

Zarządzenie Nr 6²/2015

Burmistrza Miasta i Gminy Kunów

z dnia 11.03.2015

w sprawie: wyznaczenia **Administradora Bezpieczeństwa Informacji** oraz **Administradora Systemów Informatycznych** w Urzędzie Miasta i Gminy w Kunowie.

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz.U. z 2013 r. poz. 594 z późn. zm.), w związku z art. 36 i 36a i ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r. poz. 1182 z późn. zm.) - zarządza się co następuje:

§ 1.

1. Wyznacza się Pana Michała Brodę na **Administradora Bezpieczeństwa Informacji (ABI)** w Urzędzie Miasta i Gminy w Kunowie.
2. Wyznacza się Pana Daniela Ożdżyńskiego (informatyka) na **Administradora Systemów Informatycznych (ASI)** w Urzędzie Miasta i Gminy w Kunowie.

§ 2.

Ustala się zakresy zadań **Administradora Bezpieczeństwa Informacji** oraz **Administradora Systemów Informatycznych** w Urzędzie Miasta i Gminy w Kunowie, w brzmieniu załącznika nr 1 i nr 2 do zarządzenia.”

§ 3

Wykonanie zarządzenia powierza się Sekretarzowi Gminy Kunów.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ

mgr Lech Łodej

**ZAKRES ZADAŃ ORAZ UPRAWNIENIA I UPOWAŻNIENIA
Administradora Bezpieczeństwa Informacji
w Urzędzie Miasta i Gminy w Kunowie.**

I. Administrator Bezpieczeństwa Informacji – zwany dalej **ABI** wykonuje zadania w zakresie niniejszego zarządzenia oraz upoważnień i pełnomocnictw nadanych przez **Administradora Danych Osobowych (ADO)**.

II. Celem działania **ABI** jest nadzorowanie i kontrolowanie przestrzegania zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych w komórkach organizacyjnych Urzędu Miasta i Gminy w Kunowie, w tym w szczególności związanych z przeciwdziałaniem dostępowi do danych osobowych osób nieupoważnionych, zabranii przez osobę nieuprawnioną, zmianą, utratą, uszkodzeniem oraz przetwarzaniem danych z naruszeniem ustawy o ochronie danych osobowych.

III. Zadaniem **ABI** jest realizacja i kontrola przedsięwzięć określonych w:

- art. 36a Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2014 r. poz 1182 z późn. zm.),
- zarządzeniach **Administradora Danych Osobowych**,
- Zarządzeniu Burmistrza w sprawie wdrożenia **Polityki Bezpieczeństwa Przetwarzania Danych Osobowych** w Urzędzie Miasta i Gminy w Kunowie,
- Zarządzeniu Burmistrza w sprawie wdrożenia **Instrukcji Zarządzania Systemem Informatycznym** w Urzędzie Miasta i Gminy w Kunowie.

IV. **ABI** realizując swoje zadania współpracuje z **Administratorem Systemów Informatycznych** w Urzędzie Miasta i Gminy w Kunowie (**ASI**)

Do szczegółowych zadań **ABI** należą: m.in.:

1. Okresowa aktualizacja **Polityki Bezpieczeństwa Przetwarzania Danych Osobowych** w Urzędzie Miasta i Gminy w Kunowie.
2. Założenie, prowadzenie i aktualizacja **Rejestru zbiorów danych przetwarzanych przez ADO**, z wyjątkiem zbiorów, o których mowa w art.43 ust. 1.
3. Rejestrowanie i aktualizacja w **Generalnego Inspektora Ochrony Danych Osobowych (GIODO)** zbiorów zawierających dane osobowe wrażliwe, o których mowa w art. 27 ust. 1 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i przechowywanie kompletnej dokumentacji związanej z ich rejestracją.
4. Koordynowanie czynności realizowanych w wyniku postępowań administracyjnych prowadzonych przez **GIODO**.
5. Wyrażanie w porozumieniu z **ADO** i **ASI** zgody na utworzenie nowego zbioru w systemie informatycznym Urzędu oraz utworzenie nowego zbioru w formie papierowej.
6. Uzgadnianie projektów umów w przypadku zamiaru przyjęcia zbioru danych osobowych w wyniku zawarcia umowy o powierzeniu przetwarzania danych lub w przypadku

- zamiaru przekazania zbioru danych osobowych do przetwarzania podmiotowi zewnętrznemu oraz ich rejestrowanie i archiwizowanie.
7. Konsultowanie zmian warunków technicznych i organizacyjnych związanych z ochroną danych osobowych.
 8. Wyrejestrowanie zbiorów danych osobowych z prowadzonego przez ABI Rejestru zbioru danych przetwarzanych przez ADO i rejestru GODO.
 9. Nadzorowanie działań związanych z fizycznym usunięciem każdej posiadanej formy (papierowej, elektronicznej) wyrejestrowanych zbiorów danych osobowych.
 10. Przyjmowanie zgłoszeń o stwierdzeniu naruszenia lub zaistnienia okoliczności wskazujących na naruszenie systemu ochrony danych osobowych.
 11. Podejmowanie działań wyjaśniających i dokumentujących zgłoszony przypadek naruszenia zasad bezpieczeństwa przetwarzania i ochrony danych osobowych, obejmujących w szczególności:
 - a) ocenę sytuacji, uwzględniającą stan pomieszczenia, w którym przetwarzane są dane, stan urządzenia i zbioru oraz identyfikację zakresu negatywnych następstw naruszenia ochrony danych osobowych,
 - b) wysłuchanie relacji użytkownika lub osoby, która dokonała zgłoszenia,
 - c) podjęcie działań mających na celu ustalenie sprawcy, miejsca, czasu i sposobu dokonania naruszenia ochrony,
 - d) wydanie użytkownikowi zaleceń co do dalszego użytkowania urządzeń wykorzystywanych przy przetwarzaniu zbioru danych osobowych,
 - e) powiadomienie ADO o zaistniałym zdarzeniu oraz w zależności od jego skali i skutków, powołania w porozumieniu z nim doraźnego zespołu do komisijnego zbadania zgłoszonego przypadku naruszenia ochrony danych osobowych,
 - f) sporządzenie dla ADO raportu ze stwierdzonego naruszenia bezpieczeństwa przetwarzania danych osobowych, zawierającego: skalę stwierdzonych naruszeń ochrony, przyczyny ich powstania i skutki oraz wnioski określające zakres działań organizacyjnych i technicznych, zapobiegających w przyszłości podobnym naruszeniom ochrony danych osobowych.
 12. Prowadzenie Ewidencji osób upoważnionych do przetwarzania danych osobowych i rejestrowanie w niej wydanych upoważnień.
 13. Przeprowadzenie odpowiednich procedur wydania upoważnienia do przetwarzania zbiorów danych osobowych, w zależności od tego czy ma ono być udzielone pracownikowi czy też podmiotowi zewnętrznemu lub osobie nie będącej pracownikiem Urzędu.
 14. Opracowanie projektu upoważnienia i przedstawienie go ADO do akceptacji.
 15. Podpisywanie upoważnień pod warunkiem otrzymania w tym zakresie pisemnego upoważnienia od ADO.
 16. Przechowywanie jako załącznika do Ewidencji osób upoważnionych do przetwarzania danych osobowych jednego z trzech egzemplarzy wydanego upoważnienia.
 17. Unieważnianie w porozumieniu z ADO wydanego upoważnienia w zakresie przetwarzania danych osobowych, w przypadku zaistnienia okoliczności powodujących ich utratę.

18. Nadzorowanie wyrejestrowania z systemu informatycznego użytkowników, którym cofnięto udzielone im upoważnienia.
19. Odnoszenie w Ewidencji osób upoważnionych do przetwarzania danych osobowych cofnięcia udzielonego upoważnienia.
20. Prowadzenie Wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.
21. Uzgadnianie instrukcji określających zasady zabezpieczenia pomieszczeń i budynków, w których przetwarzane są zbiory danych osobowych.
22. Sprawowanie wspólnie z ASI i ADO doraźnej i okresowej kontroli bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Kunowie.
23. Przeprowadzenie raz w roku wspólnie z ASI kompleksowej kontroli sprawdzającej przestrzeganie zasad określonych w **Polityce Bezpieczeństwa Przetwarzania Danych Osobowych i Instrukcji Zarządzania Systemem Informatycznym** obowiązujących w Urzędzie Miasta i Gminy w Kunowie
24. Sporządzenie dla ADO pokontrolnego sprawozdania ze zgodności przetwarzania danych osobowych z przepisami o ich ochronie, pozwalającego na podjęcie właściwych działań korygujących i doskonalących zabezpieczenie zbiorów danych osobowych przetwarzanych w Urzędzie.
25. Przeprowadzenie szkoleń dla pracowników, którzy będą pracowali przy przetwarzaniu danych osobowych i wydawanie im **Zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony danych osobowych.**
26. Prowadzenie Wykazu pracowników przeszkolonych w zakresie ochrony danych osobowych i rejestrowanie w nim wydanych **Zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony danych osobowych.**
27. Przechowywanie i rejestrowanie w ww. wykazie **Oświadczeń pracowników Urzędu o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych.**
28. Przygotowanie i prowadzenie we współpracy z ASI **Opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi.**
29. Przygotowanie i aktualizacja we współpracy z ASI **Opisu przepływu danych osobowych między systemami informatycznymi.**

IV. Wykonując swoje czynności ABI realizuje zadania w imieniu ADO i posiada uprawnienia oraz upoważnienia do:

1. Nadzorowania, kontrolowania i koordynowania czynności realizowanych przez ASI.
2. Wskazywania odpowiednich zabezpieczeń technicznych i czynności organizacyjnych mających na celu zapewnienie skutecznej ochrony przetwarzania danych osobowych, w zakresie zapewnienia im integralności, poufności i rozliczalności,
3. Wnioskowania o zawarcie w zakresach czynności osób zatrudnionych przy przetwarzaniu danych osobowych odpowiedzialności tych osób za: nieodpowiednią ochronę danych przed niepowołanym dostępem, nieuzasadnioną modyfikację lub zniszczenie danych oraz ich nielegalne ujawnienie, w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.

4. Kontrolowania realizacji umów dotyczących udostępniania lub powierzenia danych do przetwarzania osobom lub podmiotom zewnętrznym w zakresie stosowania zapisów bezpieczeństwa przetwarzania i ochrony danych osobowych,
 5. Decydowania o pozbawieniu lub ograniczeniu zakresu przetwarzania danych osobowych i uprawnień nadanych w systemie informatycznym dla użytkowników, którzy powodują zagrożenia bezpieczeństwa i ochrony danych osobowych
 6. Udzielania wytycznych dotyczących usuwania nieprawidłowości stwierdzonych w czasie prowadzonych kontroli i dostosowywania ochrony danych do stanu zgodnego z przepisami prawa,
 7. Przechowywania haseł dostępu do stacji roboczych, programów, urządzeń, użytkowanych przez pracowników Urzędu Miasta i Gminy w Kunowie.
 8. Kontrolowania pracowników poprzez audyty związane z bezpieczeństwem informacji oraz ochroną danych osobowych.
- V. W czasie nieobecności ABI jego zadania wykonuje powołany przez ADO zastępca ABI.

BURMISTRZ

Zatwierdzam

mgr Lech Łodej

**ZAKRES ZADAŃ ORAZ UPRAWNIENIA
Administradora Systemów Informatycznych
w Urzędzie Miasta i Gminy w Kunowie.**

I. Administrator Systemów Informatycznych – zwany dalej ASI, jest informatykiem Urzędu i wykonuje zadania w zakresie niniejszego zarządzenia oraz upoważnienia nadanego przez **Administradora Danych Osobowych (ADO)**.

II. Celem działania ASI jest nadzorowanie i realizowanie zasad bezpieczeństwa przetwarzania i ochrony danych osobowych w systemach informatycznych Urzędu Miasta i Gminy w Kunowie.

III. Zadaniem ASI jest realizacja i kontrola przedsięwzięć określonych w:

- art. 36 ust. 1 i w art. 38 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2014 r. poz 1182 z późn. zm.),
- Rozporządzeniu MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024),
- Zarządzeniu Burmistrza w sprawie wdrożenia **Instrukcji Zarządzania Systemem Informatycznym** w Urzędzie Miasta i Gminy w Kunowie.
- Zarządzeniu Burmistrza w sprawie wdrożenia **Polityki Bezpieczeństwa Przetwarzania Danych Osobowych** w Urzędzie Miasta i Gminy w Kunowie.

IV. ASI realizując swoje zadania współpracuje bezpośrednio z **Administratorem Bezpieczeństwa Informacji** w Urzędzie Miasta i Gminy w Kunowie (**ABI**).

Do szczegółowych zadań ASI należą m.in.:

1. Zapewnienie serwerom i stacjom roboczym nieprzerwanego wolnego od zakłóceń zasilania energetycznego.
2. Zapewnienie serwerom właściwej temperatury pracy i ochrony fizycznej oraz zasobów dyskowych wystarczających dla znajdujących się na nich danych.
3. Zapewnienie stabilnych i wydajnych łączy sieciowych LAN i WAN.
4. Zapewnienie zasobom IT nadmiarowości ograniczającej ryzyko przestoju systemów (wykorzystanie macierzy RAID, zapasowe zasilacze, redundancja portów LAN).
5. Wyposażenie ekranów monitorów w wygaszacze zabezpieczone hasłem.
6. Instalowanie na serwerach i stacjach roboczych programów legalnych, licencjonowanych i systematycznie aktualizowanych, z pełną opieką serwisową producenta.
7. Nadzorowanie instalacji oprogramowania, którą może wykonać tylko firma zewnętrzna.
8. Wyposażenie systemu informatycznego w mechanizmy autoryzacji oraz uwierzytelniania użytkownika zapewniające kontrolę dostępu do danych osobowych jedynie osobom upoważnionym.
9. Zapewnienie użytkownikom bezpiecznych form dostępu do Internetu.

10. Utworzenie wewnętrznych – w obrębie Urzędu - mechanizmów przekazywania danych (dyski sieciowe, udostępniony folder użytkownika docelowego).
11. Zapewnienie użytkownikom możliwości przesyłania danych z zastosowaniem mechanizmów kompresji i szyfrowania.
12. Monitorowanie stanu środowiska IT oraz stanu sprzętu IT.
13. Przyznawanie uprawnień w zakresie dostępu do systemu informatycznego polegającego na nadaniu użytkownikowi unikalnego identyfikatora, pierwszego hasła oraz zakresu dostępu do danych i wybranych funkcji narzędzi służących do ich przetwarzania w środowisku IT Urzędu.
14. Odbieranie uprawnień użytkownikowi, który je utracił i wyrejestrowanie jego identyfikatora z systemu informatycznego wraz z unieważnieniem jego hasła.
15. Prowadzenie **Rejestru użytkowników i ich uprawnień w systemie informatycznym.**
16. Monitorowanie częstotliwości zmiany haseł, która nie może następować rzadziej niż co 30 dni, o ile aplikacja nie wymusza zmiany hasła.
17. Resetowanie utraconych przez użytkowników haseł.
18. Monitorowanie wykorzystywanego oprogramowania oraz aktywności sieciowej użytkowników.
19. Ustawienie blokad konta na poziomie danego użytkownika po wykryciu trzech nieudanych prób logowania i ustalenie przyczyn zablokowania systemu.
20. Przygotowanie zewnętrznych i wewnętrznych kopii bezpieczeństwa i weryfikacja ich poprawności.
21. Zabezpieczenie w wyznaczonych miejscach kopii bezpieczeństwa zbioru danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych osobowych.
22. Oznaczenie w sposób trwały, jednoznaczny i czytelny nośników, na których znajdują się kopie zawierające dane osobowe oraz zaewidencjonowanie ich w **Rejestrze nośników komputerowych zawierających ważne dane.**
23. Niszczenie urządzeń, dysków lub innych informatycznych nośników, zawierających dane osobowe przeznaczone do likwidacji i odnotowanie tego w **Rejestrze nośników komputerowych zawierających ważne dane.**
24. Niszczenie nieprzydatnych kopii archiwalnych i odnotowanie tego w **Rejestrze nośników komputerowych zawierających ważne dane.**
25. Zapewnienie aktywnej ochrony antywirusowej na stacjach roboczych i serwerach oraz bieżącej aktualizacji stosowanych programów.
26. Przeprowadzanie cyklicznych kontroli antywirusowych na wszystkich komputerach – minimum co dwa miesiące.
27. Dokonywanie analizy przyczyn pojawienia się wirusa na zgłoszonych przez użytkowników stacjach roboczych i nośnikach pamięci.
28. Monitorowanie legalności oprogramowania wykorzystywanego na stacjach roboczych.
29. Aktualizowanie oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa stabilności nowych wersji.
30. Nadzorowanie wykonywania przeglądów i konserwacji urządzeń wchodzących w skład systemu informatycznego w terminach określonych przez ich producenta.

31. Usuwanie nieprawidłowości w działaniach systemu informatycznego oraz oprogramowania i ustalanie przyczyny ich wystąpienia.
32. Nadzorowanie prac konserwacyjnych i naprawczych sprzętu komputerowego oraz uaktualnień systemu informatycznego, które są wykonywane przez podmiot zewnętrzny.
33. Usuwanie danych osobowych ze sprzętu komputerowego, którego naprawa jest wykonywana poza Urzędem, a gdy nie ma możliwości usunięcia tych danych, osobiste nadzorowanie jego naprawy.
34. Rejestrowanie działań konserwacyjnych, awarii oraz napraw w **Dzienniku systemu informatycznego UMiG**.
35. Przygotowywanie umów związanych z konserwacją, wdrażaniem oprogramowania, aplikacji oraz urządzeń i systemów informatycznych Urzędu Miasta i Gminy w Kunowie.
36. Przygotowywanie, we współpracy z ABI instrukcji dla użytkowników systemów informatycznych zgodnych z celami i metodologią wdrożonej polityki bezpieczeństwa informacji.
37. Prowadzenie szkoleń na temat bezpiecznych zachowań użytkowników w środowisku systemów IT.
38. Planowanie inwestycji oraz dostaw i usług niezbędnych dla utrzymania i rozwoju środowiska IT w Urzędzie Gminy.

V. ASI wykonuje czynności w imieniu ADO i ABI.

1. Obszarem działania ASI są serwerownie oraz budynek i pomieszczenia biur Urzędu Miasta i Gminy w Kunowie i Urzędu Stanu Cywilnego w Kunowie, w których przetwarzane są dane osobowe w systemach informatycznych.
2. Przedmiotem działania ASI jest również:
 - a. analiza ruchu w sieci LAN i ruchu w sieci WAN w Urzędzie Miasta i Gminy w Kunowie,
 - b. analiza informacji zawartych w kopiach zapasowych oraz w systemowych rejestrach zdarzeń (logach) urządzeń i w systemach informatycznych Urzędu Miasta i Gminy w Kunowie.
3. ASI posiada uprawnienia dostępu do systemów informatycznych Urzędu Miasta i Gminy w Kunowie, umożliwiające mu realizację zadań określonych w niniejszym zarządzeniu.
4. ASI jest uprawniony do zbierania od użytkowników, ich przełożonych oraz innych osób pisemnych wyjaśnień dotyczących powodowania zagrożeń bezpieczeństwa systemów informatycznych w Urzędzie Miasta i Gminy w Kunowie.
5. ASI ma obowiązek prowadzenia analizy i przedstawiania wniosków dotyczących zmiany czynności organizacyjnych i wdrażania w systemach informatycznych zabezpieczeń technicznych mających na celu zapewnienie bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta i gminy w Kunowie.

BURMISTRZ

Zatwierdzam 