie** - błąd zabezpieczenia lub nieznana dotychczas sytuacja, która może być związana z zagrożeniem bezpieczeństwa danych osobowych;
36. **PUODO** - Prezes Urzędu Ochrony Danych Osobowych;

37. **Organ nadzorczy** - Prezes Ochrony Danych Osobowych - PUODO;
38. **Pseudonimująca** - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
39. **Dane genetyczne** - dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, uzyskane z analizy próbki biologicznej danej osoby fizycznej, w szczególności z analizy chromosomów, kwasu dezoksyrybonukleinowego (DNA) lub kwasu rybonukleinowego (RNA) lub z analizy innych elementów umożliwiających pozyskanie równoważnych informacji;
40. **Dane biometryczne** - oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
41. **Dane dotyczące zdrowia** - dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia.

§ 4

Administratorem danych osobowych gromadzonych i przetwarzanych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka jest Burmistrz Bystrzycy Kłodzkiej.

W celu zapewnienia należytej ochrony danych osobowych, zgodnie z obowiązkami nałożonymi przez przepisy RODO, Kierownicy Wydziałów UMiG oraz inne wyznaczone osoby zostały upoważnione i zobowiązane do realizowania czynności w imieniu administratora m.in. do:

1. Obligowania podległych pracowników oraz innych osób współpracujących z podległą komórką organizacyjną do zachowania poufności.
2. Wnioskowania o nadawanie, zmianę oraz odwoływanie upoważnień do przetwarzania danych osobowych w ramach podległej komórki organizacyjnej. Wszelkie wnioski w tym zakresie winny być kierowane do Administratora Danych Osobowych za pośrednictwem Inspektora Danych Osobowych.
3. Przeprowadzania wewnętrznych szkoleń personelu podległej komórki w zakresie stosowania obowiązujących u administratora procedur i zasad ochrony danych, a także przepisów o ochronie danych osobowych. Szkolenia powinny odbywać się przy wsparciu Inspektora Danych Osobowych.
4. Wnioskowania o aktualizowanie rejestru czynności oraz rejestru kategorii danych przetwarzanych w ramach danej komórki organizacyjnej. Wszelkie wnioski w tym zakresie winny być kierowane do Administratora Danych Osobowych za pośrednictwem Inspektora Danych Osobowych.
5. Udostępniania wyznaczonemu Inspektorowi Ochrony Danych oraz Administratorom Systemów Informatycznych wszelkich dostępnych informacji oraz zasobów, w zakresie niezbędnym do monitorowania zgodności przetwarzania danych z przepisami.

6. Wdrażania przyjętych przez Administratora Danych Osobowych środków technicznych i organizacyjnych mających na celu minimalizację ryzyka naruszenia dla ochrony danych.
7. Konsultowania nowych procesów przetwarzania z Inspektorem Ochrony Danych.
8. Realizowania innych zadań oraz obowiązków wskazanych przez Administratora Danych Osobowych w dokumentacji ochrony danych osobowych oraz wynikających z przepisów prawa.
9. Obligowania podległych pracowników do wypełniania obowiązków informacyjnych wynikających z rozporządzenia unijnego (RODO).
10. Zawierania umów powierzenia danych osobowych i zgłaszania ich Inspektorowi Danych Osobowych celem ujęcia w prowadzonym wykazie (rejestrze). Zgłoszenie umowy wymaga formy pisemnej.

§ 5

1. Polityka Bezpieczeństwa określa:

   a) granice dopuszczalnego zachowania Użytkowników Systemu stosowanego w Urzędzie Miasta i Gminy Bystrzyca Kłodzka oraz wskazuje konsekwencje w stosunku do osób naruszających przepisy ustawy o ochronie danych osobowych;
   b) prawa i obowiązki Użytkowników Systemu w zakresie bezpieczeństwa informacji, w tym ochrony danych osobowych w nim przetwarzanych;
   c) sposób przetwarzania danych osobowych oraz środki organizacyjne i techniczne zapewniające ochronę tych danych;
   d) podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
   e) instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych;
   f) wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe;
   g) sposób przepływu informacji pomiędzy poszczególnymi systemami;
   h) środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych.

2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

   a) poufność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym osobom,
   b) integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
   c) rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
   d) integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji zamierzonej, jak i przypadkowej,
   e) dostępność informacji - rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,

f) zarządzanie ryzykiem - rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

3. Polityka Bezpieczeństwa została wprowadzona Zarządzeniem Nr 0050.199.2021 Burmistrza Bystrzycy Kłodzkiej z dnia 25 czerwca 2021 r. w sprawie wprowadzenia Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka oraz udostępniona wszystkim Użytkownikom systemu oraz pozostałym pracownikom posiadającym dostęp do przetwarzanych danych osobowych.

4. Każda osoba, mająca dostęp do danych osobowych jest zobowiązana do zapoznania się z niniejszym dokumentem oraz potwierdzenia tego faktu poprzez złożenie pisemnego oświadczenia włączanego do akt osobowych lub innej dokumentacji niepracowniczej. Wzór oświadczenia stanowi załącznik nr 4 do Zarządzenia.

RODZIAŁ II - ZASADY PRZETWARZANIA DANYCH OSOBOWYCH. ODPOWIEDZIALNOŚĆ. OBOWIĄZEK INFORMACYJNY

§ 6

Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy Urzędu Miasta i Gminy w Bystrzycy Kłodzkiej. Każda osoba, mająca dostęp do danych osobowych przetwarzanych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka jest zobowiązana do zapoznania się z niniejszym dokumentem.

§ 7

1. Obszary przetwarzania danych osobowych określa tabela nr 1:

Tabela nr 1. Obszary przetwarzania danych osobowych

Lokalizacja - adres	**Kondygnacja**	**Precyzyjne określenie pomieszczenia**
Budynek Ratusza Urząd Miasta i Gminy Bystrzyca Kłodzka Plac Wolności 1, 57-500 Bystrzyca Kłodzka	-1	Serwerownia (-02)
Budynek Ratusza Urząd Miasta i Gminy Bystrzyca Kłodzka Plac Wolności 1, 57-500 Bystrzyca Kłodzka	Parter	Pokój 1-2,4-11, Kasa (11), BOK (11)
Budynek Ratusza Urząd Miasta i Gminy Bystrzyca Kłodzka Plac Wolności 1, 57-500 Bystrzyca Kłodzka	I Pietro	Pokój 101-103,106-117, Sala Konferencyjna (111)
Budynek Ratusza Urząd Miasta i Gminy Bystrzyca Kłodzka Plac Wolności 1, 57-500 Bystrzyca Kłodzka	II Piętro	Pokój 201-204,209-218, Sala Rajców (216)
Budynek Ratusza Urząd Miasta i Gminy Bystrzyca Kłodzka Plac Wolności 1, 57-500 Bystrzyca Kłodzka	III Piętro	Pokój 304-309, Pokój 301-302(Archiwum)
Wydział Urbanistyki i Planowania Urząd Miasta i Gminy Bystrzyca Kłodzka Plac Wolności 4, 57-500 Bystrzyca Kłodzka	Parter	Pokój 1-2, Pokój 3(Archiwum)
Wydział Turystyki i Kultury Fizycznej Urząd Miasta i Gminy Bystrzyca Kłodzka Plac Wolności 17, 57-500 Bystrzyca Kłodzka	Parter	Sala obsługi Sala konferencyjna Pokój Kierownika Pokój Zastępcy Kierownika
Wydział Rolnictwa i Ochrony Środowiska Urząd Miasta i Gminy Bystrzyca Kłodzka Mały Rynek 1, 57-500 Bystrzyca Kłodzka	Parter	Sala obsługi Pokój Kierownika

Wydział Gospodarki Komunalnej i Mieszkaniowej Urząd Miasta i Gminy Bystrzyca Kłodzka ul. Okrzei 1, 57-500 Bystrzyca Kłodzka	Parter	Sala obsługi Pokój Kierownika Pokój Zastępcy Kierownika

Straż Miejska Budynek ZUK ul. Strażacka 13 57-500 Bystrzyca Kłodzka	Parter	

Gminna Komisja Rozwiązywania problemów alkoholowych Budynek OPS ul. 1 Maja 1 57-500 Bystrzyca Kłodzka		

2. Wymagany przez rozporządzenie wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar przetwarzania danych osobowych, stanowi załącznik nr 1 do Polityki Bezpieczeństwa.

§ 8

Załącznikiem do Polityki Bezpieczeństwa jest opracowany zgodnie z art. 30 RODO - Rejestr czynności przetwarzania danych osobowych, stanowiący załącznik nr 11 do Polityki bezpieczeństwa.

§ 9

Wszystkie osoby, które przetwarzają dane osobowe w obszarze wymienionym w § 7, muszą posiadać pisemne upoważnienie do przetwarzania danych nadane przez ADO oraz podpisać oświadczenie o zachowaniu poufności tych danych. Wzór upoważnienia stanowi załącznik nr 2 do Polityki Bezpieczeństwa. Wzór oświadczenia o zachowaniu poufności stanowi załącznik nr 3 do PB.

§ 10

1. Do przetwarzania powierzonych danych osobowych mogą być dopuszczeni jedynie pracownicy Urzędu Miasta i Gminy Bystrzyca Kłodzka oraz pracownicy podmiotów świadczących usługi na jej rzecz w związku z realizacją celów i zadań (prace doraźne o charakterze serwisowym lub innym).

2. Każdy podmiot wymieniony w pkt 1 niniejszego paragrafu zobowiązany jest do podpisania z Urzędem Miasta i Gminy Bystrzyca Kłodzka umowy powierzenia przetwarzania danych osobowych.

3. Zakres danych osobowych powierzanych przez Urząd Miasta i Gminy Bystrzyca Kłodzka powinien być adekwatny do celu powierzenia oraz udokumentowany w postaci wykazu podmiotów, którym powierzono dane osobowe, za każdym razem, gdy takie powierzenie nastąpi.

§ 11

1. Upoważnienia i polecenie do przetwarzania danych osobowych w systemie informatycznym wydawane są zgodnie z właściwą procedurą określoną w niniejszym dokumencie oraz w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka.

2. Upoważnienia i polecenie do przetwarzania danych osobowych zawartych w rejestrze, o którym mowa w paragrafie 8 wydawane są zgodnie z właściwą procedurą określoną w niniejszym dokumencie.

3. Upoważnienia i polecenie, o których mowa w pkt 1 & 2 niniejszego paragrafu, ważne są do dnia odwołania lub do chwili ustania zatrudnienia upoważnionego pracownika lub osoby upoważnionej

§ 12

1. W zbiorach danych gromadzonych w systemie informatycznym zabrania się przetwarzania danych ujawniających:

   a) stan zdrowia;
   b) pochodzenie rasowe lub etniczne;
   c) poglądy polityczne;
   d) przekonania religijne lub filozoficzne;
   e) przynależność wyznaniową;
   f) przynależność partyjną lub związkową;
   g) dane genetyczne;
   h) dane biometryczne
   i) nałogi;
   j) preferencje seksualne;

   chyba że wymagają tego obowiązujące przepisy prawa lub osoba, której dane dotyczą, wyraziła na to pisemną zgodę.

2. Dane o skazaniach, w tym dane o niekaralności można przetwarzać wyłącznie pod nadzorem władz publicznych.

3. Do profilowania zabrania się używania danych wymienionych w pkt 1 niniejszego paragrafu, chyba, że osoba, której dane dotyczą wyraziła na to zgodę lub jest to podyktowane ważnym interesem publicznym.

4. Przy profilowaniu ADO obowiązkowo wdraża środki ochrony praw, wolności i uzasadnionych interesów osoby, której dane dotyczą.

5. O profilowaniu należy informować osobę, której ono dotyczy na etapie zbierania danych, a także na każdy wniosek osoby, której dane dotyczą.

6. Każda osoba, której dane dotyczą, ma prawo wyrażenia sprzeciwu na profilowanie przez Urząd jej danych osobowych, jeżeli uzna, że narusza to jej prawa i wolności.

§ 13

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

§ 14

1. Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie w sytuacji, w której administrator danych udostępniający dane oraz administrator danych pozyskujący dane drogą udostępnienia posiadają odpowiednią podstawę prawną w sprawie ww. czynności.

2. Administrator Danych Osobowych może odmówić udostępnienia danych osobowych w sytuacji, w której spowodowałoby to istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób oraz w sytuacji, w której dane osobowe nie mają istotnego związku ze wskazanymi motywami działania wnioskującego o udostępnienie danych

3. W przypadku konieczności udostępniania dokumentów i danych w nich zawartych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych.

4. W przypadku, gdy dane osobowe osoby, od której zostały zebrane, są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem ustawy lub są zbędne do realizacji celu, dla którego zostały zebrane, ADO lub osoba przez niego upoważniona jest zobowiązana do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

§ 15

1. Do przetwarzania powierzonych danych osobowych mogą być dopuszczeni jedynie pracownicy Urzędu oraz pracownicy podmiotów (procesorów) świadczących usługi na jego rzecz w związku z realizacją celów i zadań administratora.

2. Powierzenie przetwarzania danych osobowych następuje na podstawie umowy powierzenia przetwarzania danych osobowych lub innego aktu (instrumentu) prawnego, zawartej w formie pisemnej lub dopuszczalnej prawem formie elektronicznej w postaci oświadczenia złożonego za pośrednictwem poczty e-mail, określonej opcji internetowej lub zapisanego na elektronicznym nośniku informacji.

3. Zgodnie art. 28 RODO, umowa powierzenia danych osobowych powinna określać przedmiot i czas trwania przetwarzania, zakres, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą, obowiązki i prawa stron umowy (administratora i procesora).

4. Zakres danych osobowych powierzanych powinien być adekwatny do celu powierzenia.

5. Administrator danych osobowych zobowiązany jest do dokumentowania powierzania tych danych w postaci wykazu podmiotów, którym powierzono dane osobowe, za każdym razem, gdy takie powierzenie nastąpi. Kierownicy Wydziałów oraz osoby zatrudnione na samodzielnych stanowiskach zobowiązane są do zgłaszania wszelkich umów powierzenia Inspektorowi Danych Osobowych.

6. W przypadku, w którym podmiot określony w umowie powierzenia danych osobowych, w zakresie realizacji swoich usług korzysta z pomocy innych podmiotów (podpowierzenie danych), wymagana jest szczegółowa lub ogólna zgoda Urzędu na przekazanie powierzonych danych, wyrażona w formie pisemnej lub równoważnej jej formie elektronicznej.

§ 16

W celu zapewnienia należytej ochrony przetwarzania danych osobowych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka zastosowano środki zabezpieczające powierzone zbiory danych w postaci następujących zabezpieczeń technicznych i organizacyjnych:

1. Zabezpieczenia techniczne

   1) Dokumenty zawierające dane osobowe w formie papierowej, upoważnione osoby przechowują w obszarze przetwarzania danych w pomieszczeniach zabezpieczonych drzwiami zamykanymi na klucz w szafach zamykanych na klucz (lub w inny sposób), do których dostęp mają jedynie upoważnione osoby;
   2) Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na klucz na czas nieobecności w nich osób zatrudnionych;
   3) Pracownicy zobowiązani są do zorganizowania stanowiska pracy w ten sposób, aby uniemożliwić swobodny dostęp do danych osobowych osobom do tego nieupoważnionym (np. poprzez pozostawienie na biurku dokumentów zawierających dane osobowe);
   4) Pomieszczenia, w których przetwarzane są dane osobowe wyposażone są w przeciwwłamaniowy system alarmowy;
   5) Pomieszczenia, w których przetwarzane są dane osobowe są zabezpieczone przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy;
   6) Dostęp do pomieszczeń, w których przetwarzane są dane osobowe kontrolowany jest przez system monitoringu z zastosowaniem kamer.
   7) Celem monitoringu wizyjnego jest:
      a) Zapewnienie bezpieczeństwa pracowników urzędu i klientów urzędu;
      b) Ochrona mienia pracodawcy i mienia publicznego;
      c) Ograniczenie zachowań niepożądanych zagrażających zdrowiu i bezpieczeństwu pracowników i klientów urzędu.
   8) Odpowiedzialnym za obsługę oraz kontrolę urządzeń rejestrujących jest Administrator Systemu Informatycznego;
   9) W przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenia dokonuje się poprzez pocięcie w niszczarce;
   10) Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania;

11) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
12) Do ochrony dostępu do sieci komputerowej użyto systemu Firewall;
13) Zastosowany system informatyczny umożliwia rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych;
14) Zastosowany system informatyczny umożliwia określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego w tym systemie zbioru danych osobowych;
15) Dostęp do danych osobowych w systemie informatycznym wymaga uwierzytelnienia z wykorzystaniem identyfikatora (loginu) Użytkownika oraz hasła;
16) Stosowany system informatyczny posiada mechanizm wymuszający okresową zmianę haseł dostępu;
17) Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika;

2. Środki ochrony w ramach oprogramowania systemu:

a) dostęp fizyczny do baz danych osobowych zastrzeżony jest wyłącznie dla IOD i ASI oraz podmiotów zewnętrznych, zgodnie z zawartymi umowami powierzenia przetwarzania danych;
b) konfiguracja systemu umożliwia użytkownikom dostęp do danych osobowych tylko za pośrednictwem aplikacji;
c) system operacyjny serwera pozwala zdefiniować prawa dostępu do zasobów systemu;
d) zastosowano działający w „tle" program antywirusowy na komputerach użytkowników.

3. Zabezpieczenia organizacyjne

1. Opracowano i wdrożono Politykę bezpieczeństwa oraz Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka;
2. Powołano Inspektora Ochrony Danych, który sprawuje nadzór nad przetwarzaniem danych osobowych;
3. Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie;
4. Prowadzone są wykazy pomieszczeń i osób przetwarzających dane opisane w § 7 niniejszego dokumentu;
5. Wszystkie osoby wykonujące czynności związane z przetwarzaniem danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych;
6. Wszyscy Użytkownicy systemu informatycznego zostali przeszkoleni w zakresie zabezpieczeń tego systemu;
7. Kierownicy wydziałów są zobowiązani do przeprowadzania wewnętrznych szkoleń personelu podległej komórki w zakresie stosowania obowiązujących u administratora procedur i zasad ochrony danych, a także przepisów o ochronie danych osobowych;
8. Wszystkie osoby wykonujące czynności związane z przetwarzaniem danych osobowych obowiązane zostały do zachowania ich w tajemnicy;

9. Wykonywane są kopie zapasowe baz danych systemów informatycznych. System Acronis odpowiedzialny za wykonywanie kopii zapasowych kopii wirtualnych serwerów. Kopie zgrywane są na serwer oraz na urządzenie do wykonywania kopii Qnap znajdujące się na innej kondygnacji budynku Urzędu (serwerownia znajduje się na kondygnacji -1, kopie zapasowe znajdują się na kondygnacji 2);
10. Przebywanie osób nieuprawnionych do dostępu do danych osobowych w pomieszczeniach tworzących obszar przetwarzania danych osobowych jest możliwe jedynie w obecności osoby zatrudnionej przy przetwarzaniu danych;
11. W przypadku przebywania osób nieposiadających dostępu do przetwarzania danych, monitory stanowisk komputerowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane (wykorzystanie filtrów prywatyzujących);
12. Wyznaczono Administratora Systemu przetwarzania danych osobowych - ASI;
13. Wprowadzono instrukcję zarządzania system informatycznym służącym do przetwarzania danych osobowych;
14. ASI jest również zobowiązany do przeprowadzania analizy ryzyka związanych z zagrożeniami związanymi z przetwarzaniem danych osobowych w systemie informatycznym.

§ 17

1. Przetwarzanie danych osobowych, które jest niedopuszczalne albo dokonane przez osobę, która nie jest uprawniona do podejmowania takich czynności, jest zagrożone karą grzywny, ograniczenia wolności lub pozbawienia wolności do lat dwóch. W przypadku, w którym czyn dotyczy danych osobowych o szczególnym znaczeniu (np. danych biometrycznych, danych ujawniających pochodzenie rasowe lub etniczne, danych dotyczących zdrowia), wymiar kary pozbawienia wolności wynosi do lat trzech.

2. Przestępstwem jest również udaremnianie lub utrudnianie przeprowadzenia kontroli przestrzegania przepisów o ochronie danych osobowych. Czyn ten jest zagrożony karą grzywny, ograniczenia wolności lub pozbawienia wolności do lat dwóch.

§ 18

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, ADO jest obowiązany poinformować tę osobę o:

a) adresie swojej siedziby i pełnej nazwie, tożsamości administratora
b) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych;
c) prawie dostępu do treści swoich danych oraz ich poprawiania;
d) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

2. Obowiązek poinformowania wymieniony w ust. 1 powinien być wykonany w momencie zbierania danych z wyjątkiem sytuacji, w której:

a) przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania;

b) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.

3. W przypadku pozyskania danych osobowych z innego źródła niż osoba, której dane dotyczą, ADO jest zobowiązany poinformować tę osobę o:

a) adresie swojej siedziby i pełnej nazwie, tożsamości administratora
b) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych;
c) źródle danych;
d) prawie dostępu do treści swoich danych oraz ich poprawiania;

4. Obowiązek poinformowania wymieniony w ust. 2 powinien zostać spełniony bezpośrednio po utrwaleniu zebranych danych, a więc po zapisaniu danych w sposób umożliwiający ich dalsze przetwarzanie z wyjątkiem sytuacji, w której:

a) przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą;
b) dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie wymagań określonych w ust. 3 wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania;

ROZDZIAŁ III - INSPEKTOR OCHRONY DANYCH

§ 19

1. ADO powołał Inspektora Ochrony Danych, który sprawuje nadzór nad przetwarzaniem danych osobowych.

2. Podczas nieobecności funkcję pełni Zastępca Inspektora Ochrony Danych.

3. Administrator zapewnia, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych, w tym zapewnia mu dostęp do danych osobowych i operacji przetwarzania.

4. Zadaniem IOD jest monitorowanie stanu prawnego i wsparcie ADO i ASI w zakresie spełnienia wymogów prawnych. IOD na żądanie ADO i ASI dokonuje oceny planowanych lub przyjętych środków pod kątem ich zgodności z przepisami prawa.

5. Do zadań IOD należy:

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział

obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
d) współpraca z Prezesem Urzędu Ochrony Danych Osobowych;
e) pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem danych osobowych;
f) pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.

§ 20

Ponadto IOD prowadzi następujące wykazy w oparciu o informacje i dane przekazywane przez kierowników wydziałów:

a) wykaz osób, którym nadano upoważnienia do przetwarzania danych osobowych;
b) wykaz pomieszczeń, w których przetwarzane są dane osobowe, stanowiących obszar przetwarzania;
c) wykaz podmiotów, którym powierzono dane osobowe do przetwarzania;
d) wykaz udostępnień danych osobowych osobom których dotyczą.

ROZDZIAŁ IV - WARUNKI KORZYSTANIA Z SYSTEMU INFORMATYCZNEGO

§ 21

1. Każdy Użytkownik jest zobowiązany do zapoznania się i zaakceptowania zasad korzystania z systemu informatycznego, co potwierdza przez pisemną akceptacją udzielonego przez ADO upoważnienia do przetwarzania danych osobowych lub dostępu do danych osobowych (adnotacja na upoważnieniu o treści: „Przyjmuję do wiadomości i stosowania" (wraz z własnoręcznym podpisem i datą).

2. Zgodnie z postanowieniami niniejszej Polityki bezpieczeństwa, zabrania się Użytkownikowi systemu podejmowania jakichkolwiek czynności mających na celu naruszenie bezpieczeństwa przetwarzanych danych, w tym prób przełamania zabezpieczeń systemu.

3. Spełnienie obowiązków, o których mowa w ust. 1 i 2, jest warunkiem uzyskania dostępu do systemu. Jeden egzemplarz upoważnienia przechowuje się w teczce akt osobowych upoważnionego pracownika.

4. Zabronione jest korzystanie z systemu informatycznego z użyciem danych dostępowych innego Użytkownika.

5. Użytkownicy są zobowiązani do zachowania zasady bezpiecznego ustawienia monitora, czyli w przypadku przebywania osób nieposiadających dostępu do przetwarzania danych, monitory stanowisk komputerowych powinny być ustawione w taki sposób, aby uniemożliwić

tym osobom wgląd w dane. Stosuje się wygaszacze ekranów, które włączają się po upływie maksymalnie 15 minut bezczynności komputera. W razie potrzeby stosuje się filtry prywatyzujące.

6. Użytkownik zobowiązany jest do przestrzegania zasady czystego biurka, w szczególności przed opuszczeniem swego stanowiska pracy, Użytkownik powinien schować wszelkie dokumenty związane z używanym systemem oraz informatyczne nośniki danych (płyty CD, DVD, pendrive itp.).

7. Dokumenty zawierające wydruki oraz inne dokumenty przeznaczone do likwidacji muszą być niezwłocznie trwale uszkodzone w sposób uniemożliwiający odczytanie z nich informacji osobowych (stosuje się niszczarki dokumentów).

8. Użytkownik jest zobowiązany do przestrzegania zasady czystej drukarki/kopiarki, czyli wydrukowane/kopiowane dokumenty winny być niezwłocznie po ich wydrukowaniu/ skopiowaniu zabrane z urządzenia, a w przypadku korzystania z urządzeń sieciowych, używanych w innym pomieszczeniu niż przebywa użytkownik, drukowanie/kopiowanie dokumentów może rozpocząć się dopiero po uruchomieniu urządzenia osobiście przez użytkownika np. za pomocą kodu dostępu, a nie automatycznie po zleceniu wydruku/kopii dokumentu z komputera użytkownika. Bezpośrednio po wydrukowaniu/skopiowaniu dokumenty winny być zabrane z urządzenia.

§ 22

Szczegółowe procedury korzystania oraz zasady konfiguracji sprzętu komputerowego Użytkownika systemu informatycznego reguluje Instrukcja zarządzania systemem informatycznym, w której opisane są niezbędne środki do prawidłowego korzystania z systemu informatycznego.

ROZDZIAŁ V - POCZTA ELEKTRONICZNA, INTERNET W SYSTEMIE

§ 23

1. Użytkownik zobowiązany jest do dbania o bezpieczeństwo konta mailowego, o którym mowa powyżej, w szczególności do:

a) nieotwierania załączników do poczty i linków pochodzących z nieznanych źródeł;
b) zachowania ostrożności podczas otwierania nieoczekiwanych załączników w korespondencji pochodzącej od znanych nadawców.

2. Użytkownik zobowiązany jest do korzystania z sieci Internet w sposób, który nie zagraża bezpieczeństwu danych gromadzonych i przetwarzanych w systemie.

ROZDZIAŁ VI - POSTĘPOWANIE NA WYPADEK ZAGROŻENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

§ 24

1. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

   a) próby naruszenia ochrony danych:
      - z zewnątrz- włamania do systemu, podsłuch, kradzież danych;
      - wewnątrz - nieumyślna lub celowa modyfikacja danych, kradzież danych.
   b) programy destrukcyjne;
   c) awarie sprzętu lub uszkodzenie oprogramowania;
   d) zabór sprzętu lub nośników z ważnymi danymi;
   e) inne skutkujące utratą danych osobowych bądź wejściem w ich posiadanie osób nieuprawnionych;
   f) usiłowanie zakłócenia działania systemu informatycznego;

2. Do typowych incydentów bezpieczeństwa danych osobowych należą:

   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
   b) niewłaściwe zabezpieczenie sprzętu informatycznego, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
   c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek);
   d) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
   e) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych);
   f) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

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

   a) zgłoszenia od Użytkowników;
   b) alarmy z systemów informatycznych;
   c) analizy incydentów;
   d) wyniki audytów / kontroli.

§ 25

Każdy pracownik Urzędu Miasta i Gminy Bystrzyca Kłodzka, w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować ADO oraz IOD. Zasady działania w takich przypadkach określa tabela nr 2.

Tabela nr 2. Zasady działania w przypadku zagrożenia lub naruszenia ochrony danych osobowych

L.p. uchybienia lub zagrożenia	**Uchybienie i zagrożenie nieświadome wewnętrzne i zewnętrzne**	**Postępowanie w przypadku uchybienia lub zagrożenia**
1.	Pomieszczenie, w którym przechowywane są dane osobowe pozostaje bez nadzoru	Należy zabezpieczyć dane osobowe oraz powiadomić IOD, który sporządza Protokół uchybienia
2.	Komputer nie jest zabezpieczony hasłem	Należy zabezpieczyć dane osobowe oraz powiadomić IOD, który sporządza Protokół uchybienia
3.	Dostęp do danych mają osoby nieupoważnione	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić IOD, który sporządza Protokół uchybienia
4.	Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym	Należy powiadomić IOD, który powinien sprawdzić system uwierzytelniania oraz sprawdzić, czy nie doszło do kradzieży lub zniszczenia danych. IOD sporządza Protokół uchybienia
L.p. uchybienia lub zagrożenia	**Uchybienie i zagrożenie nieświadome wewnętrzne i zewnętrzne**	**Postępowanie w przypadku uchybienia lub zagrożenia**
5.	Próba kradzieży danych osobowych poprzez zewnętrzny nośnik danych	Należy nie dopuścić do kradzieży danych i powiadomić IOD.IOD powinien zabezpieczyć nośnik danych i powiadomić

		Beneficjenta. IOD sporządza Protokół zagrożenia.
6.	Próba kradzieży danych osobowych w formie papierowej	Należy nie dopuścić do kradzieży danych osobowych i powiadomić IOD. IOD powinien zabezpieczyć dane i powiadomić ADO. IOD sporządza Protokół zagrożenia
7.	Nieuprawniony dostęp do danych osobowych w formie papierowej	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić IOD, który sporządza Protokół uchybienia
8.	Dane osobowe przechowywane są w niezabezpieczonym pomieszczeniu	Należy powiadomić IOD, który powinien zabezpieczyć pomieszczenie i sporządzić Protokół uchybienia
9.	Próba włamania do pomieszczenia/budynku	Należy zabezpieczyć dowody i powiadomić IOD. IOD sprawdza stan uszkodzeń, zabezpiecza dowody i wzywa policję. IOD sporządza protokół zagrożenia.
10.	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania	Należy zrobić audyt systemów zabezpieczeń, a w szczególności systemów antywirusowych i firewall. IOD powinien ocenić, czy nie doszło do utraty danych osobowych i w zależności od tego sporządzić protokół uchybienia lub zagrożenia
11.	Brak aktywnego oprogramowania antywirusowego	Należy powiadomić IOD. IOD powinien zaktualizować lub nabyć oprogramowanie antywirusowe. IOD sporządza Protokół uchybienia
12.	Zniszczenie lub modyfikacja danych osobowych w formie papierowej	Należy zabezpieczyć dowody i powiadomić IOD. IOD sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia IOD. IOD sporządza protokół zagrożenia

13.	Zniszczenie lub modyfikacja danych osobowych w systemie informatycznym	Należy zabezpieczyć dowody i powiadomić IOD. IOD sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia ADO. IOD sporządza Protokół zagrożenia
14.	Uszkodzenie komputerów, nośników danych	Należy powiadomić IOD, który powinien ocenić w wyniku czego doszło do zniszczenia i przywrócić dane z kopii zapasowej. IOD powiadamia ADO i sporządza Protokół zagrożenia
15.	Próba nieprawidłowej interwencji przy sprzęcie komputerowym	Należy uniemożliwić dostęp osób do sprzętu komputerowego oraz powiadomić IOD, który sporządza Protokół uchybienia
16.	Zdarzenia losowe	Należy oszacować powstałe straty i sporządzić Protokół zagrożenia lub uchybienia

§ 26

W przypadku stwierdzenia wystąpienia zagrożenia, IOD prowadzi postępowanie wyjaśniające, w toku, którego:

a) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki;
b) inicjuje ewentualne działania dyscyplinarne;
c) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości;
d) dokumentuje prowadzone postępowania.

§ 27

1. W przypadku stwierdzenia incydentu (naruszenia), Inspektor Ochrony Danych (IOD) prowadzi postępowanie wyjaśniające w toku, którego:

a) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały;
b) zabezpiecza ewentualne dowody;
c) ustala osoby odpowiedzialne za naruszenie;
d) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);
e) inicjuje działania dyscyplinarne;
f) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości;
g) dokumentuje prowadzone postępowania.

2. Zgodnie z zasadami zawartymi w art. 33 RODO, w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

3. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu, działając zgodnie z procedurą zawartą w art. 34 RODO.

§ 28

IOD jest odpowiedzialny za analizę incydentów bezpieczeństwa, zagrożeń lub słabości systemu ochrony danych osobowych. Gdy stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa:

a) źródło powstania incydentu lub zagrożenia;
b) zakres działań korygujących lub zapobiegawczych;
c) termin realizacji, osobę odpowiedzialną.

§ 29

IOD jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych. Po przeprowadzeniu działań korygujących lub zapobiegawczych, jest zobowiązany do oceny efektywności ich zastosowania i prowadzenia stosownej dokumentacji.

§ 30

Integralną częścią Polityki Bezpieczeństwa są poniższe dokumenty prowadzone przez IOD w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych:

a) Dziennik uchybień i zagrożeń - załącznik nr 7 do niniejszej Polityki;
b) Protokół uchybienia - załącznik nr 8 do niniejszej Polityki;
c) Protokół zagrożenia - załącznik nr 9 do niniejszej Polityki.

ROZDZIAŁ VII - POSTANOWIENIA KOŃCOWE

§ 31

1. W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie przepisy z zakresu danych osobowych oraz przepisy sektorowe.

2. Zgodnie z zasadami zawartymi w art. 5 RODO Administrator Danych Osobowych jest odpowiedzialny za przestrzeganie przepisów i musi być w stanie wykazać ich przestrzeganie (zasada rozliczalności).

§ 32

Niniejszy dokument wchodzi w życie z dniem 1 lipca 2021 r.

Burmistrz
Bystrzycy Kłodzkiej
Renata Surma

.....

podpis Administratora Danych Osobowych

WYKAZ POMIESZCZEŃ W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

L.p	Lokalizacja	Precyzyjne określenie pomieszczenia	Wydział/osoba użytkująca pomieszczenie	Zabezpieczenie pomieszczenia
1.				
2.				
3.				
4.				
5.				

Bystrzyca Kłodzka, dnia roku

UPOWAŻNIENIE I POLECENIE PRZETWARZANIA DANYCH OSOBOWYCH

Nr / u Administratora Danych Osobowych
Urzędu Miasta i Gminy Bystrzyca Kłodzka

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przeplywu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

upoważniam Panią/Pana* **imię i nazwisko**

stanowisko

do przetwarzania danych osobowych w zakresie i celu niezbędnym do prawidlowego wykonywania u Administratora praw i obowiązków na zajmowanym przez Panią/Pana stanowisku, zgodnie z zakresem kompetencji oraz obowiązków zawodowych i służbowych na tym stanowisku, a także zgodnie z wytycznymi Administratora oraz **polecam Pani/Panu przetwarzanie danych osobowych** w powyższym zakresie i celu. Powyższe upoważnienie i polecenie obejmuje powierzone do przetwarzania dane osobowe przez innego administratora, w zakresie i celu określonym w umowie powierzenia, w przypadku jej zawarcia.

Upoważniam:

1. do dostępu i przetwarzania danych osobowych w następujących zbiorach danych osobowych o numerze w rejestrze:

2. w systemie informatycznym nadaję uprawnienia do przetwarzania danych w programie:

Upoważnienie i polecenie wygasa z chwilą ustania Pana/Pani zatrudnienia lub współpracy (bez względu na podstawę prawną zatrudnienia lub współpracy) lub odwołania upoważnienia. Jednocześnie informuję, że zobowiązany(a) jest Pan(i) do zachowania w tajemnicy powyższych informacji, w szczególności w zakresie danych osobowych i sposobów ich zabezpieczania, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia lub współpracy.

_____

(podpis Administratora)

Przyjmuję do wiadomości i stosowania

Data i podpis osoby upoważnionej:

OŚWIADCZENIE o zachowaniu poufności

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał/-a dostęp w związku z wykonywaniem jakichkolwiek czynności na rzecz Urzędu Miasta i Gminy Bystrzyca Kłodzka.

Zobowiązuję się przestrzegać wszelkich procedur obowiązujących w Urzędzie Miasta i Gminy Bystrzyca Kłodzka, dotyczących ochrony danych osobowych – w szczególności określonych w **Polityce Bezpieczeństwa** oraz **Instrukcji Zarządzania Systemem Informatycznym.**

Oświadczam, że zapoznałem/-am się z przepisami dotyczącymi ochrony danych osobowych, w tym z obowiązującą ustawą o ochronie danych osobowych, wraz z zasadami odpowiedzialności karnej określonymi w ww. ustawie.

Przyjmuję do wiadomości i stosowania.

Data i podpis osoby upoważnionej:

Bystrzyca Kłodzka, dnia roku

Nazwisko i imię
Komórka organizacyjna*
Stanowisko *

Rodzaj zadań i obowiązków wynikających:	**Właściwe zaznaczyć znakiem „X"**
Zatrudnienia w Urzędzie Miasta i Gminy Bystrzyca Kłodzka	
Umowy cywilnoprawnej zawartej z Gminą Bystrzyca Kłodzka	
Z odbywania stażu	
Z odbywania praktyki	

OŚWIADCZENIE

Pouczona/y o odpowiedzialności oświadczam, że zapoznalam/em się z Zarządzeniem Nr 0050.199.2021 Burmistrza Bystrzycy Kłodzkiej z dnia 25 czerwca 2021 r. w sprawie wprowadzenia Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka, zawierającym ww. dokumenty w formie załączników do zarządzenia i zobowiązuję się do przestrzegania wynikających z nich zasad.

Oświadczam również, że:

1) Zapoznałem (am) się z aktualnymi przepisami dotyczącymi ochrony danych osobowych i zobowiązuję się do ich przestrzegania.
2) Jednocześnie w czasie wykonywania swoich obowiązków służbowych zobowiązuję się do:
3) zapewnienia ochrony danym osobowym przetwarzanym w zbiorach Urzędu Miasta i Gminy Bystrzyca Kłodzka, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnianiem osobom trzecim i nieuprawnionym, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem;
4) zachowania w tajemnicy informacji związanych przetwarzaniem danych osobowych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka;
5) zachowania w tajemnicy, także po ustaniu stosunku pracy, wszelkich informacji dotyczących funkcjonowania systemów lub urządzeń służących do przetwarzania danych osobowych w zbiorach Urzędu Miasta i Gminy Bystrzyca Kłodzka;
6) zachowania w tajemnicy haseł dostępu do systemów informatycznych, przetwarzających dane osobowe w Urzędzie Miasta i Gminy Bystrzyca Kłodzka, również po upływie ich ważności;
7) natychmiastowego zgłaszania przełożonemu i Inspektorowi Ochrony Danych podejrzenia na swoim stanowisku pracy próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa zbioru lub systemu informatycznego, w którym przetwarzane są dane osobowe.
8) Zostałem(am) poinformowany(a) o odpowiedzialności służbowej i karnej w przypadku naruszenia przepisów dotyczących ochrony danych osobowych.

Przyjmuję do wiadomości i stosowania
Data i podpis osoby upoważnionej:

Wykaz osób upoważnionych do przetwarzania danych osobowych

L.p.	Nr upoważnienia	Imię i nazwisko upoważnionej osoby	Stanowisko	Zakres	Data udzielenia upoważnienia	Data ustania upoważnienia
1.						
2.						
3.						
4.						

WYKAZ PODMIOTÓW KTÓRYM POWIERZONO PRZETWARZANIE DANYCH OSOBOWYCH

L.p.	**Nazwa podmiotu, któremu powierzono dane**	**Data powierzenia**	**Cel powierzenia oraz numer umowy powierzenia**	**Zakres powierzonych danych** *(jakie dane zostały powierzone)*	**Określenie zbioru/zasobu**
1.					
2.					
3.					

DZIENNIK UCHYBIEŃ I ZAGROŻEŃ

Kod	Data i godzina zdarzenia	Rodzaj zdarzenia (uchybienie lub zagrożenie)	Opis zdarzenia	Skutki zdarzenia	Działania naprawcze	Podpis IOD

PROTOKÓŁ UCHYBIENIA

Data i godzina wystąpienia uchybienia

……

Kod uchybienia

……

Opis uchybienia

……
……
……
……
……
……

Przyczyny powstania uchybienia

……
……
……
……
……
……

Zaistniałe skutki uchybienia

……
……
……
……
……

Podjęte działania naprawczo-zapobiegawcze

……
……
……
……
……

Inspektor Ochrony Danych

……

Administrator Danych Osobowych

……

PROTOKÓŁ ZAGROŻENIA

Data i godzina wystąpienia zagrożenia

……..

Kod zagrożenia

……..

Opis zagrożenia

……
……
……
……
……
……

Przyczyny powstania zagrożenia

……
……
……
……
……
……

Zaistniałe skutki zagrożenia

……
……
……
……
……

Podjęte działania naprawczo-zapobiegawcze

……
……
……
……
……

Inspektor Ochrony Danych

……

Administrator Danych Osobowych

……

Bystrzyca Kłodzka, dnia roku

WNIOSEK
o nadanie uprawnień do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka

Na podstawie na art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) oraz Ustawy o Ochronie Danych Osobowych z dnia 10 maja 2018 r. (Dz.U. 2019 poz. 1781 t.j.) wnioskuję o

nadanie Pani/Panu* **imię i nazwisko**

stanowisko

1. uprawnień do przetwarzania danych osobowych w następujących zbiorach danych osobowych o numerze w rejestrze:

2. w systemie informatycznym uprawnienia do przetwarzania danych w programie:

Proszę o upoważnienie w/w pracownika od dnia ... w powyższym zakresie.

.....

(podpis wnioskodawcy)

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH PROWADZONY PRZEZ ADMINISTRATORA

na podstawie art. 30, ust. 1 RODO

Pozycja Rejestru		
L.p.	**Nazwa czynności przetwarzania**	
1.	**Jednostka przetwarzająca/ stanowisko**	
2.	**Dane administratora danych**	
3.	**Dane inspektora ochrony danych**	
4.	**Nazwa współadministratora**	
5.	**Cel przetwarzania**	
6.	**Kategorie osób**	
7.	**Kategorie danych**	
8.	**Podstawa prawna**	
9.	**Źródło danych**	
10.	**Planowany termin usunięcia kategorii danych**	
11.	**Dane podmiotu przetwarzającego**	
12.	**Kategorie odbiorców**	
13.	**Nazwa systemu lub oprogramowania**	
14.	**Opis technicznych i organizacyjnych środków bezpieczeństwa**	
15.	**Transfer do kraju trzeciego lub organizacji międzynarodowej**	

WYKAZ UDOSTĘPNIEŃ DANYCH OSOBOWYCH OSOBOM KTÓRYCH DOTYCZĄ

L.p.	Imię i nazwisko osoby, której dane są udostępniane	Data udostępnienia	Poz. w rejestrze czynności przetwarzania danych osobowych
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Załącznik nr 2 do Zarządzenia Nr 0050.199.2021 Burmistrza Bystrzycy Kłodzkiej z dnia 25 czerwca 2021 r. w sprawie wprowadzenia Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIASTA I GMINY BYSTRZYCA KŁODZKA

Spis treści

ROZDZIAŁ I – INFORMACJE OGÓLNE

§ 1

Na podstawie:

1. Ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U. 2019 poz.1781t.j.);
2. 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. 2016 z roku, poz. 113 ze zm.);
3. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. UE L 119 z 4 maja 2016 r., Polskie Wydanie Specjalne 2016 t.59);

ustanawia się **Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka.**

§ 2

Przez użyte w niniejszym dokumencie określenia należy rozumieć:

1. **IOD** – Inspektor Ochrony Danych;
2. **ASI** – Administrator Systemów Informatycznych;
3. **ADO** – Administrator Danych Osobowych;
4. **Baza danych osobowych** – zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane osobowe;
5. **Urząd** – Urząd Miasta i Gminy Bystrzyca Kłodzka;
6. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, uwierzytelniający osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
7. **Identyfikator Użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika);
8. **Instrukcja** – niniejszy dokument;
9. **Kopia pełna** – kopię zapasową całości danych osobowych przetwarzanych w systemie informatycznym;
10. **Niezgodność** – niespełnienie wymagania, czyli potrzeby lub oczekiwania, które zostało ustalone, przyjęte zwyczajowo lub jest obowiązkowe;
11. **Nośniki danych** – płyty CD lub DVD, pamięć Flash, dyski twarde lub inne urządzenia/materiały służące do przechowywania plików z danymi;

12. **Polityka Bezpieczeństwa (PB)** – przyjęty do stosowania dokument o nazwie: Polityka Bezpieczeństwa Urzędu Miasta i Gminy Bystrzyca Kłodzka;
13. **Przetwarzane danych** – wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemie informatycznym;
14. **Raport** – przygotowane przez system informatyczny zestawienie zakresu i treści przetwarzanych danych;
15. **Rozporządzenie** – odpowiednio użyte w tekście rozporządzenie, o którym mowa w § 1 niniejszego rozdziału;
16. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
17. **Serwisant** – firma lub pracownik firmy zajmujący się instalacją, naprawą i konserwacją sprzętu komputerowego;
18. **Sieć publiczna** – sieć telekomunikacyjna wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;
19. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
20. **Użytkownik** – upoważniony przez ADO wyznaczony do przetwarzania danych osobowych pracownik, który odbył stosowne szkolenie w zakresie ochrony tych danych na wniosek bezpośredniego przełożonego;
21. **Ustawa** – odpowiednio użytą w tekście ustawę, o której mowa w § 1 niniejszego rozdziału;
22. **Zarządzenie** – aktualne Zarządzenie Burmistrza Bystrzycy Kłodzkiej w sprawie Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym w Urzędzie Miasta i Gminy Bystrzyca Kłodzka;
23. **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
24. **Wydział** – komórka organizacyjna Urzędu.

§ 3

1. ASI wyznaczany jest przez ADO drogą pisemnego upoważnienia i polecenia przetwarzania danych. W przypadku niewyznaczenia ASI, jego funkcję pełni ADO.
2. ASI jest również zobowiązany do podpisania oświadczenia o zachowaniu poufności.
3. Podczas nieobecności ASI jego funkcję pełni upoważniony przez Burmistrza zastępca.

§ 4

1. Wszyscy Użytkownicy przetwarzający dane osobowe w systemie informatycznym stosowanym w Urzędzie Miasta i Gminy Bystrzyca Kłodzka są odpowiedzialni za przestrzeganie zasad bezpieczeństwa przetwarzania danych osobowych.

2. Do obowiązków ASI należy kontrola przepływu informacji pomiędzy systemami informatycznymi a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej i systemu informatycznego.
3. ASI odpowiada za wdrożenie systemu zarządzania bezpieczeństwem systemów informatycznych, o którym mowa w § 20 KRI (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).
4. Obowiązkiem ASI jest również zabezpieczenie użytkowanego sprzętu komputerowego przed nieuprawnionym dostępem oraz przeprowadzanie analizy ryzyka uwzględniającej realne zagrożenia dla systemu informatycznego.
5. Rolą IOD jest monitorowanie stanu prawnego i wsparcie ASI w zakresie spełnienia wymogów prawnych. IOD na żądanie ADO i ASI dokonuje oceny planowanych lub przyjętych środków pod kątem ich zgodności z przepisami prawa.

§ 5

Zgodnie z rozporządzeniem, uwzględniając fakt, że użytkowany w Urzędzie Miasta i Gminy Bystrzyca Kłodzka system informatyczny służący do przetwarzania danych osobowych jest połączony z siecią Internet, wprowadza się wysoki poziom bezpieczeństwa.

ROZDZIAŁ II – INFORMACJE SZCZEGÓŁOWE

§ 6

Procedury nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemie informatycznym stosowanym w Urzędzie określa się w sposób następujący:

1. Kierownicy komórek organizacyjnych Urzędu zostali upoważnieni i zobowiązani przez ADO do wnioskowania o nadawanie, zmianę oraz odwoływanie uprawnień. Wszelkie wnioski w tym zakresie winny być kierowane do ADO za pośrednictwem IOD. ADO może w każdym czasie nadawać, zmieniać oraz odwoływać upoważnienia do przetwarzania danych osobowych. W przypadku samodzielnych stanowisk o uprawnienia i ich zmianę oraz odwołanie wnioskuje bezpośredni przełożony. Po nadaniu upoważnienia IOD jest zobowiązany do przekazania zakresu upoważnienia Użytkownika do ASI. Ciężar obowiązku wnioskowania do ADO o nadawanie, zmianę oraz odwoływanie uprawnień leży wyłącznie po stronie bezpośrednich przełożonych.
2. ASI przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia do przetwarzania danych osobowych nadanego przez Administratora Danych Osobowych, określającego zakres uprawnień Użytkownika.
3. Po pozytywnym zweryfikowaniu upoważnienia, ASI zobowiązany jest niezwłocznie przydzielić Użytkownikowi identyfikator i hasło. Podanie użytkownikowi hasła nie może nastąpić w sposób umożliwiający zapoznanie się z nim osobom trzecim.

4. Użytkownikom nadawane są uprawnienia do prac tylko w modułach i funkcjach programu wymaganych dla realizacji powierzonych im zadań.
5. Użytkownik systemu informatycznego ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
6. W przypadku wygaśnięcia przesłanek uprawniających Użytkownika do przetwarzania danych osobowych, w szczególności odwołania upoważnienia do ich przetwarzania, ASI zobowiązany jest do dopełnienia czynności uniemożliwiających ponowne wykorzystanie identyfikatora użytkownika, którego uprawnienia wygasły. Kierownicy komórek organizacyjnych (bezpośredni przełożeni użytkownika) są zobligowani do odwoływania upoważnień, o czym pisemnie powiadamiają IOD i ASI. Obligatoryjnie w powiadomieniu należy wskazać datę ustania uprawnień.
7. Wyłączenie użytkownika z ewidencji osób upoważnionych do przetwarzania informacji obliguje ASI do zablokowania go we wszystkich systemach informatycznych, do których miał dostęp.
8. ASI dysponuje wykazem identyfikatorów przekazanych poszczególnym pracownikom, który wiąże identyfikator z imiennie wskazanym pracownikiem.
9. Hasło składa się z co najmniej 8 znaków (liter, cyfr i znaków specjalnych).
10. Osobą odpowiedzialną za przydział identyfikatora i pierwszego hasła jest ASI.
11. Użytkownik jest zobowiązany do zabezpieczenia swojego hasła przed nieuprawnionym dostępem osób trzecich.
12. W przypadku nieumyślnego ujawnienia hasła osobie nieuprawnionej lub podejrzenia ujawnienia, należy bezzwłocznie dokonać zmiany hasła na nowe.
13. Kolejne hasła zmienia sam użytkownik, chyba, że użytkowany system sam wymusza jego zmianę.
14. Identyfikatory dla użytkowników przydziela ASI. Identyfikator po wylogowaniu danej osoby z systemu, nie może być przydzielony innemu użytkownikowi.
15. Użytkownik ponosi odpowiedzialność za czynności wykonywane w systemie przy użyciu identyfikatora i hasła, którymi się posługuje lub posługiwał.

§ 7

1. Zarejestrowanie użytkownika w systemie wymaga spełnienia następujących warunków:
   a) zgłoszenie pisemne przez bezpośredniego przełożonego do IOD konieczności dostępu do przetwarzania danych osobowych w konkretnych zbiorach (zgodnie z zajmowanym stanowiskiem i zakresem obowiązków);
   b) podpisanie przez osobę, ubiegającą się o dostęp, oświadczenia dotyczącego zapoznania się z obowiązującymi przepisami o ochronie danych osobowych oraz z aktualnym Zarządzeniem Burmistrza Bystrzycy Kłodzkiej w sprawie wprowadzenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka oraz zobowiązania do zachowania w tajemnicy informacji związanych z ich przetwarzaniem wydania przez Administratora (lub osobę upoważnioną).
   c) upoważnienia i polecenie dla użytkownika do dostępu i przetwarzania danych osobowych.

2. Z chwilą zarejestrowania w systemie użytkownik jest informowany przez ASI o ustalonym dla niego identyfikatorze i obowiązku posługiwania się hasłem dostępu.
3. Dokumenty, o których mowa w ust. 1 podlegają przechowaniu:
   a) oryginał oświadczenia osoby ubiegającej się o dostęp przechowuje się w aktach osobowych pracownika i w aktach IOD (w przypadku osoby niebędącej pracownikiem Urzędu – w dokumentach tej osoby, przechowywanych u pracownika odpowiedzialnego za kadry;
   b) upoważnienia do dostępu i przetwarzania danych przechowuje się w aktach osobowych pracownika (w przypadku osoby niebędącej pracownikiem Urzędu – w dokumentach tej osoby), przechowywanych u pracownika odpowiedzialnego za kadry (ASI i IOD jeśli uznają to za potrzebne, mogą dysponować kopiami dokumentów wskazanych w pkt 1 i 2.
4. W przypadku konieczności powierzenia przetwarzania danych osobowych innemu podmiotowi, Administrator zawiera z tym podmiotem umowę na piśmie.
5. Podmiot, z którym zawarta jest umowa może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie;
6. Umowa sporządzana jest w dwóch egzemplarzach: jeden dla podmiotu, drugi dla Administratora. Kierownicy Wydziałów zobowiązani są zgłaszać wszelkie umowy powierzenia do IOD, który prowadzi ich rejestr. Obowiązek zgłaszania dotyczy również samodzielnych stanowisk pracy.
7. Oświadczenie, o którym mowa w ust. 1 pkt 2 składają wszyscy pracownicy Urzędu oraz inne osoby, które mogą mieć dostęp do danych osobowych nawet, jeśli nie ubiegają się o upoważnienie do przetwarzania danych osobowych w Urzędzie. Za realizację obowiązku odpowiada Wydział Organizacyjno-Prawny.
8. Użytkownika wyrejestrowuje się z systemu na zgłoszenie przełożonego – po utracie uprawnień dostępu do przetwarzania danych, co może mieć miejsce w sytuacjach:
   a) ustania zatrudnienia użytkownika;
   b) zmiany zakresu obowiązków użytkownika;
   c) zakończeniu umowy - w przypadku osoby niebędącej pracownikiem Urzędu (np. praktykant, stażysta, umowa cywilnoprawna).
9. Rozwiązanie umowy o pracę lub zaistnienie okoliczności zawartych w ust. 8 pkt 2 i 3, powoduje utratę dostępu do przetwarzania danych i niezwłoczne wyrejestrowanie użytkownika z systemu, odnotowanie w ewidencji osób upoważnionych do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Bystrzyca Kłodzka oraz unieważnienie jego hasła i identyfikatora. Przełożeni użytkowników zobowiązani są do poinformowania IOD i ASI w przypadku zaistnienia okoliczności, o których mowa w ust.8.
10. Uprawnienia administratora systemów w Urzędzie posiada ASI, a w przypadku jego nieobecności inna osoba upoważniona przez Administratora Danych.
11. Hasła administratora systemów przechowywane są w dokumentacji ASI, zachowując zasady określone w niniejszej instrukcji.
12. Awaryjne użycie haseł administratora systemów może być wykonane wyłącznie przez Administratora Danych lub inna osobę upoważnioną.
13. Z każdorazowego awaryjnego użycia haseł administratora sporządzana jest notatka.

§ 8

1. Czas trwania nieaktywnej sesji (czas bezczynności) po jakim następuje automatyczne wylogowanie Użytkownika wynosi maksymalnie 15 minut.
2. Uruchomienie wygaszacza ekranu wiąże się z koniecznością ponownego zalogowania, celem wznowienia pracy stacji roboczej.

ROZDZIAŁ III – KONFIGURACJA SPRZĘTU KOMPUTEROWEGO UŻYTKOWNIKA SYSTEMU

§ 9

1. Komputer Użytkownika powinien posiadać oprogramowanie antywirusowe, którego sygnatury wirusów powinny być aktualizowane na bieżąco. Oprogramowanie antywirusowe powinno być stale aktywne.
2. W przypadku niesprawdzenia przez użytkownika systemu pliku dostarczonego z zewnątrz, oprogramowanie antywirusowe automatycznie chroni system poprzez monitorowanie plików w stanie rzeczywistym. W przypadku wykrycia zagrożenia, oprogramowanie stosownie reaguje na to zagrożenie.
3. Użytkownik jest zobowiązany do stałego monitorowania komunikatów pochodzących z oprogramowania antywirusowego zainstalowanego na stacji roboczej i reagowania na nie.
4. Komputer Użytkownika powinien być chroniony zaporą sieciową (firewall).
5. Oprogramowanie komputera powinno być regularnie aktualizowane, w szczególności dotyczy to systemu operacyjnego.
6. Użytkownik nie może w sposób samodzielny tj. bez uzgodnienia z ASI instalować żadnych programów komputerowych na sprzęcie służbowym.
7. Wszelkie sprawy związane z oprogramowaniem na komputerze służbowym winne być zgłaszane Administratorowi Systemów Informatycznych.

ROZDZIAŁ IV – ROZPOCZYNANIE, ZAWIESZANIE I KOŃCZENIE PRACY

§ 10

1. Użytkownik rozpoczynający pracę zobowiązany jest przestrzegać procedur, które mają na celu sprawdzenie zabezpieczenia pomieszczenia, w którym przetwarzane są dane osobowe, swojego stanowiska pracy oraz stanu sprzętu komputerowego, a w szczególności:
   a) przed wejściem do pomieszczenia sprawdzić czy na drzwiach i zamkach nie ma widocznych śladów prób niepowołanego ich otwierania;
   b) sprawdzić stan okien i krat (jeśli są w danym pomieszczeniu) oraz ocenić,
   c) czy w pomieszczeniu nie ma znaków wskazujących na pobyt w nim osób nieuprawnionych;
   d) sprawdzić stan sprzętu informatycznego oraz zamknięcie szaf i biurek.
2. Użytkownik przed przystąpieniem do przetwarzania danych powinien zalogować się w systemie, posługując się swoim identyfikatorem i hasłem. Po zalogowaniu się należy ocenić pracę systemu i stan przetwarzanych danych.
3. Użytkownik w czasie pracy powinien stosować zasady zapewniające bezpieczeństwo przetwarzania danych osobowych w systemie:

a) ustawić ekrany monitorów w pomieszczeniach tak, aby uniemożliwiać podgląd osób nieuprawnionych lub w przypadku niemożliwości zastosowanie filtra prywatyzującego;
b) dopilnować aby w pomieszczeniach, stanowiących obszar przetwarzania danych osobowych przebywały osoby trzecie, tylko za zgodą przełożonych i w obecności osób uprawnionych;
c) stosować urządzenia zabezpieczające przed utratą danych, spowodowaną awarią zasilania lub zakłóceniami w sieci elektrycznej. Potrzeby w tym zakresie zgłaszają pisemnie do ASI – przełożeni Użytkownika;
d) jeżeli użytkownik komputera na stanowisku jest zalogowany do systemu i nie wykazuje aktywności przez okres dłuższy niż 15 minut, następuje jego blokada, odblokowanie jest możliwe po podaniu aktualnego hasła użytkownika
e) stosować tzw. wygaszacze ekranów, które włączają się po upływie 15 minut bezczynności komputera.

4. Po zakończeniu pracy użytkownik powinien przestrzegać następujących zasad:
   a) wylogować się z systemu i zaczekać na jego wyłączenie się;
   b) sprawdzić czy nie zostały pozostawione bez nadzoru nośniki informacji;
   c) upewnić się, że szafy i biurka z dokumentacją są zamknięte;
   d) wyłączyć odbiorniki energii elektrycznej, zamknąć pomieszczenie i klucze oddać
   e) w wyznaczone miejsce, zgodnie z obowiązującą instrukcją postępowania z kluczami dostępu do pomieszczeń w Urzędzie;
   f) Po godzinach pracy Administrator lub osoba upoważniona przez niego zapewnia monitorowanie lub fizyczną ochronę pomieszczeń, w których przetwarzane są dane osobowe.
5. W przypadku stwierdzenia przez użytkownika prób niepowołanego naruszenia urządzeń, zawartość zbiorów danych, ujawnione metody pracy lub sposób działania programu mogą wskazywać na naruszenie danych osobowych – postępuje zgodnie z Procedurą postępowania w sytuacji podejrzenia naruszenia danych osobowych, zawartą w Polityce Bezpieczeństwa.
6. Rozpoczynając pracę użytkownik powinien zwrócić szczególną uwagę na okoliczności, o których mowa w ust. 1 i przypadku ich zaistnienia natychmiast informować IOD i przełożonego.

ROZDZIAŁ V – ZABEZPIECZANIE DANYCH W SYSTEMIE

§ 11

1. Dane osobowe przetwarzane w systemie informatycznym Urzędu Miasta i Gminy Bystrzyca Kłodzka podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych.
2. Za tworzenie i przechowywanie kopii zapasowych w sposób zgodny z przepisami ustawy oraz niniejszej Instrukcji odpowiedzialny jest Administrator Systemów Informatycznych.
3. Stosuje się następujące procedury tworzenia oraz przechowywania kopii zapasowych baz danych:
   a) codziennie ASI wykonuje kopię przyrostową;
   b) raz tydzień ASI wykonuje kopię pełną;

c) system Acronis odpowiedzialny za wykonywanie kopii zapasowych kopii wirtualnych serwerów. Wykonywane są kopie zapasowe baz danych systemów informatycznych. Kopie zgrywane są na serwer oraz na urządzenie do wykonywania kopii Qnap znajdujące się na innej kondygnacji budynku Urzędu (serwerownia znajduje się na kondygnacji -1 , kopie zapasowe znajdują się na kondygnacji 2);

d) nośniki zawierające kopie zapasowe przechowywane są maksymalnie przez 5 lat, w wyznaczonym do tego celu pomieszczeniu, innym niż zbiory danych osobowych użytkowane na bieżąco;

e) w przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych, Użytkownicy systemu informatycznego zobowiązani są do przechowywania danych, tak aby możliwe było zabezpieczenie ich dostępności poprzez wykonanie kopii zapasowych.

4. ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność. ASI testuje kopie zapasowe posiadanych zasobów informacyjnych w celu zminimalizowania ryzyka utraty informacji.

§ 12

1. Elektroniczne nośniki informacji zawierające dane osobowe przechowywane są zgodnie z zasadami opisanymi w paragrafie 10 niniejszej instrukcji.
2. Dane są przechowywane przez okres, w którym istnieją przesłanki do ich przetwarzania.
3. Sprzęt komputerowy, na którego dyskach twardych zawarte są dane osobowe przechowywany jest w pomieszczeniach odpowiednio zabezpieczonych znajdujących się w obszarze przetwarzania danych osobowych.
4. Kopiowanie danych osobowych na nośniki informacji oraz wykonywanie wydruków jest zabronione chyba, że istnieje konieczność ich sporządzania, która wynika z nałożonych na użytkownika obowiązków i dozwolona jest przepisami prawa.
5. Wykorzystywanie nośników informacji lub wydruków w innym celu niż wskazany w ust. 5 jest zabronione.
6. Dane są przechowywane przez okres, w którym istnieją przesłanki do ich przetwarzania. Po ustaniu przesłanek do przetwarzania, dane muszą zostać usunięte w sposób uniemożliwiający ich odtworzenie.
7. Kopie zapasowe przechowuje ASI w miejscu, zapewniającym im odpowiednie warunki bezpieczeństwa.
8. Urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe przeznaczone do likwidacji pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe – uszkadza się w sposób uniemożliwiający ich odczytanie.
9. Zdezaktualizowane i uszkodzone kopie zapasowe należy mechanicznie niszczyć w sposób uniemożliwiający ich ponowne użycie.
10. Nie wolno sporządzać wydruków z kopii zapasowych i innych nośników informacji, które podlegają zniszczeniu.

§ 13

1. Systemy informatyczne zabezpieczone są przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego w następujący sposób:
   a) dane przetwarzane są przy użyciu systemów pracujących w wewnętrznej sieci oddzielonej fizycznie od sieci publicznej przy pomocy bramy internetowej wyposażonej w firewall;
   b) zastosowano działający w „tle" program antywirusowy na komputerach użytkowników.
2. Użytkownik ma obowiązek na bieżąco sprawdzać obecność wirusów komputerowych. Czynność ta powinna być zaprogramowana w systemie, który automatycznie sygnalizuje obecność wirusów, w trakcie włączania systemu lub wprowadzania danych z zewnętrznych nośników informacji.
3. Kontrola antywirusowa systemu obejmować powinna wszystkie nośniki magnetyczne i optyczne, służące zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
4. Obowiązkiem ASI jest dostarczanie, uaktualnianie i instalowanie nowego oprogramowania antywirusowego.
5. Instalację nowego oprogramowania systemowego oraz oprogramowania użytkowego, gwarantującego bezpieczeństwo przetwarzania danych osobowych wykonuje ASI lub osoba upoważniona przez Burmistrza.

§ 14

1. Instalację nowego oprogramowania systemowego oraz oprogramowania użytkowego, gwarantującego bezpieczeństwo przetwarzania danych osobowych wykonuje ASI lub osoba upoważniona przez Burmistrza.
2. Okresowe przeglądy i konserwacje sprzętu komputerowego, wynikające z eksploatacji, warunków zewnętrznych oraz ważności systemu dla funkcjonowania Urzędu, wykonuje ASI lub osoba upoważniona przez Burmistrza.
3. Bieżącą konserwację i naprawę sprzętu wykonuje ASI lub osoba upoważniona przez Burmistrza.
4. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do napraw w firmach zewnętrznych, pozbawia się przed naprawą zapisu danych osobowych albo naprawia się je pod nadzorem ASI.
5. W przypadku stwierdzenia przez ASI nieprawidłowości w działaniu elementów systemu opisanych w ust.1 pkt a, podejmuje on niezwłocznie czynności zmierzające do przywrócenia ich prawidłowego działania. IOD powiadamiany jest w przypadku wystąpienia podejrzenia naruszenia ochrony danych lub stwierdzenia naruszenia ochrony danych.
6. Jeżeli do przywrócenia prawidłowego działania systemu niezbędna jest pomoc podmiotu zewnętrznego, wszelkie czynności na sprzęcie komputerowym dokonywane w obszarze przetwarzania danych osobowych, powinny odbywać się w obecności ASI.
7. Stosuje się następujące procedury wykonywania przeglądów nośników informacji służących do przetwarzania danych:

a) Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające zapis danych osobowych przeznaczone do likwidacji należy pozbawić zapisu, a w przypadku, gdy nie jest to możliwe, uszkodzić mechanicznie w sposób uniemożliwiający ich odczytanie.

Podlegające likwidacji uszkodzone lub przestarzałe nośniki a w szczególności twarde dyski z danymi osobowymi ze stacji roboczych i laptopów / pendrive / pamięci flash / płyty DVD / telefony komórkowe / smartfony są niszczone w sposób fizyczny w tym również komisyjnie. Stosowana metoda niszczenia, to fizyczne niszczenie (pocięcie, nawiercenie, młotkowanie) wymontowanych nośników zmielenie w specjalistycznej firmie potwierdzone protokołem zniszczenia lub certyfikatem bezpieczeństwa firmy utylizacyjnej lub nagraniem z procesu transportu i utylizacji.

b) Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające zapis danych osobowych przeznaczone do przekazania innemu podmiotowi, który nie jest uprawniony do otrzymania takich danych, należy wcześniej pozbawić zapisów danych – postępując zgodnie z zasadami opisanymi w niniejszej instrukcji.

§ 15

1. System informatyczny służący do przetwarzania danych osobowych jest zabezpieczony przed utratą danych spowodowaną awarią lub zakłóceniami w sieci poprzez stosowanie:
   a) Centralnego UPS o odpowiednich parametrach;
   b) listew przepięciowych, połączonych pomiędzy siecią a komputerami;
   c) skrzynek rozdzielczych z bezpiecznikami.
2. Systemy informatyczne zabezpieczone są przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego w następujący sposób:
3. Użytkownik ma obowiązek na bieżąco sprawdzać obecność wirusów komputerowych. Czynność ta powinna być zaprogramowana w systemie, który automatycznie sygnalizuje obecność wirusów, w trakcie włączania systemu lub wprowadzania danych z zewnętrznych nośników informacji. Kontrola antywirusowa systemu obejmować powinna wszystkie nośniki magnetyczne i optyczne, służące zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
4. Obowiązkiem ASI jest dostarczanie, uaktualnianie i instalowanie nowego oprogramowania antywirusowego. Użytkownicy nie mogą instalować samodzielnie żadnego oprogramowania na sprzęcie służbowym, wszelkie zmiany wyłącznie za wiedzą ASI.
5. Instalację nowego oprogramowania systemowego oraz oprogramowania użytkowego, gwarantującego bezpieczeństwo przetwarzania danych osobowych wykonuje ASI, zastępca ASI lub inna osoba upoważniona przez Burmistrza.
6. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych.

§ 16

1. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   a) **likwidacji** – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
   b) **przekazania podmiotowi nieuprawnionemu do przetwarzania danych** – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
   c) **naprawy** – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ASI; (umowa powierzenia)
2. W celu usunięcia danych zapisanych na elektronicznych nośnikach, ASI może dokonać ich fizycznego uszkodzenia w taki sposób, by nie istniała możliwość odtworzenia zapisanych na nich danych.
3. Zabronione jest, aby Użytkownik wynosił poza swoje miejsce przydzielone przez Administratora, w szczególności poza pomieszczenia lub budynki Administratora, jakichkolwiek dokumentów i sprzętu IT wytworzonych u Administratora zawierających dane osobowe, chyba że Administrator wyrazi na to konkretnej osobie indywidualną zgodę na wynoszenie dokumentacji.

§ 17

1. Stosuje się następującą procedurę w przypadku stwierdzenia naruszenia zasad bezpieczeństwa systemu informatycznego:
   a) w przypadku stwierdzenia przez Użytkownika naruszenia zabezpieczeń przez osoby nieuprawnione, jest on zobowiązany niezwłocznie poinformować o tym fakcie IOD;
   b) IOD jest zobowiązany niezwłocznie podjąć czynności zmierzające do ustalenia przyczyn naruszeń zasad bezpieczeństwa i zastosować środki uniemożliwiające ich naruszanie w przyszłości określone w Polityce Bezpieczeństwa;
   c) w przypadku wykrycia zagrożenia automatycznym działaniem, możliwe jest zablokowanie pracy w systemie do chwili podjęcia decyzji o sposobie postępowania;
   d) w celu minimalizacji zagrożeń dąży się, w miarę możliwości organizacyjnych, do maksymalnej unifikacji sprzętu działającego w systemie informatycznym, stosowanego oprogramowania, konfiguracji sprzętu i oprogramowania, a także rozwiązań organizacyjnych;
   e) w Urzędzie funkcjonuje zakaz samowolnego korzystania z prywatnych lub pochodzących ze źródła innego, niż miejsce pracy, nośników informacji (magnetycznych, optycznych, urządzeń podłączanych do stacji roboczych). Mechanizmem zapobiegającym zmaterializowaniu się ryzyka zainfekowania systemu oprogramowaniem złośliwym jest obowiązek regularnego poddania nośników informacji badaniu oprogramowaniem antywirusowym.

§ 18

2. W przypadku stwierdzenia:
   a) błędu użytkownika systemu – ASI przeprowadza dodatkowe szkolenie osób zatrudnionych przy przetwarzaniu danych w komórce organizacyjnej. ASI dokumentuje odbycie szkolenia;
   b) uaktywnienia wirusa – należy zgłosić ASI, który ustali źródło jego pochodzenia oraz uaktualni zabezpieczenia antywirusowe;
   c) zaniedbania ze strony użytkownika – należy w stosunku do niego zastosować konsekwencje wynikające z właściwych przepisów prawa;
   d) włamania, w celu nielegalnego pozyskania danych – należy dokonać szczegółowej analizy wdrożonych środków zabezpieczenia i zapewnić skuteczniejszą ochronę;
   e) złego stanu urządzenia lub złego działania programu – należy niezwłocznie powiadomić ASI i przeprowadzić kontrolę czynności serwisowo-programowych.

ROZDZIAŁ VI – POSTANOWIENIA KOŃCOWE

§ 19

Wprowadzanie do systemu informacji z zewnątrz jest dopuszczalne tylko przy stwierdzeniu legalności i wiarygodności źródeł informacji i przez użytkownika posiadającego uprawnienia, wynikające z zakresu jego obowiązków.

§ 20

Pomieszczenie, w którym znajdują się serwery systemów, jest wydzielone wyłącznie dla potrzeb systemów informatycznych. Dostęp do w/w pomieszczenia powinien mieć wyłącznie ASI oraz osoby upoważnione przez Burmistrza.

§ 21

1. Każdy pracownik zatrudniony przy przetwarzaniu danych osobowych w systemie, zobowiązany jest zapoznać się z niniejszą Instrukcją i stosować jej przepisy na swoim stanowisku pracy.
2. Nadużycie przez użytkownika postanowień niniejszej Instrukcji, może stanowić podstawę do pociągnięcia go do odpowiedzialności przewidzianej właściwymi przepisami prawa.

§ 22

W sprawach nieuregulowanych niniejszą Instrukcją, znajdują zastosowanie przepisy wymienione w § 1 pkt 1 – 6.

§ 23

Niniejszy dokument wchodzi w życie z dniem 1 lipca 2021 r.

Burmistrz
Bystrzycy Kłodzkiej
Renata Suma

.....

podpis Administratora Danych Osobowych