WÓJT GMINY CZARNA

Zarządzenie Nr 59/2014
Wójta Gminy w Czarnej
z dnia 28 sierpnia 2014 r.

w sprawie zmiany zarządzenia własnego Nr 9/2009 w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych w Urzędzie Gminy Czarna oraz Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Czarna

Na podstawie art. 31 ustawy z dnia 8 marca 1990r., o samorządzie gminnym (Dz. U z 2013r. poz. 594 z późn. zm.), .), art. 36 ust. 1 i ust .2 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.) oraz § 1 i § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024) zarządzam, co następuje:

§ 1. W Polityce bezpieczeństwa danych osobowych w Urzędzie Gminy Czarna stanowiącej załącznik Nr 1 do zarządzenia własnego Nr 9/2009 z dnia 16.02.2009r. w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych w Urzędzie Gminy Czarna oraz Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Czarna, zwanej dalej „Polityką bezpieczeństwa " wprowadzam następujące zmiany :

1. W **§ 2 pkt 5** otrzymuje nowe brzmienie:
   „ 5. Administratorze Danych Osobowych zwanym dalej „ADO" lub „Administratorem" – należy przez to rozumieć Wójta Gminy Czarna,"

2. w **§ 2** po dotychczasowym **pkt 13** dodaje się nowe punkty **14 i 15** w brzmieniu:
   „ 14. urzędzie – należy przez to rozumieć Urząd Gminy w Czarnej,
   15. Administratorze Systemów Informatycznych zwanym dalej „ASI" – należy przez to rozumieć osobę wyznaczoną przez ADO do zarządzania systemami informatycznymi w Urzędzie Gminy w Czarnej."

3. w **§ 3** dotychczasowy **ust. 3** otrzymuje nowe brzmienie:
   „3. Administrator Bezpieczeństwa Informacji zwany dalej „ABI" odpowiada za:
   1. prowadzenie i realizację postanowień zawartych w niniejszej polityce bezpieczeństwa oraz postanowień zawartych w Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Czarna zwanej dalej „instrukcją",
   2. nadzór nad przestrzeganiem zasad ochrony danych osobowych w urzędzie,
   3. nadzór nad właściwym zabezpieczeniem sprzętu oraz pomieszczeń, w których przetwarzane są dane osobowe,
   4. nadzór nad zabezpieczeniem danych przed ich udostępnieniem osobom nieupoważnionym,

WÓJT GMINY CZARNA

Zarządzenie Nr 59/2014
Wójta Gminy w Czarnej
z dnia 28 sierpnia 2014 r.

w sprawie zmiany zarządzenia własnego Nr 9/2009 w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych w Urzędzie Gminy Czarna oraz Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Czarna

Na podstawie art. 31 ustawy z dnia 8 marca 1990r., o samorządzie gminnym (Dz. U z 2013r. poz. 594 z późn. zm.),), art. 36 ust. 1 i ust .2 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.) oraz § 1 i § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024) zarządzam, co następuje:

§ 1. W Polityce bezpieczeństwa danych osobowych w Urzędzie Gminy Czarna stanowiącej załącznik Nr 1 do zarządzenia własnego Nr 9/2009 z dnia 16.02.2009r. w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych w Urzędzie Gminy Czarna oraz Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Czarna, zwanej dalej „Polityką bezpieczeństwa " wprowadzam następujące zmiany :

1. W **§ 2 pkt 5** otrzymuje nowe brzmienie:
   „ 5. Administratorze Danych Osobowych zwanym dalej „ADO" lub „Administratorem" – należy przez to rozumieć Wójta Gminy Czarna,"

2. w **§ 2** po dotychczasowym **pkt 13** dodaje się nowe punkty **14 i 15** w brzmieniu:
   „ 14. urzędzie – należy przez to rozumieć Urząd Gminy w Czarnej,
   15. Administratorze Systemów Informatycznych zwanym dalej „ASI" – należy przez to rozumieć osobę wyznaczoną przez ADO do zarządzania systemami informatycznymi w Urzędzie Gminy w Czarnej."

3. w **§ 3** dotychczasowy **ust. 3** otrzymuje nowe brzmienie:
   „3. Administrator Bezpieczeństwa Informacji zwany dalej „ABI" odpowiada za:
   1. prowadzenie i realizację postanowień zawartych w niniejszej polityce bezpieczeństwa oraz postanowień zawartych w Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Czarna zwanej dalej „instrukcją".
   2. nadzór nad przestrzeganiem zasad ochrony danych osobowych w urzędzie,
   3. nadzór nad właściwym zabezpieczeniem sprzętu oraz pomieszczeń, w których przetwarzane są dane osobowe,
   4. nadzór nad zabezpieczeniem danych przed ich udostępnieniem osobom nieupoważnionym,

5. niezwłoczne informowanie Administratora o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
6. prowadzenie i aktualizację ewidencji osób upoważnionych do przetwarzania danych osobowych oraz ewidencji wniosków o nadanie lub cofnięcie uprawnień w systemie informatycznym,
7. prowadzenie i aktualizację wykazu podmiotów uprawnionych przez administratora do wykonywania naprawy i konserwacji systemu w obszarze przetwarzania danych w urzędzie,
8. nadzór nad wykorzystywanym w urzędzie oprogramowaniem do przetwarzania danych osobowych oraz jego legalnością,
9. badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych,
10. opiniowanie decyzji o instalowaniu nowych urządzeń oraz oprogramowaniu wykorzystywanym do przetwarzania danych osobowych,
11. nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe,
12. nadzór nad definiowaniem użytkowników oraz nadawaniem haseł dostępu do zbiorów danych osobowych,
13. nadzór nad aktualizowaniem oprogramowania antywirusowego,
14. nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym przeglądaniem pod kątem ich dalszej przydatności,
15. nadzór nad pracą ASI (Administratora Systemów Informatycznych),
16. nadzór nad sporządzaniem przez ASI raportów z naruszenia bezpieczeństwa systemu informatycznego,
17. przeprowadzanie szkoleń pracowników z zakresu ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych,
18. wdrażanie, przechowywanie i aktualizowanie dokumentacji opisującej sposób przetwarzania danych osobowych,
19. zgłaszanie zbiorów danych osobowych do rejestracji w GIODO oraz zmian w zbiorach uprzednio zgłoszonych,
20. ustalanie wspólnie z ASI właściwych poziomów bezpieczeństwa przetwarzanych danych w systemie informatycznym."

4. w **§ 3** po dotychczasowym **ust. 3** dodaje się nowy **ust. 4** w brzmieniu:

„ 4. Pracownicy urzędu, mający dostęp do danych osobowych są zobligowani do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych w tym m.in. do:

1. ochrony danych osobowych przed dostępem osób nieupoważnionych (pracownik nie może pod rygorem odpowiedzialności służbowej i karnej - ujawniać danych, kopiować baz danych oraz przetwarzać danych w sposób inny niż opisany procedurami),
2. ochrony danych przed przypadkowym lub nieumyślnym zniszczeniem, utratą lub modyfikacją,
3. utrzymywania w tajemnicy powierzonych identyfikatorów, haseł (również w zakresie częstotliwości ich zmiany) – także po ustaniu stosunku pracy w Urzędzie Gminy Czarna,
4. ochrony nośników optycznych i elektronicznych (płyty , pendrivy, dyski zewnętrzne itp.) oraz wydruków komputerowych przed dostępem osób nieupoważnionych,
5. właściwego przechowywania i archiwizowania danych.

5. w **§ 5** dotychczasowy **ust. 2** otrzymuje nowe brzmienie:
„2. Fizyczny dostęp do pomieszczeń, w których przetwarzane są dane osobowe blokują zwykłe drzwi zamykane na zamki typu łucznik. Po zakończeniu pracy pomieszczenia biurowe są zamykane, a klucze od nich umieszczane w zamykanej na klucz specjalnej szafce na klucze znajdującej się sekretariacie urzędu."

6. w **§ 5** po dotychczasowym **ust. 5** dodaje się nowy **ust. 6** w brzmieniu:
„6. W pomieszczeniu, w którym funkcjonuje odrębny serwer obsługujący jedynie Referat Usług Komunalnych jest zainstalowany system alarmowy oraz są urządzenia wentylacyjne. Nadzór nad pracą serwera i jego obsługa jest w dyspozycji ASI oraz zastępcy ASI będącego pracownikiem tego referatu. "

7. w **§ 7**dotychczasowe **ustępy od 1 do 4** otrzymują nowe brzmienia:
„1. Odrębnymi zarządzeniami wyznaczono Administratora Bezpieczeństwa Informacji oraz Administratora Systemów Informatycznych.
2. Pracownicy przetwarzający dane osobowe w wersji papierowej posiadają upoważnienia wydane przez Administratora, wg wzoru określonego w załączniku nr 6 do niniejszej polityki.
3. Pracownicy przetwarzający dane osobowe w systemie informatycznym otrzymują uprawnienia nadane przez ASI w formie wniosku o nadanie uprawnień, a w przypadku zaprzestania ich przetwarzania lub zmiany użytkownika programu uprawnienia w tym samym trybie zostają cofnięte wg wzoru określonego w załączniku nr 1 do instrukcji zarządzania systemami informatycznymi.
4. Ewidencję osób upoważnionych do przetwarzania danych osobowych (wzór określa załącznik nr 8 do polityki bezpieczeństwa) oraz ewidencję wniosków o nadanie lub cofnięcie uprawnień w systemie informatycznym (wzór określa załącznik nr 7 do instrukcji zarządzani systemami informatycznymi) prowadzi Administrator Bezpieczeństwa Informacji.

8. **§ 10** otrzymuje nowe brzmienie:

„§ 10

W ramach zapewnienia środków sprzętowych, informatycznych i telekomunikacyjnych podjęto następujące działania:
1. Zastosowano niszczarki dokumentów.
2. Zastosowano ochronę komputerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS.
3. Kopie zapasowe wykonywane są na nośnikach optycznych, elektronicznych (płyty DVD, dyski zewnętrzne) oraz na serwerze zewnętrznym."

9. w **§ 11 ust. 2** otrzymuje nowe brzmienie:
„2. W ramach ochrony programowania systemu zastosowano następujące środki:
1. Dostęp do bazy danych osobowych zastrzeżony jest wyłącznie dla ASI, jego zastępcy, ABI oraz wyznaczonych pracowników firm dostarczających oprogramowanie dla urzędu na podstawie upoważnień udzielonych przez Administratora,
2. Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji.

3. System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu,
4. Zastosowano działający w „tle" program antywirusowy na komputerach użytkowników."

10. § 19 otrzymuje nowe brzmienie:

„§ 19

1. Przypadki nieuzasadnionego zaniechania wykonywania obowiązków wynikających z polityki bezpieczeństwa mogą być potraktowane prze Administratora jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym ABI lub bezpośredniego przełożonego.
2. W sprawach nie uregulowanych mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).
3. Wykaz załączników do polityki bezpieczeństwa:
   1. Załącznik nr 1 – Wykaz budynków i pomieszczeń, w których są przetwarzane dane osobowe
   2. Załącznik nr 2 – Wykaz zbiorów danych, formy ich prowadzenia oraz nazwy programów wykorzystywanych do prowadzenia formy elektronicznej,
   3. Załącznik nr 3 – Opis struktury zbiorów, zawartość poszczególnych pól informacyjnych i powiązania między nimi
   4. Załącznik nr 4 – Określenie pochodzenia danych osobowych oraz przepływu danych pomiędzy poszczególnymi systemami w Urzędzie Gminy Czarna,
   5. Załącznik nr 5 – Określenie środków technicznych i organizacyjnych, niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych,
   6. Załącznik nr 6 – Wzór upoważnienia do przetwarzania danych osobowych,
   7. załącznik nr 7 – Wzór oświadczenia o zapoznaniu się przez pracownika z zasadami ochrony danych osobowych,
   8. Załącznik nr 8 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych.
4. Zmiany w polityce bezpieczeństwa dokonywane są w trybie przyjętym dla jej wprowadzenia."

11. W **załączniku Nr 2** do Polityki bezpieczeństwa, w tabeli pt. **Wykaz zbiorów danych w Urzędzie Gminy w Czarnej, formy ich prowadzenia oraz nazwy programów wykorzystywanych do prowadzenia formy elektronicznej** po pozycji 74 dodaje się nową pozycję oznaczoną nr 75 w brzmieniu:

Lp.	**Nazwa zbioru danych**	**Referat/stanowisko**	**Forma papierowa** tak/nie	**Forma elektroniczna** Nazwa programu
75.	DOKUMENTACJA ZWIĄZANA Z UMOWAMI ZLECENIA I O DZIEŁO	Referat Budżetu i Finansów	Tak	-

12. W **załączniku Nr 3** do Polityki bezpieczeństwa, w tabeli pt. **Opis struktury zbiorów w Urzędzie Gminy Czarna , zawartość poszczególnych pól informacyjnych i powiązania między nimi** po pozycji 74 dodaje się nową pozycję oznaczoną nr 75 w brzmieniu:

Lp.	Nazwa zbioru danych	Pola informacyjne	Powiązania pól informacyjnych
75.	DOKUMENTACJA ZWIĄZANA Z UMOWAMI ZLECENIA I O DZIEŁO	Imię nazwisko, drugie imię, PESEL, nazwisko rodowe , adres zamieszkania, nr konta bankowego, stopień niepełnosprawności	Nie dotyczy

13. W **załączniku Nr 4** do Polityki bezpieczeństwa, w tabeli pt. **Określenie pochodzenia danych osobowych oraz przepływu danych pomiędzy poszczególnymi systemami w Urzędzie Gminy Czarna** po pozycji 74 dodaje się nową pozycję oznaczoną nr 75 w brzmieniu:

Lp.	Nazwa zbioru danych	Pochodzenie danych osobowych	Sposób przepływu danych pomiędzy systemami
75.	DOKUMENTACJA ZWIĄZANA Z UMOWAMI ZLECENIA I O DZIEŁO	Dane osobowe od osób zainteresowanych	Nie dotyczy

14. **załączniku Nr 5** do Polityki bezpieczeństwa, w tabeli pt. **Określenie środków technicznych i organizacyjnych, niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych w Urzędzie Gminy Czarna** po pozycji 74 dodaje się nową pozycję oznaczoną nr 75 w brzmieniu:

Lp.	Nazwa zbioru danych	Zastosowane środki techniczne	Zastosowane środki organizacyjne
75.	DOKUMENTACJA ZWIĄZANA Z UMOWAMI ZLECENIA I O DZIEŁO	Jak w pkt 9	Jak w pkt 1

§ 2. W Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Czarna, stanowiącej załącznik Nr 2 do zarządzenia własnego Nr 9/2009 z dnia 16.02.2009r. w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych w Urzędzie Gminy Czarna oraz Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Czarna, zwanej dalej „instrukcją" wprowadzam następujące zmiany :

1. W **§ 2 pkt 19** otrzymuje nowe brzmienie:
   „19. serwerowni – należy przez to rozumieć wydzielone pomieszczenia w urzędzie w którym znajdują się serwery, będące pod nadzorem ASI lub jego zastępcy".

2. dotychczasowe **§ 3 do § 8** włącznie otrzymują nowe brzmienie:

„**§ 3**

1. Administrator informuje ABI o podmiotach, które będą wykonywać dla urzędu prace związane z przetwarzaniem danych osobowych, m.in. w związku z podpisaniem umów z dostawcami programów licencyjnych, zatrudnieniem pracowników w ramach prac interwencyjnych i robót publicznych, praktykantów, stażystów lub wolontariuszy itp.
2. Wykonywanie prac serwisowych i naprawczych przez podmioty zewnętrzne udzielające licencji na programy komputerowe w systemach w których są przetwarzane dane osobowe odbywa się na warunkach określonych w umowach licencyjnych oraz na podstawie imiennych upoważnień dla pracowników licencjodawców udzielonych przez Administratora.
3. W umowach licencyjnych są zawarte zapisy obligujące licencjodawców do ochrony danych osobowych do których mają wgląd, przestrzegania przepisów ustawy o ochronie danych osobowych oraz ustaleń polityki bezpieczeństwa i instrukcji zarządzania systemami informatycznymi w urzędzie.
4. Zdalny serwis licencjodawcy jest realizowany za pomocą bezpiecznych i szyfrowanych połączeń zgodnie z zapisami w umowach licencyjnych.
5. ABI prowadzi wykaz podmiotów uprawnionych przez Administratora do wykonywania napraw i konserwacji systemu w obszarze przetwarzania danych osobowych zgodnie z wzorem stanowiącym **załącznik nr 5** do niniejszej instrukcji.
6. ABI nadzoruje prawidłowość wykonywania czynności o których mowa wyżej."

§ 4

1. Do przetwarzania danych osobowych mogą mieć dostęp wyłącznie osoby posiadające upoważnienie podpisane przez Administratora oraz ABI.
2. ABI przygotowuje dla pracownika upoważnienie do przetwarzania danych osobowych zgodnie z wzorem określonym w **załączniku nr 6** do polityki bezpieczeństwa danych osobowych,
3. Upoważnienie podpisane przez ABI przekazywane jest do podpisu Administratorowi, a następnie pracownikowi.
4. ABI wpisuje dane pracownika do ewidencji osób upoważnionych do przetwarzania danych osobowych, której wzór stanowi **załącznik nr 8** do polityki bezpieczeństwa.
5. ABI prowadzi okresową kontrolę przestrzegania zasad ochrony danych osobowych w Urzędzie.
6. ABI przedstawia Administratorowi. raz w roku sprawozdanie dotyczące przestrzegania zasad ochrony danych osobowych w urzędzie, które m.in. zawiera:
   1. ogólne dane statystyczne dotyczące ochrony danych osobowych (np. ilość osób upoważnionych do przetwarzania danych, ilość osób pozbawionych uprawnień, ilość osób przeszkolonych w zakresie ochrony danych, ilość zbiorów danych w tym zarejestrowanych przez GIODO, wykaz aplikacji przetwarzających dane, ilość i formy naruszeń bezpieczeństwa przetwarzania danych, ilość obszarów przetwarzania danych).
   2. ocenę ochrony danych osobowych przetwarzanych tzw. metodą klasyczną,
   3. ocenę ochrony danych osobowych przetwarzanych w systemie informatycznym,
   4. wnioski i propozycje usprawniające bezpieczeństwo przetwarzania danych."

§ 5

1. W przypadku przetwarzania przez pracownika danych w systemie informatycznym ASI nadaje lub cofa uprawnienia na wniosek złożony przez bezpośredniego przełożonego pracownika o nadanie/cofnięcie uprawnień w systemie informatycznym zgodnie z wzorem określonym w **załączniku nr 1** do niniejszej instrukcji.
2. Wniosek sporządza i podpisuje bezpośredni przełożony pracownika, ASI który potwierdza nadanie lub cofnięcie uprawnień oraz ABI, który potwierdza wpisanie danych do ewidencji wniosków o nadanie/cofnięcie uprawnień w systemie informatycznym zgodnie z wzorem stanowiącym **załącznik nr 7** do niniejszej instrukcji.

§ 6

1. W przypadku upoważnień dla pracowników podmiotów zewnętrznych, o których mowa w § 3 ust. 1 ABI postępuje podobnie jak w stosunku do pracowników urzędu.
2. Upoważnienie do przetwarzania danych osobowych lub wniosek o nadanie uprawnień w systemie informatycznym traci ważność z chwilą ustania: zatrudnienia u Administratora, zakończenia wykonywania pracy na rzecz urzędu przez podmioty zewnętrzne lub zmiany stanowiska pracy, którego upoważnienie lub wniosek dotyczy.
3. W przypadku utraty ważności upoważnienia do przetwarzania danych osobowych ABI wpisuje datę ustania upoważnienia do ewidencji osób upoważnionych do przetwarzania danych osobowych, a w przypadku ustania uprawnień do przetwarzania danych w systemie informatycznym bezpośredni przełożony sporządza wniosek do ASI o cofnięcie uprawnień, a ABI odnotowuje ten fakt w ewidencji, o której mowa w § 5 ust. 2.
4. W przypadku zmiany jedynie danych identyfikacyjnych pracownika zarejestrowanego w systemie informatycznym postępuje się zgodnie z procedurą określoną w § 5.

§ 7

1. Administrator informuje niezwłocznie ABI i ASI o przypadkach określonych w § 6 ust. 2.
2. Przed rozpoczęciem pracy przez pracownika ABI oraz ASI dokonują przeszkolenia pracownika w zakresie ochrony danych osobowych i zasad bezpieczeństwa informacji w urzędzie.
3. Każdy pracownik składa pisemne oświadczenie zgodnie z wzorem określonym w **załączniku nr 7** do polityki bezpieczeństwa o zapoznaniu się z ustawą o ochronie danych osobowych, polityką bezpieczeństwa i instrukcją zarządzania systemami informatycznymi w urzędzie.
4. Upoważnienie, wniosek o nadanie/cofnięcie uprawnień oraz oświadczenie sporządzane jest w 3 egzemplarzach po jednym dla ABI, akt osobowych i pracownika.

§ 8

1. Identyfikator użytkownika powinien składać się z ciągu znaków literowych, jednoznacznie identyfikujących w systemie osobę upoważnioną do przetwarzania danych osobowych.

2. Identyfikator po wyrejestrowaniu osoby z systemu nie może być przydzielony innej osobie.
3. Używanie identyfikatorów oraz haseł należących do innych osób jest zabronione."

3. w **§ 9** dotychczasowy **ust. 3** otrzymuje nowe brzmienie:
„3. Hasła dostępu nie mogą się powtarzać w danym roku i powinny być zmieniane przynajmniej co 60 dni."

4. w **§ 9** dotychczasowy **ust. 6** otrzymuje nowe brzmienie:
„ 6. Hasła dostępu używanego do uwierzytelniania użytkowników powinny się składać z co najmniej 8 znaków z użyciem cyfr, małych i dużych liter oraz znaków specjalnych."

5. **§ 10** otrzymuje nowe brzmienie:

„§ 10

1. Hasła ASI przechowywane są w postaci klasycznego zapisu w zapieczętowanej kopercie, przechowywanej w metalowej kasecie z szyfrem, umieszczonym w sejfie zlokalizowanym w kasie urzędu gminy objętej monitoringiem i chronionej alarmem.
2. W sytuacjach awaryjnych lub w razie nieobecności ASI jego zadania wypełnia wyznaczony przez Administratora pracownik zastępujący ASI.
3. W przypadku wykorzystania haseł podczas nieobecności ASI muszą być one niezwłocznie zmienione po wznowieniu wykonywania przez niego obowiązków."

6. w **§ 12 ust. 5 pkt 5** skreśla się wyrazy: „poprzez użycie polecenia «Zamknij system»".

7. w **§ 12** dotychczasowy **ust. 6 pkt 4** otrzymuje nowe brzmienie:
„5. uruchomić systemy alarmowe w pomieszczeniach w których są one zainstalowane."

8. **w § 18 ust. 8** otrzymuje nowe brzmienie:
„8. Nośniki informacji wycofane z eksploatacji podlegają procedurze usuwania danych o której mowa w ust. 6 i 7."

9. **w § 18** skreśla się **ust. 9 i 10,**

10. **§ 19 do § 21** włącznie otrzymują nowe brzmienie:

„§ 19

1. Procedury niszczenia kopii zapasowych i innych elektronicznych nośników informacji przeprowadza ASI w obecności ABI, sporządzając z tych czynności protokół zgodnie z wzorem stanowiącym załącznik nr 4 do niniejszej instrukcji, a jego kopię przekazuje ABI.
2. Do obowiązków ASI należy ponadto:
    1. współpraca z ABI w opracowywaniu i aktualizacji polityki Bezpieczeństwa danych osobowych i instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych oraz innych dokumentów służących zapewnieniu bezpieczeństwa informacji w urzędzie.
    2. udzielanie ABI pomocy w wypełnianiu jego zadań w odniesieniu do systemu informatycznego w urzędzie.

3. nadzór i kontrola systemów informatycznych oraz innych zbiorów danych służących do przetwarzania danych osobowych oraz nad pracą osób przy nich zatrudnionych,
4. zapewnienie sprawnego i nieprzerwanego funkcjonowania systemów informatycznych w urzędzie oraz urządzeń i programów służących do zapewnienia bezpieczeństwa informacji w tym ochrony danych osobowych,
5. kontrola przestrzegania instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych ,
6. zarządzanie hasłami użytkowników, systemami antywirusowymi i ich procedurami,
7. nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem, okresowym sprawdzaniem pod kątem ich dalszej przydatności oraz ich likwidacja,
8. nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których są zapisane dane osobowe,
9. prowadzenie rejestru zdarzeń i incydentów zagrażających bezpieczeństwu informacji w urzędzie,
10. prowadzenie ewidencji wszystkich komputerów w rozbiciu na poszczególnych użytkowników, zainstalowanego na nich oprogramowania, wraz z ewidencją dokonywanych napraw i wymiany części,
11. przygotowywanie we współpracy z ABI rejestru ryzyka bezpieczeństwa informacji w urzędzie,
12. prowadzenie szkoleń pracowników na stanowiskach pracy w zakresie bezpieczeństwa informacji ze szczególnym uwzględnieniem ochrony danych osobowych,
13. monitorowanie funkcjonowania zabezpieczeń systemów informatycznych, wdrożonych w celu ochrony danych osobowych,
14. pełnienie zastępstwa za Administratora Bezpieczeństwa Informacji."

§ 20

1. Elektroniczne nośniki informacji zawierające dane osobowe lub kopie zapasowe przechowuje się zgodnie z przepisami prawa.
2. Czas przechowywania kopii zapasowych powinien być nie dłuższy niż jest to konieczne dla bezpieczeństwa systemu.
3. W celu zapewnienia bezpieczeństwa kopii zapasowych przed nieuprawnionym dostępem, modyfikacją, uszkodzeniem lub zniszczeniem są one przechowywane w metalowej kasecie z szyfrem, umieszczonym w sejfie zlokalizowanym w kasie urzędu gminy objętej monitoringiem i chronionej alarmem oraz umieszczane przez ASI szyfrowanymi połączeniami w tzw. chmurze na serwerze zewnętrznym, zgodnie z zapisami odrębnej umowy.
4. Zapisy umowy zapewniając bezpieczeństwo przechowywania danych poprzez określenie obowiązków i odpowiedzialność wykonawcy w zakresie zabezpieczenia nośników danych przed nieuprawnionym odczytem, kopiowaniem, modyfikacją lub zniszczeniem.
5. Nośniki informacji zawierające dane osobowe z których korzystają pracownicy przechowuje się w urzędzie zamykanych na klucz typu łucznik pomieszczeniach biurowych, w zamkniętych na klucz szafach i zabezpieczonych zamkami meblach biurowych.

§ 21

1. Nośniki informacji zawierające dane osobowe można przekazywać do innej jednostki organizacyjnej tylko na pisemny, umotywowany wniosek za pisemna zgodą Administratora.
2. Nośniki informacji, o których mowa w ust. 1, trzeba na czas transportu odpowiednio zabezpieczyć przed dostępem osób nieuprawnionych.
3. Przesyłu danych osobowych z wykorzystaniem sieci publicznej można dokonać tylko z zastosowanie środków kryptograficznych."

11. w **§ 22 ust. 3** skreśla się wyrazy „oraz dyskietki" ,

12. dotychczasowe **§ 23 do § 28** włącznie otrzymują nowe brzmienie:

„§ 23

1. Urządzenia i elektroniczne nośniki informacji, zawierające dane sensytywne przekazywane poza obszar przetwarzania tych danych, obowiązkowo zabezpiecza się przed dostępem osób i podmiotów nieupoważnionych, modyfikacją lub zniszczeniem w sposób nieautoryzowany.
2. Osoba użytkująca komputer przenośny lub inne urządzenie zawierające dane osobowe, zobowiązana jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i używania poza obszarem przetwarzania danych, w tym stosowania środków ochrony kryptograficznej podczas transmisji.
3. Użytkownikom korzystającym z systemu informatycznego zabrania się instalowania na komputerach jakiegokolwiek oprogramowania, jeżeli nie są do tego uprawnieni.
4. Użytkownik dopuszczony do korzystania z systemu informatycznego musi być przeszkolony przez ASI w zakresie inicjowania pracy komputerów pracujących w sieci oraz postępowania w wypadku wykrycia awarii lub wystąpienia nietypowych zdarzeń.
5. Pracownicy urzędu są odpowiedzialni za przestrzeganie procedur przetwarzania danych osobowych określonych przez Administratora.
6. Naruszenie przez pracownika posiadającego upoważnienie do przetwarzania danych osobowych postanowień niniejszej instrukcji może stanowić podstawę do pociągnięcia go do odpowiedzialności z tytułu naruszenia obowiązków pracowniczych.
7. ASI lub inne osoby upoważnione przez Administratora zobowiązani są do uwzględniania warunków bezpieczeństwa danych osobowych przy wprowadzeniu rozwiązań programowych i sprzętowych służących do przetwarzania danych.
8. Pracownik ma prawo korzystania wyłącznie z oprogramowania w które wyposaża go pracodawca na danym stanowisku pracy .
9. Pracownik ma prawo korzystać wyłącznie z oprogramowania zainstalowanego i zatwierdzonego przez ASI za zgodą Administratora i zobowiązuje się do niekorzystania z jakiegokolwiek innego oprogramowania komputerowego, do którego nie jest uprawniony przez Pracodawcę w czasie pracy, w miejscu pracy ani przy użyciu sprzętu Pracodawcy.
10. Wzór pisemnego zobowiązania pracownika stanowi **załącznik nr 6** do niniejszej instrukcji.

§ 24

1. ASI jest zobowiązany zabezpieczyć system przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do danych poprzez wdrożenie technicznych i logicznych zabezpieczeń chroniących system.
2. ASI może stosować dodatkowe metody ochrony przed szkodliwym działaniem programów mających na celu uzyskanie nieuprawnionego dostępu do danych, w szczególności poprzez:
   1) pozbawienie systemu możliwości pracy w sieci informatycznej oraz założenia do odczytu danych z elektronicznych nośników informacji,
   2) wydzielenie osobnego stanowiska komputerowego w sieci wewnętrznej do wymiany danych za pomocą nośników zewnętrznych.
3. ASI realizując zadania, o których mowa w ust. 2 podejmuje działania w zakresie:
   1) kontroli przepływu informacji pomiędzy wewnętrznym systemem informatycznym i publiczną siecią informatyczną oraz kontroli działań inicjowanych z sieci informatycznej i systemu,
   2) instalowania w systemie oprogramowania zapobiegającego nieuprawnionemu dostępowi do danych osobowych.

§ 25

1. System przetwarzający dane osobowe, musi zapewniać osobom, których dane są przetwarzane, odnotowanie:
   1) daty pierwszego wprowadzenia danych do systemu,
   2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu posiada tylko jedna osoba,
   3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą,
   4) informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie udostępnienia, chyba że system używany jest do przetwarzania danych w zbiorach jawnych,
   5) sprzeciwu odnośnie przetwarzania danych, o których mowa w art. 32 ust. 1 pkt 8 ustawy.
2. Odnotowywanie w systemie informacji, o których mowa w ust. 1 pkt 1 i 2 następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
3. System zapewnia każdej osobie, której dane są w nim przetwarzane, wydrukowanie raportu zawierającego w zrozumiałej formie informacje, o których mowa w ust. 1.

§ 26

1. Wykonywanie przeglądów i konserwacja systemu ma na celu:
   1) przegląd stosowanych elementów bezpieczeństwa,
   2) kontrolę właściwej konfiguracji systemu,
   3) sprawdzenie funkcjonalności i jakości pracy systemu,
   4) zakwalifikowanie sprzętu i urządzeń do naprawy lub modyfikacji.
2. Zakres czynności, o których mowa w ust. 1 pkt 1, obejmuje w szczególności:
   1) sprawdzenie stanu kont użytkowników,
   2) sprawdzenie wersji programu antywirusowego pod kątem aktualności jego konfiguracji oraz baz wirusów,
   3) sprawdzenie działania urządzeń zabezpieczających przed nieuprawnionym dostępem,
   4) kontrolę działania awaryjnego zasilania.

§ 24

1. ASI jest zobowiązany zabezpieczyć system przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do danych poprzez wdrażanie technicznych i logicznych zabezpieczeń chroniących system.
2. ASI może stosować dodatkowe metody ochrony przed szkodliwym działaniem programów mających na celu uzyskanie nieuprawnionego dostępu do danych, a w szczególności poprzez:
   1) pozbawienie systemu możliwości pracy w sieci informatycznej oraz zdolności do odczytu danych z elektronicznych nośników informacji,
   2) wydzielenie osobnego stanowiska komputerowego w sieci wewnętrznej do wymiany danych za pomocą nośników zewnętrznych.
3. ASI realizując zadania, o których mowa w ust. 2 podejmuje działania w zakresie:
   1) kontroli przepływu informacji pomiędzy wewnętrznym systemem informatycznym i publiczną siecią informatyczną oraz kontroli działań inicjowanych z sieci informatycznej i systemu,
   2) instalowania w systemie oprogramowania zapobiegającego nieuprawnionemu dostępowi do danych osobowych.

§ 25

1. System przetwarzający dane osobowe musi zapewniać osobom, których dane są przetwarzane, odnotowanie:
   1) daty pierwszego wprowadzenia danych do systemu,
   2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu posiada tylko jedna osoba,
   3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą,
   4) informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie udostępnienia, chyba że system używany jest do przetwarzania danych w zbiorach jawnych,
   5) sprzeciwu odnośnie przetwarzania danych, o których mowa w art. 32 ust. 1 pkt 8 ustawy.
2. Odnotowywanie w systemie informacji, o których mowa w ust. 1 pkt 1 i 2 następuje automatycznie, po zatwierdzeniu przez użytkownika operacji wprowadzania danych.
3. System zapewnia każdej osobie, której dane są w nim przetwarzane, wydrukowanie raportu zawierającego w zrozumiałej formie informacje, o których mowa w ust. 1.

§ 26

1. Wykonywanie przeglądów i konserwacja systemu ma na celu:
   1) przegląd stosowanych elementów bezpieczeństwa,
   2) kontrolę właściwej konfiguracji systemu,
   3) sprawdzenie funkcjonalności i jakości pracy systemu,
   4) zakwalifikowanie sprzętu i urządzeń do naprawy lub modyfikacji.
2. Zakres czynności, o których mowa w ust. 1 pkt 1 obejmuje w szczególności:
   1) sprawdzenie stanu kont użytkowników,
   2) sprawdzenie wersji programu antywirusowego pod kątem aktualności jego konfiguracji oraz bazy wirusów,
   3) sprawdzenie działania urządzeń zabezpieczających przed nieuprawnionym dostępem,
   4) kontrolę działania awaryjnego zasilania.

13) załącznik nr 7 – Ewidencja wniosków o nadanie/cofnięcie uprawnień w systemie informatycznym.

13. kolejne rozdziały instrukcji począwszy od nr VI do Nr XI tworzą obecnie zmienione paragrafy:
1) rozdział VI Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania – **§ 17 do § 19** włącznie,
2) rozdział VII Przechowywanie i udostępnianie nośników informacji zawierających dane osobowe oraz kopii zapasowe – **§ 20 do § 21** włącznie,
3) rozdział VIII Zabezpieczenie systemu przed wirusami komputerowymi, awarią zasilania oraz nieuprawnionym dostępem – **§ 22 do § 24** włącznie
4) rozdział IX Wymogi systemu w zakresie procedur przetwarzania danych osobowych – **§ 25,**
5) rozdział X Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych – **§ 26 do § 27** włącznie
6) rozdział XI Postanowienia końcowe – § 28

14. skreśla się dotychczasowe paragrafy – **od § 29 do § 41 włącznie,**

15. **Załącznik nr 5** do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Czarna **Wykaz podmiotów uprawnionych do przez Administratora do wykonywania napraw i konserwacji systemów w obszarze przetwarzania danych** – otrzymuje brzmienie określone w załączniku nr 1 do niniejszego zarządzenia

16. **Załącznik nr 6** do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Czarna **Zobowiązanie pracownika** otrzymuje brzmienie określone w załączniku nr 2 do niniejszego zarządzenia

17. Dodaje się nowy **załącznik nr 7 Ewidencja wniosków o nadanie uprawnień w systemie informatycznym** stanowiący załącznik nr 3 do niniejszego zarządzenia

§ 3. Wykonanie niniejszego zarządzenia powierza się Sekretarzowi Gminy.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

15) załącznik nr 7 – Ewidencja wniosków o nadanie/cofnięcie uprawnień w systemie informatycznym.

13. Kolejne rozdziały instrukcji począwszy od nr VI do Nr XI tworzą obecnie zmienione paragrafy:
    1) rozdział VI Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania – **§ 17 do § 19** włącznie
    2) rozdział VII Przechowywanie i udostępnianie nośników informacji zawierających dane osobowe oraz kopie zapasowe – **§ 20 do § 21** włącznie
    3) rozdział VIII Zabezpieczenie systemu przed wirusami komputerowymi oraz działaniami oraz nieuprawnionym dostępem – **§ 22 do § 24** włącznie.
    4) rozdział IX Wymogi systemu w zakresie procedur przetwarzania danych osobowych – **§ 25.**
    5) rozdział X Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych – **§ 26 do § 27** włącznie.
    6) rozdział XI Postanowienia końcowe – § 28

14. skreśla się dotychczasowe paragrafy – **od § 29 do § 41 włącznie.**

15. **Załącznik nr 5** do Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Czarna **Wykaz podmiotów uprawnionych do przez Administratora do wykonywania napraw i konserwacji systemów w obszarze przetwarzania danych** otrzymuje brzmienie określone w załączniku nr 1 do niniejszego zarządzenia.

16. **Załącznik nr 6** do Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Czarna **Zobowiązanie pracownika** otrzymuje brzmienie określone w załączniku nr 2 do niniejszego zarządzenia.

17. Dodaje się nowy **załącznik nr 7 Ewidencja wniosków o nadanie uprawnień w systemie informatycznym** stanowiący załącznik nr 3 do niniejszego zarządzenia.

§ 3. Wykonanie niniejszego zarządzenia powierzam Sekretarzowi Gminy.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 1 do zarz. Nr 59/2014 Wójta Gminy Czarna z dnia 28.08.2014r.

„Załącznik nr 5 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie będącym załącznikiem nr 2 do zarz. Nr 9/2008 Wójta Gminy Czarna z dnia 16.01.2008r"

WYKAZ PODMIOTÓW UPRAWNIONYCH PRZEZ ADMINISTRATORA DO WYKONYWANIA NAPRAW I KONSERWACJI SYSTEMU W OBSZARZE PRZETWARZANIA DANYCH W URZĘDZIE GMINY W CZARNEJ

Lp	Nr i data umowy	Podmiot			Pracownicy podmiotu		
		Nazwa	Adres	NIP	Imię	Nazwisko	Nr upoważnienia wydanego przez Administratora

Załącznik nr 1 do zarz. Nr 59/2014 Wójta Gminy Czarna z dnia 28.06.2014r.

„Załącznik nr 5 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" stanowiącym załącznik nr 2 do zarz. Nr 6/2009 Wójta Gminy Czarna z dnia 16.02.2009r.

WYKAZ PODMIOTÓW UPRAWNIONYCH PRZEZ ADMINISTRATORA DO WYKONYWANIA NAPRAW I KONSERWACJI SYSTEMU W OBSZARZE PRZETWARZANIA DANYCH W URZĘDZIE GMINY W CZARNEJ

Lp.	Nr umowy	Podmiot			Pracownicy podmiotu		
		Nazwa	Adres	NIP	Imię	Nazwisko	Nr upoważnienia wydanego przez Administratora

[redacted]

Załącznik nr 3 do zarz. Nr 59/2014 Wójta Gminy Czarna z dnia 28.08.2014r

„Załącznik nr 5 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych [illegible] będącym załącznikiem nr 2 do zarz. Nr 9/2009 Wójta Gminy Czarna z dnia 16.02.2009r."

EWIDENCJA WNIOSKÓW O NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM
w Urzędzie Gminy Czarna

Administrator Danych Osobowych: Administrator Bezpieczeństwa Informacji:

Lp.	Imię i nazwisko / referat	Numer wniosku	Nazwa identyfikatora (login)	Data		Rodzaj uprawnień	Nazwa programu / aplikacji	Uwagi
				nadania uprawnień	wygaśnięcia uprawnień			

Załącznik nr 3 do zarz. Nr 59/2014 Wójta Gminy Czarna z dnia 29.08.2014r

„Załącznik nr [illegible] do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie" będącym załącznikiem nr 2 do zarz. Nr 9/2009 Wójta Gminy Czarna z dnia [illegible].2009r.

EWIDENCJA WNIOSKÓW O NADANIE/COFNIĘCIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

w Urzędzie Gminy Czarna

Administrator Danych Osobowych

Administrator Bezpieczeństwa Informacji

Lp.	Imię i nazwisko referenta	Numer wniosku	Nazwa identyfikatora użytkownika	Data		Rodzaj uprawnień	Nazwa przyznanej aplikacji	Uwagi
				nadania uprawnień	ostatnia aktualizacja uprawnień			