WÓJT GMINY
42-283 BORONÓW
ul. Dolna 2
Tel. 34 366 98 15, fax 34 366 98 14

ZARZĄDZENIE NR 6/2019
WÓJTA GMINY BORONÓW
z dnia 14 stycznia 2019 r.

w sprawie ustalenia Polityki Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Boronów oraz przyjęcia Instrukcji Zarządzania Systemem Informatycznym.

Na podstawie art. 24 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) zarządzam, co następuje:

§ 1

Ustala się „Politykę Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Boronów" zwaną dalej „Polityką", oraz „Instrukcję Zarządzania Systemem Informatycznym", zwaną dalej „Instrukcją", które stanowią załączniki do niniejszego zarządzenia.

§ 2

Zobowiązuje się pracowników Urzędu Gminy Boronów do stosowania zasad określonych w „Polityce" i „Instrukcji"

§ 3

Wszyscy pracownicy mają obowiązek zapoznać się z wymogami bezpieczeństwa zawartymi w „Polityce" oraz „Instrukcji". Zapoznanie się z wymogami bezpieczeństwa pracownik potwierdza podpisem.

§ 4

Wykonanie zarządzenia powierza się Inspektorowi Ochrony Danych

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Krzysztof Bełkot

Załącznik Nr 1
do Zarządzenia nr 6/2019
Wójta Gminy Boronów
z dnia 14 stycznia 2019 r.

Polityka bezpieczeństwa danych osobowych

w Urzędzie Gminy Boronów

1. Wstęp

Niniejszy dokument stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad bezpieczeństwa danych osobowych i informacji zgodnie z przepisami Rozporządzenia o ochronie danych osobowych UE z dnia 27 kwietnia 2016 r. (Dz.U.UE.L.2016.119.1) dla:

- Pracowników (Użytkowników) Urzędu Gminy Boronów,
- Pracowników podmiotów trzecich (Użytkowników), posiadających uprawniony dostęp do danych osobowych przetwarzanych przez Administratora danych/Podmiot przetwarzający,
- Użytkowników systemów informatycznych z uprawnionym dostępem do danych osobowych przetwarzanych przez Administratora danych/Podmiot przetwarzający.

Każda z w/w osób powinna zapoznać się z poniższym dokumentem oraz zobowiązać się do stosowania zasad w nim zawartych

2. Definicje

1) **Urząd** – w tym dokumencie jest rozumiany, jako Urząd Gminy Boronów, z siedzibą w Boronowie, ul. Dolna 2

2) **Administrator (danych)** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych – Administratorem (danych) w Urzędzie Gminy w Boronowie jest Wójt Gminy Boronów

3) **RODO** – Rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016)

4) **Dane osobowe** - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego, tożsamość tej osoby fizycznej.

5) **Użytkownik systemu** – osoba upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w urzędzie, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w urzędzie.

6) **Identyfikator użytkownika** – jest to ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

7) **Administrator systemu informatycznego** – pracownik odpowiedzialny za funkcjonowanie systemu teleinformatycznego, oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie. Powołany zarządzeniem Wójta Gminy Boronów.

8) **Przetwarzanie danych osobowych** to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

9) **Podmiotem danych** jest każda osoba fizyczna, której dane dotyczą.

10) **Podmiot przetwarzający** (Procesor) to jednostka lub inny podmiot przetwarzający dane osobowe w imieniu administratora.

11) **Inspektor Ochrony Danych Osobowych** (IODO) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/Podmiotowi

przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

12) **Poufność danych** – jest to właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

13) **Integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione, lub zniszczone w sposób nieautoryzowany.

14) **Rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

15) **Aplikacja** – program komputerowy wykonujący konkretne zadanie.

16) **Komórka organizacyjna** – rozumie się przez to referat, samodzielne stanowisko pracy.

17) **Sieć lokalna** – połączenie komputerów pracujących w urzędzie w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych.

18) **Sieć publiczna** – sieć telekomunikacyjna, niebędąca siecią wewnętrzną służąca do świadczenia usług telekomunikacyjnych w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (t.j. Dz.U.2018.1954 ze zm.).

19) **Sieć telekomunikacyjna** – urządzenia telekomunikacyjne zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci za pomocą przewodów, fal radiowych, bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j.Dz.U.2018.1954 ze zm.).

20) **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

21) **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

22) **Teletransmisja** – przesyłanie informacji za pomocą sieci telekomunikacyjnej.

3. Zadania Inspektora Ochrony Danych

1. Inspektor ochrony danych ma następujące zadania:

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

b) monitorowanie przestrzegania rozporządzenia (RODO), 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 zgodnie z art. 35 RODO.

d) współpraca z organem nadzorczym.

e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

f) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń, lub podejrzenia naruszenia zabezpieczeń.

g) nadzór nad prowadzeniem odpowiedniej dokumentacji.

2. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

4. Obszar przetwarzania danych osobowych

Dane osobowe przetwarzane są w budynku Urzędu Gminy w Boronowie, ul. Dolna 2, 42-283 Boronów

5. Do przetwarzania danych osobowych w systemie informatycznym urzędu stosuje się aplikacje:

1) System Adas - firmy Tensoft ,
2) System BDMB FK i Plan firmy BDMB Systemy Informatyczne,
3) Yuma Kadry Płace - firmy YUMA sp. z o.o. ,
4) Płatnik - firmy Asseco Poland SA – dostarczane przez Zakład Ubezpieczeń Społecznych,
5) Besti@ firmy Sputnik Software – dostarczane przez RIO,
6) SIO – dostarczany przez Ministerstwo Edukacji Narodowej,
7) Selwin, Uscwin, Rwwin firmy Aram sp. z o.o.,
8) System Wydawania Dowodów Osobistych firmy Wasko S.A. dostarczone przez MSWiA
9) HomeNet firmy SoftNet – oprogramowanie do przelewów dostarczone przez Bank Spółdzielczy

6. Przepływy między systemami:

Skąd	Dokąd	Kierunek przepływu danych osobowych	Sposób przesyłania danych osobowych
Systemy BDMB	Bestia	=>	eksport/import pliku
SELWIN	USCWIN	=>	eksport/import pliku

USCWIN	Główny Urząd Statystyczny	=>	transmisja bezpośrednio z programu lub poprzez dedykowany do tego portal GUS
SELWIN	Portal Informacyjny Administracji	<=>	eksport/import pliku poprzez portal MSWIA
System ADAS	Główny Urząd Statystyczny	=>	eksport pliku poprzez portal GUS

Pozostałe programy działają niezależnie w oparciu o własne bazy danych i nie posiadają wbudowanego mechanizmu umożliwiającego przepływ danych osobowych między innymi systemami informatycznymi stosowanymi w Urzędzie Gminy Boronów.

7. Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i wyćwiczalności danych przetwarzanych w systemie

a. Środki ochrony fizycznej

Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami patentowymi. Dostęp do pokoi jest kontrolowany za pomocą wydawania kluczy tylko osobom uprawnionym. Zastosowano szafę stalową do przechowywania nośników z kopiami zapasowymi zawierających dane osobowe.

b. Środki sprzętowe, informatyczne i telekomunikacyjne

Stosuje się niszczarki dokumentów oraz niszczarkę płyt CD.

Urządzenia wchodzące w skład infrastruktury sieciowej, serwera oraz komputery, na których przetwarzane są dane osobowe podłączone są do lokalnych awaryjnych zasilaczy UPS, zabezpieczających przed skokami napięcia i zanikiem zasilania.

Sieć lokalna skonfigurowana jest w topologii gwiazdy.

Sieć lokalna podłączona jest do Internetu poprzez router spełniający jednocześnie funkcję sprzętowego, zewnętrznego firewalla filtrującego dane przechodzące pomiędzy siecią lokalną i siecią publiczną.

Kopie zapasowe wykonywane są zgodnie z instrukcją zarządzania systemem informatycznym.

c. Środki ochrony w ramach oprogramowania urządzeń teletransmisji:

Na komputerach użytkowników systemu działa program antywirusowy.

Na komputerach użytkowników systemu działa programowy firewall.

Dostęp do komputerów i serwerów zawierających dane osobowe zabezpieczony jest hasłem.

d. Środki ochrony w ramach oprogramowania systemu:

Dostęp do baz danych osobowych zastrzeżony jest wyłącznie dla uprawnionych pracowników.

System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu odrębnie dla każdego pracownika. Zastosowano działający w tle program antywirusowy na komputerach użytkowników.

e. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych.

Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji. Dla każdego użytkownika systemu wyznaczony jest odrębny identyfikator. Użytkownicy mają dostęp do aplikacji umożliwiający dostęp tylko do tych danych osobowych, do których mają uprawnienia.

f. Środki ochrony w ramach systemu użytkowego.

Komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem uruchomieniowym. Zastosowano wygaszenie ekranu w przypadku dłuższej nieaktywności użytkownika. Zastosowano blokadę hasłem podczas dłuższej nieaktywności użytkownika.

g. Środki organizacyjne.

Wyznaczono Inspektora Ochrony Danych. Tymczasowe wydruki z danymi osobowymi są po ustaleniu ich przydatności niszczone. Do przetwarzania danych osobowych przy użyciu systemu informatycznego dopuszczane są osoby na podstawie indywidualnego pozwolenia na dostęp do przetwarzania danych osobowych wydawanego przez Administratora Danych Osobowych.

Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane są do zachowania ich w tajemnicy.

Osoby przetwarzające dane osobowe są przed dopuszczeniem ich do tych danych szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych w systemie informatycznym.

Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.

Ustalono Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.

Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych.

W przypadku, gdy zachodzi konieczność naprawy sprzętu poza siedzibą urzędu, należy wymontować z niego nośniki informacji zawierające dane osobowe.

8. Postanowienia końcowe

1. Za nadzór nad przestrzeganiem Polityki odpowiada bezpośredni przełożony Użytkownika.
2. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
3. Naruszając zapisy Polityki Użytkownik podlega sankcjom dyscyplinarnym, które regulują przepisy prawa.

9.Załączniki

a. Załącznik Nr 1 Wzór wykazu osób, które zostały zapoznane z „Polityką Ochrony Danych Osobowych w Urzędzie Gminy Boronów" oraz „Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Boronów".

b. Załącznik Nr 2 Wzór upoważnienia imiennego do przetwarzania danych osobowych.

c. Załącznik Nr 3 Wzór wykazu osób upoważnionych do przetwarzania danych osobowych w Urzędzie Gminy Boronów.

WÓJT

Krzysztof Bełkot

Załącznik Nr 1
do „Polityki bezpieczeństwa danych osobowych
w Urzędzie Gminy Boronów"

WZÓR

Wykaz osób, które zostały zapoznane z „Polityką ochrony danych osobowych w Urzędzie Gminy Boronów" oraz „Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Boronów"

L.p.	Imię i nazwisko	Stanowisko	Data	Podpis

Załącznik Nr 2
do „Polityki bezpieczeństwa
danych osobowych
w Urzędzie Gminy Boronów"

WZÓR

....., dn. ..... 20..... r.

UPOWAŻNIENIE

DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej RODO – nadaję upoważnienie Pani/Panu:

.....

(imię i nazwisko)

.....

(stanowisko)

do przetwarzania danych osobowych zgodnie z powierzonym zakresem czynności. Upoważnienie obejmuje uprawnienie do przetwarzania danych w okresie zatrudnienia.

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, ustawy z dnia z dnia 10 maja 2018 r. o ochronie danych osobowych, Kodeksu pracy, a także z Polityką bezpieczeństwa danych osobowych i Instrukcją zarządzania systemami informatycznymi.

Jednocześnie upoważniam Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w Urzędzie Gminy Boronów.

.....

podpis osoby uprawnionej do nadania upoważnienia

Załącznik Nr 3
do „Polityki bezpieczeństwa
danych osobowych
w Urzędzie Gminy Boronów"

WZÓR

Ewidencja osób upoważnionych do przetwarzania danych osobowych w Urzędzie Gminy Boronów

L.p	Identyfikator użytkownika*	Imię i nazwisko	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania upoważnienia
1				
	Zmiany danych			
2				
	Zmiany danych			
3				
	Zmiany danych			
4				
	Zmiany danych			

Załącznik Nr 2
do Zarządzenia nr 6/2019
Wójta Gminy Boronów
z dnia 14 stycznia 2019 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

W

URZĘDZIE GMINY

BORONÓW

Informacje podstawowe.

§ 1

Niniejsza „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" zwana dalej instrukcją, jest dokumentem wewnętrznym wydanym przez Wójta Gminy Boronów i ma zastosowanie do przetwarzania danych osobowych w systemie informatycznym Urzędu Gminy Boronów, w celu bezpiecznego ich przetwarzania.

§ 2

1. Instrukcja określa ogólne zasady i tryb postępowania Administratora Danych oraz wszystkich użytkowników przetwarzających dane osobowe w systemie informatycznym Urzędu Gminy Boronów.
2. Podstawę prawną do niniejszej instrukcji stanowią:
    1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1)
    2) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000)

§ 3

1. Każdy pracownik Urzędu Gminy Boronów 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.
3. Inspektor Ochrony Danych lub Administrator Systemu Informatycznego ma prawo do monitorowania pracy urządzeń przyłączonych do sieci informatycznej pod kątem przesyłania i przetwarzania danych, rejestracji zdarzeń związanych z przesyłaniem i przetwarzaniem danych w oprogramowaniu oraz prawidłowości wykorzystania powierzonego użytkownikom sprzętu i oprogramowania.

§ 4

Określenia i skróty użyte w instrukcji oznaczają:

1. **Administrator (danych)** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych – Administratorem (danych) w Urzędzie Gminy w Boronowie jest Wójt Gminy Boronów.
2. **Inspektor Ochrony Danych Osobowych** (IODO) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/Podmiotowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

3. **Administrator Systemów Informatycznych,** zwany dalej **ASI** – osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych. W Urzędzie Gminy Boronów funkcję tą pełni **Informatyk**.
4. **System informatyczny -** sieć teleinformatyczna, stacje robocze, serwery, oraz wszelkie inne urządzenia na których można przetwarzać dane wykorzystywane do pracy Urzędzie Gminy Boronów, a także wszelkie oprogramowanie dostępne w lokalnej sieci komputerowej lub zainstalowanych na poszczególnych stacjach roboczych, zlokalizowanych w budynkach Urzędu Gminy w Boronowie ul. Dolna 2.
5. **Bezpieczeństwo systemu informatycznego** – wdrożenie przez ADO lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem.
6. **Przetwarzanie danych osobowych** to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.
7. **Osoba upoważniona lub użytkownik systemu** – osoba posiadająca upoważnienie wydane przez ADO lub uprawnioną przez niego osobę i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej, zwana dalej użytkownikiem.
8. **Osoba uprawniona** – osoba posiadająca upoważnienie wydane przez ADO do wykonywania w jego imieniu określonych czynności.
9. **Obszar przetwarzania danych osobowych** – budynek Urzędu Gminy w Boronowie

§ 5

Określenie sposobu przydziału haseł dla użytkowników i częstotliwość ich zmian.

1. Dla każdego użytkownika systemu informatycznego, w którym przetwarzane są dane osobowe, administrator bezpieczeństwa informacji ustala identyfikator i hasło.
2. W celu zapewnienia wysokiego poziomu bezpieczeństwa hasło musi zawierać co najmniej 8 znaków i zawierać jednocześnie duże i małe litery oraz cyfry lub znaki specjalne.
3. Hasło jest wpisywane i przechowywane w systemie informatycznym w postaci zaszyfrowanej.
4. Zmiany hasła dokonuje użytkownik .
5. Hasło użytkownika systemu musi być zmienianie nie rzadziej niż raz na 30 dni. W przypadku gdy użytkownik systemu informatycznego nie korzysta z danego systemu przez okres dłuższy niż 30 dni hasło musi zostać zmienione podczas najbliższego ponownego zalogowania. Każdorazowo po zmianie hasła użytkownik systemu zobowiązany jest zapisać nowe hasło , umieścić je w zaklejonej kopercie opatrzonej imieniem, nazwiskiem oraz datą zmiany i w tym samym dniu kopertę przekazać ASI.

6. Hasła użytkownika, umożliwiające dostęp do systemu informatycznego, utrzymywane są w tajemnicy, a po upływie ich ważności niszczone. ASI prowadzi rejestr w którym użytkownicy potwierdzają przekazanie haseł, zaś otrzymane zaklejone koperty z bieżącymi hasłami przechowuje w zamkniętej metalowej szafie.
7. Hasła użytkowników mogą zostać użyte jedynie w sytuacji awaryjnej i po bezpośredniej dyspozycji wydanej przez ADO.
8. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.
9. Hasło użytkownika, który utracił uprawnienia dostępu do danych osobowych unieważnia się bezzwłocznie oraz podejmuje inne niezbędne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych
10. Osobą odpowiedzialną za prawidłowe funkcjonowanie mechanizmów zawartych w § 5 jest ASI.
11. Użytkownik ponosi odpowiedzialność za czynności wykonane w systemie przy użyciu identyfikatora i hasła, którymi się posługuje lub posługiwał. Użytkownik zobowiązany jest do utrzymania haseł dostępu w tajemnicy, a w szczególności do dołożenia starań w celu uniemożliwienia zapoznania się z nimi osób trzecich, nawet po ustaniu ich ważności.

§ 6

Określenie sposobu rejestrowania i wyrejestrowywania użytkowników.

1.Wykaz użytkowników wraz z zakresem dostępu do zbiorów tworzony jest przez Sekretarza Gminy Boronów

2. Sekretarz Gminy Boronów prowadzi „Ewidencje osób zatrudnionych przy przetwarzaniu danych osobowych", która zawiera:

- imię i nazwisko użytkownika
- nazwę identyfikatora
- datę uzyskania upoważnienia (uprawnień dostępu) do przetwarzania danych osobowych

3.Jakakolwiek zmiana informacji wyszczególnionych w ewidencji podlega natychmiastowemu odnotowaniu.

4. Użytkownik, który utracił uprawnienia dostępu do systemu zawierającego dane osobowe, zostaje niezwłocznie wyrejestrowany z systemu przez Administratora Systemu Informatycznego a stosowną informację umieszcza się w ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych.

§ 7

Procedury rozpoczęcia zawieszenia i zakończenia pracy.

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 nie ma widocznych śladów prób niepowołanego ich otwierania,

b) ocenić czy w pomieszczeniu nie ma znaków wskazujących na pobyt w nim osób nieuprawnionych,
c) po włączeniu komputera ocenić jakość jego pracy i stwierdzić zmiany,
d) sprawdzić czy nie zostało zainstalowane jakieś nowe oprogramowanie,
e) w przypadku stwierdzenia zmian niezwłocznie powiadomić zwierzchnika lub ASI jeśli zmiany dotyczą pkt c lub d .

2.Użytkownik przed przystąpieniem do przetwarzania danych powinien zalogować się w systemie, posługując się swoim identyfikatorem i hasłem.

3.Użytkownik w czasie pracy powinien stosować przedsięwzięcia zapewniające bezpieczeństwo przetwarzania danych osobowych w systemie:

- ustawić ekrany monitorów w pomieszczeniach tak, aby uniemożliwić podgląd osobom nieuprawnionym
- dopilnować, aby w pomieszczeniach , stanowiących obszar przetwarzania danych osobowych, osoby trzecie przebywały tylko za zgodą przełożonych i w obecności osób uprawnionych
- stosować urządzenia zabezpieczające przed utratą danych, spowodowanych awarią zasilania lub zakłóceniami w sieci elektrycznej
- w przypadku , kiedy przerwa w pracy wynosi ponad 10 minut stosować automatyczne wylogowanie z systemu bądź automatyczny wygaszacz ekranu chroniony hasłem.

4. Po zakończeniu pracy użytkownik powinien przestrzegać następujących zasad:

- wylogować się z systemu i zaczekać na jego wyłączenie się
- sprawdzić czy nie zostały pozostawione bez nadzoru nośniki informacji (płyty CD, dyskietki, pamięci usb, itp.)

§ 8

Tworzenie kopii zapasowych

1. Kopie zapasowe należy wykonywać z częstotliwością adekwatną do częstotliwości dokonywania zmian w tych zbiorach, tj. przynajmniej raz na tydzień w przypadku danych aktualizowanych na bieżąco oraz nie rzadziej niż raz w miesiącu w przypadku zbiorów danych przetwarzanych sporadycznie.
2. W przypadku braku technicznych możliwości sporządzenia kopii zgodnie z planem, należy je wykonać w najbliższym możliwym terminie.
3. Kopie zapasowe należy tworzyć na odpowiedniej jakości nośnikach informacji i przechowywać je w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
4. Kopiami zapasowymi, zgodnie z rozporządzeniem zabezpiecza się zarówno dane jak i programy służące do ich przetwarzania.
5. Osobą odpowiedzialną za ustalanie sposobów i standardów tworzenia kopii zapasowych jest ASI.
6. Użytkownicy we własnym zakresie odpowiadają za sporządzanie kopii zapasowych i awaryjnych wytworzonych przez siebie dokumentów i danych znajdujących się na lokalnych dyskach twardych wykorzystywanych przez nich stacji roboczych. Jednocześnie mają obowiązek dopilnowania, aby dane przetwarzane przy pomocy oprogramowania nie przeznaczonego do przetwarzania danych osobowych bądź też oprogramowania służącego przetwarzaniu danych osobowych wyłącznie w celu ich

udostępnienia na piśmie, i zapisywane na nośnikach informatycznych nie zawierały danych osobowych.

§ 9

Sposób i czas przechowywania nośników informacji (w tym kopii zapasowych).

1. Kopii awaryjnych wykonywanych na nośnikach magnetycznych nie należy przechowywać w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.
2. Nośniki informacji oraz wydruki z danymi osobowymi, które nie są przeznaczone do udostępniania przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.
3. Kopie awaryjne należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu.
4. Kopie awaryjne usuwane są niezwłocznie po ustaniu ich użyteczności

§ 10

Sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania

1. W celu zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych należy zastosować środki bezpieczeństwa na poziomie wysokim.
2. System informatyczny służący do przetwarzania danych osobowych powinien być zabezpieczony programem antywirusowym, który nadzoruje i automatycznie sygnalizuje obecność wirusów oraz niebezpiecznego oprogramowania ułatwiającego zdalny dostęp do informacji.
3. Program antywirusowy powinien posiadać mechanizmy uaktualniania bazy danych wirusów.
4. O każdorazowym wykryciu wirusa użytkownik zobowiązany jest niezwłocznie powiadomić ASI , który dokonuje analizy problemu i podejmuje stosowne działania naprawcze.
5. Dodatkowo należy zastosować sprzętowe urządzenie oddzielające sieć komputerową od bezpośredniego dostępu do Internetu, typu zarządzany router, stanowiące blokadę przed nieuprawnionym dostępem z zewnątrz do systemu informatycznego Urzędu Gminy Boronów.
6. W sytuacji konieczności podłączenia do systemu komputerowego nośnika informacji pochodzącego z zewnętrznego źródła (np. płyty cd/dvd, pamięci usb itp.) nośnika taki musi zostać poddany weryfikacji pod kątem infekcji szkodliwym oprogramowaniem przez ASI.
7. Zabrania się używania do codziennej pracy urządzeń pamięci masowej nie będących na wyposażeniu Urzędu Gminy w Boronowie i nie zatwierdzonych przez ADO po zasięgnięciu opinii ASI.
8. Zabrania się używania i wynoszenia urządzeń i nośników informacji wykorzystywanych do pracy w Urzędzie Gminy w Boronowie poza obszar przetwarzania danych. W przypadku zaistnienia takiej konieczności należy uzyskać zgodę ADO. Jeśli nośnik danych umożliwiający zapis (dyskietka, pamięć USB itp.) został podłączony do

zewnętrznego urządzenia (np. komputer domowy, stacja robocza w jednostce podległej itp.) przed jego ponownym podłączeniem do systemu informatycznego Urzędu Gminy w Boronowie musi zostać poddany weryfikacji jak w pkt 6.

§ 11

Sposób dokonywania przeglądów i konserwacji systemu oraz zbiorów danych osobowych

1. Okresowe oraz bieżące przeglądy i konserwacje sprzętu komputerowego, wynikające z eksploatacji, warunków zewnętrznych oraz ważności systemu dla funkcjonowania Urzędu Gminy Boronów wykonuje ASI.
2. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do naprawy w firmach zewnętrznych, pozbawia się przed naprawą zapisu danych osobowych, albo naprawia je pod nadzorem ASI.
3. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do likwidacji należy pozbawić zapisu, a w przypadku gdy jest to niemożliwe uszkodzić mechanicznie w sposób uniemożliwiający ich odczytanie.

§ 12

Postępowanie w przypadku przekazywania nośników z danymi osobowymi poza obszar przetwarzania danych.

1. Dane osobowe zapisane na urządzeniach i nośnikach informacji przekazywane poza obszar przetwarzania danych osobowych, w celu zapewnienia ich poufności i integralności powinny wcześniej zostać zakodowane stosownym programem przy użyciu co najmniej 8 literowego hasła, które musi zawierać duże i małe litery oraz cyfry lub znaki specjalne.

§ 13

Postanowienia końcowe.

1. Użytkownik systemu informatycznego nie ma prawa dokonywania samodzielnych instalacji, deinstalacji jakiegokolwiek oprogramowania, ani wprowadzania zmian w konfiguracji oprogramowania wykraczających poza jego normalne użytkowanie.
2. Czynności o których mowa w **§ 13 pkt 1** wykonuje ASI.
3. Sekretarz Gminy prowadzi „Rejestr zbiorów danych osobowych przetwarzanych w systemach informatycznych"
4. ASI przeprowadza szkolenia dla nowozatrudnionych pracowników oraz w przypadku istotnych zmian w systemach informatycznych, w których przetwarzane są dane osobowe z zakresu stosowania Instrukcji Zarządzania Systemem Informatycznym.
5. Inspektor Ochrony Danych dokonuje okresowego sprawdzenia sprawności funkcjonowania zabezpieczeń systemów w których przetwarzane są dane osobowe.

§ 14

W sprawach nieuregulowanych niniejszą Instrukcją zastosowanie znajdują przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000).

WÓJT
Krzysztof Bełkot