Zarządzenie Nr 160/2008
Wójta Gminy Brudzeń Duży
z dnia 10 grudnia 2008 roku

w sprawie Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Gminy w Brudzeniu Dużym

Na podstawie § 3 i 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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. z 2004 r. Nr 100, poz. 1024) zarządza się co następuje:

§ 1

Wprowadza się Instrukcję Zarządzania Systemami Informatycznymi w Urzędzie Gminy w Brudzeniu Dużym stanowiącą załącznik do niniejszego zarządzenia.

§ 2

Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji w Urzędzie Gminy w Brudzeniu Dużym.

§ 3

Traci moc Zarządzenia Nr 89/08 Wójta Gminy Brudzeń Duży z dnia 31stycznia 2008 roku w sprawie wprowadzenia do użytku służbowego instrukcji dotyczącej ochrony danych osobowych w Urzędzie Gminy Brudzeń Duży.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
inż. Henryk Kisielewski

URZĄD GMINY
BRUDZEŃ DUŻY
powiat płocki
woj. mazowieckie
09-414 Brudzeń Duży
tel. 024-260-40-13; 260-40-81
fax 024-260-40-23

Załącznik do Zarządzenia nr 160/2008
Wójta Gminy Brudzeń Duży
z dnia 10 grudnia 2008 roku

SPIS TREŚCI

I. Cel

Instrukcja określa sposób zarządzania systemami informatycznymi, wykorzystywanym do przetwarzania danych i informacji, przez Administratora Danych – w celu zabezpieczenia ich przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

II. Definicje

Ilekroć jest mowa o:

1) **Ustawie** – należy przez to rozumieć ustawę z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
2) **Rozporządzeniu** - należy przez to rozumieć rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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. z 2004 r. Nr 100, poz. 1024),
3) **Administratorze Danych** - należy przez to rozumieć Wójta Gminy Brudzeń Duży,
4) **Administratorze Bezpieczeństwa Informacji** (*ABI*) – należy przez to rozumieć **Sekretarza Urzędu Gminy Brudzeń Duży** pisemnie wyznaczonego przez **Wójta Gminy Brudzeń Duży - Administratora Danych** do nadzorowania przestrzegania zasad przetwarzania danych i informacji oraz wymagań w zakresie ich ochrony, określonych w Polityce Bezpieczeństwa Informacji oraz wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych,
5) **Administratorze Systemów Informatycznych** (*ASI*)– należy przez to rozumieć informatyka Urzędu Gminy pisemnie wskazanego przez **Wójta Gminy Brudzeń Duży - Administratora Danych** do nadzorowania funkcjonowania systemów informatycznych oraz stosowania technicznych i organizacyjnych środków ochrony użytkowanych w tych systemach,
6) **Administratorach Informacji** (*AI*)– należy przez to rozumieć, Sekretarza Gminy oraz Skarbnika Gminy decydujących o narzędziach, metodach, miejscu i czasie przetwarzania, przechowywania, tworzenia i niszczenia informacji chronionych w komórkach organizacyjnych,
7) **Użytkownikach Informacji** (*UI*)– należy przez to rozumieć upoważnionych na piśmie pracowników Urzędu Gminy Brudzeń Duży, którym nadano identyfikator i przyznano hasło, mających dostęp do informacji chronionych. Użytkownikiem informacji może być również osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż, wolontariusz lub inna osoba pod warunkiem uzyskania upoważnienia,
8) **Informacji chronionej** – należy przez to rozumieć wszelkie zapisy na papierze, w układach elektronicznych, na nośnikach magnetycznych, optycznych itp., które ze względu na dobro Urzędu Gminy Brudzeń Duży lub jego interesantów podlegają ochronie przed nieautoryzowanym dostępem, powieleniem, ujawnieniem, modyfikacją, wykorzystaniem, zniszczeniem, utratą, kradzieżą lub zatajeniem,
9) **Przetwarzaniu** – należy przez to rozumieć dokonywanie jakichkolwiek operacji na danych i informacjach, w szczególności, takich jak zbieranie, przechowywanie, opracowywanie, zmienianie, kopiowanie, udostępnianie i usuwanie, a zwłaszcza tych, które wykonuje się w systemach informatycznych,
10) **Systemach przetwarzania** – należy przez to rozumieć systemy tradycyjne oraz systemy informatyczne, w których dokonywane są operacje na danych i informacjach,
11) **Systemie tradycyjnym** – należy przez to rozumieć wszelką dokumentację papierową zawierającą informacje o funkcjonowaniu Urzędu Gminy w Brudzeniu Dużym lub jego interesantach - rejestry, ewidencje, księgi, wykazy oraz inne zbiory danych i informacji, w tym korespondencję z interesantami Urzędu Gminy w Brudzeniu Dużym,

12) **Systemie informatycznym** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, oprogramowanie, zastosowane narzędzia programowe, procedury przetwarzania danych i informacji oraz dane eksploatowane w tych urządzeniach,
13) **Sieci lokalnej** – należy przez to rozumieć połączenie systemów informatycznych Urzędu Gminy Brudzeń Duży wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci Internet,
14) **Teletransmisji** – należy przez to rozumieć przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
15) **Identyfikatorze** - należy przez to rozumieć ciąg znaków literowych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych w systemie informatycznym,
16) **Haśle** - należy przez to rozumieć ciąg znaków literowych, cyfrowych lub znaków specjalnych znanych jedynie osobie uprawnionej do pracy w systemie informatycznym,
17) **Uwierzytelnianiu** - należy przez to rozumieć działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby, polegająca na podaniu identyfikatora osoby upoważnionej oraz związanego z nim hasła,
18) **Rozliczalności** - należy przez to rozumieć właściwość zapewniającą, że działania mogą być przypisane w sposób jednoznaczny tylko Urzędowi Gminy Brudzeń Duży,
19) **Integralności danych** - należy przez to rozumieć właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
20) **Poufności danych** - należy przez to rozumieć właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

III. Poziom bezpieczeństwa

Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemach informatycznych połączonych z siecią publiczną, **wprowadza się „poziom wysoki" bezpieczeństwa** w rozumieniu § 6 rozporządzenia.

IV. Procedury nadawania i zmiany uprawnień do przetwarzania danych oraz ich rejestrowania w systemach informatycznych

Każdy użytkownik systemu informatycznego przed przystąpieniem do przetwarzania danych i informacji musi zapoznać się z:

- Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 z późn. zm.), jeżeli wykonywane obowiązki służbowe są związane z danymi osobowymi,
- Zarządzeniem Nr 159/2008 Wójta Gminy Brudzeń Duży z dnia 10 grudnia 2008 roku w sprawie Polityki Bezpieczeństwa w Urzędzie Gminy w Brudzeniu Dużym,
- Zarządzeniem Nr 160/2008 Wójta Gminy Brudzeń Duży z dnia 10 grudnia 2008 roku w sprawie Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Gminy w Brudzeniu Dużym,
- Podstawowymi zagrożeniami związanymi z przetwarzaniem danych i informacji oraz zastosowanych w celu ich ochrony środków technicznych i organizacyjnych.

1. Podstawowe zasady nadawania i rejestrowania uprawnień

1) Dostęp do systemu informatycznego służącego do przetwarzania danych może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych.
2) Podstawą do nadania uprawnień w systemie oraz dokonania wpisu w Ewidencji osób upoważnionych do przetwarzania danych jest prawidłowo wypełniony Imienny Dokument Uprawnień.
3) Imienny Dokument Uprawnień wykonuje Administrator Informacji.
   Wyżej wymieniony dokument sporządzany jest również w przypadku modyfikacji lub odebrania uprawnień.
4) Dopuszczalne jest sporządzenie Imiennego Dokumentu Uprawnień określającego czas obowiązywania uprawnień.

5) Rejestracja użytkownika informacji polega na nadaniu identyfikatora, przydzieleniu hasła, wprowadzeniu danych do bazy użytkowników systemu oraz wpisu użytkownika informacji do ewidencji osób upoważnionych do przetwarzania danych.

2. Procedura nadawania i rejestrowania uprawnień

1) Administrator Informacji:
   a) podejmuje decyzję o dopuszczeniu do przetwarzania danych osoby, która w związku z wykonywanymi przez siebie obowiązkami będzie miała dostęp do danych i informacji,
   b) wypełnia i podpisuje dla osoby dopuszczonej do przetwarzania danych Imienny Dokument Uprawnień (wzór - **załącznik nr 1**),
   c) przekazuje wypełniony Imienny Dokument Uprawnień Administratorowi Bezpieczeństwa Informacji, w celu akceptacji.
2) Administrator Bezpieczeństwa Informacji bada poprawność dokumentu oraz:
   a) w przypadku braku uwag przekazuje ze swoją akceptacją Administratorowi Systemów Informatycznych, w celu nadania uprawnień użytkownikowi w systemie,
   b) w przypadku uwag zwraca dokument do Administratora Informacji. Na dokumencie dokonuje adnotacji, w której podaje przyczynę odmowy zatwierdzenia dokumentu. Postępowanie określone w punktach 1 i 2 powtarza się do czasu uzyskania akceptacji.
3) Administrator Systemów Informatycznych, zgodnie z przekazanym dokumentem:
   a) nadaje użytkownikowi identyfikator i hasło,
   b) przydziela uprawnienia określone w Imiennym Dokumencie Uprawnień (wzór – **załącznik nr 1**),
   c) przekazuje podpisany Imienny Dokument Uprawnień Administratorowi Bezpieczeństwa Informacji z adnotacją o zarejestrowaniu użytkownika w systemie.
4) Administrator Bezpieczeństwa Informacji:
   a) dokonuje wpisu (aktualizacji) użytkownika informacji w ewidencji osób upoważnionych do przetwarzania danych,
   b) przygotowuje imienne upoważnienie do przetwarzania danych do podpisu przez Administratora Danych. Podpisane upoważnienie przekazuje Administratorowi Informacji celem podpisania przez użytkownika informacji oraz sporządzenia aneksu do zakresu obowiązków.
5) Administratorowi Systemów Informatycznych, w uzasadnionym przypadku, przysługuje prawo zablokowania konta użytkownika w każdym czasie. O zablokowaniu konta niezwłocznie informuje Administratora Bezpieczeństwa Informacji podając przyczyny decyzji.

Uwaga: Procedurę nadania i rejestrowania uprawnień do przetwarzania danych w systemie informatycznym należy stosować odpowiednio w przypadku modyfikacji uprawnień oraz odebrania uprawnień

3. Procedura odebrania i wyrejestrowania uprawnień

1) Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemów Informatycznych na podstawie Imiennego Dokumentu Uprawnień sporządzonego przez Administratora Informacji.
2) Do odebrania uprawnień i wyrejestrowania użytkownika informacji stosuje się odpowiednio postępowanie określone w pkt.**2. ppkt. 1); ppkt.2); ppkt3) i ppkt4)**,
3) Wyrejestrowanie może mieć charakter czasowy lub trwały.
4) Wyrejestrowanie następuje poprzez:
   a) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
   b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).
5) Czasowe wyrejestrowanie użytkownika z systemu informatycznego następuje w razie:
   a) nieobecności użytkownika w pracy trwającej dłużej niż 21 dni kalendarzowych,
   b) zawieszenia w pełnieniu obowiązków służbowych.

6) Przyczyną czasowego wyrejestrowania z systemu informatycznego może być:
   a) wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych,
   b) wypowiedzenie umowy o pracy.
7) Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego.

V. Metody i środki uwierzytelnienia w systemach informatycznych oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Metody i środki uwierzytelniania

1) W systemach informatycznych stosuje się uwierzytelnienia dwustopniowe, na poziomie:
   a) dostępu do stacji roboczej,
   b) dostępu do aplikacji.
2) Do uwierzytelnienia użytkowników informacji w systemach stosuje się identyfikatory oraz hasła.
3) Identyfikator składa się z litery odpowiadającej pierwszej literze imienia użytkownika oraz kolejnym literom jego nazwiska. W identyfikatorze pomija się polskie znaki diakrytyczne.
4) W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika Administrator Systemów Informatycznych, za zgodą Administratora Bezpieczeństwa Informacji, nadaje użytkownikowi inny identyfikator, odstępując od zasady określonej wyżej.
5) Hasło na poziomie dostępu do aplikacji/sytemu składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika informacji ani jego imieniem lub nazwiskiem.
6) Hasło nie może być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
7) Hasło nie może być ujawnione nawet po utracie przez nie ważności.
8) Użytkownik nie może udostępniać swojego identyfikatora i hasła osobom trzecim.
9) Zabronione jest korzystania z identyfikatora i hasła innego użytkownika.
10) Zmiana hasła następuje:
   a) nie rzadziej niż co 30 dni w przypadku dostępu do aplikacji/systemów, w których przetwarzane są dane osobowe,
   b) nie rzadziej niż co 90 dni w przypadku dostępu do innych aplikacji/systemów niż wymienione wyżej,
   c) niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.

2. Procedury zarządzania środkami uwierzytelniania

1) Administrator Systemów Informatycznych nadaje hasło dostępu do aplikacji/systemu dla nowego użytkownika albo dla użytkownika, który zapomniał swoje ostatnie hasło dostępu. Przekazywanie hasła użytkownikowi informacji przez Administratora Systemów Informatycznych odbywa się w sposób poufny. Nie może ono być zapisywane w miejscu pozwalającym na dostęp osób nieupoważnionych.
2) Użytkownik dokonuje uwierzytelnienia w systemie w obecności Administratora Systemów Informatycznych.
3) Użytkownik systemu po pierwszym logowaniu niezwłocznie ustala swoje własne hasło, zgodnie z zasadami określonymi w punkcie 1. ppkt. 5 i 6.
4) Użytkownik systemu w trakcie pracy w aplikacji może zmieniać swoje hasło dostępu. O każdej zmianie hasła dostępu użytkownik informuje Administratora Systemów Informatycznych.
5) Administrator Systemów Informatycznych prowadzi rejestr zmian haseł użytkowników systemów/programów (wzór – **załącznik nr 2**).

6) Administrator Systemów Informatycznych przekazuje Administratorowi Bezpieczeństwa Informacji swój identyfikator oraz hasła dostępu w zamkniętej kopercie. Koperta jest zabezpieczona w sposób uniemożliwiający jej nieupoważnione otwarcie. Administrator Bezpieczeństwa Informacji przechowuje kopertę w pokoju nr 5. Z otwarcia koperty zawierającej identyfikator i hasło dostępu Administratora Systemów Informatycznych sporządza się protokół.

VI. Procedury rozpoczęcia, zawieszenia i zakończenia pracy

1. Procedura rozpoczęcia pracy

1) Użytkownik informacji przed rozpoczęciem pracy powinien zwrócić uwagę, czy nie istnieje prawdopodobieństwo naruszenia bezpieczeństwa przetwarzanych danych. Jeżeli poweźmie takie podejrzenie, musi postępować zgodnie z procedurą określoną w **punkcie XIII**.
2) Rozpoczęcie pracy w systemie informatycznym następuje po włączeniu monitora, stacji roboczej i drukarki.
3) Uruchomienie aplikacji/systemu, następuje poprzez wprowadzenie identyfikatora i hasła dostępu. Hasło dostępu musi być podawane (wprowadzane) w sposób dyskretny (nie literowane, nie czytane na głos). Hasło dostępu musi być wpisywane osobiście przez użytkownika.
4) Przystąpienie do wykonywania obowiązków służbowych.

2. Procedura zawieszenia pracy

Użytkownik informacji zobowiązany jest do:

1) Aktywowania wygaszacza ekranu, przy każdorazowym opuszczaniu stanowiska stacji roboczej,
2) Upewnienia się, że w czasie jego nieobecności, na monitorze stacji roboczej nie będą wyświetlane żadne dane i informacje,
3) Ustawienia ręcznego blokady stacji roboczej lub wygaszacza ekranu w przypadku opuszczaniu pokoju na dłuższy czas.

3. Procedura zakończenia pracy

W celu zakończenia pracy użytkownik zobowiązany jest do:

1) wprowadzenia (zapisania) przetwarzanych danych i informacji w odpowiednie bazy/zbiory,
2) zamknięcia aplikacji,
3) zamknięcia systemu,
4) wyłączenia monitora, drukarki i stacji roboczej.

Przed opuszczeniem pokoju użytkownik informacji musi:

1) zniszczyć w niszczarce lub schować do szaf zamykanych na klucz wszelkie wykonane wydruki zawierające dane i informacje,
2) schować do zamykanych na klucz szaf wszelkie akta zawierające dane i informacje,
3) umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,
4) zamknąć okna.

Opuszczając pokój drzwi należy zamknąć na klucz, a następnie klucz oddać do przechowania do Sekretariatu.

4. Tryb pracy na stacjach roboczych (stacjonarnych)

1) W pomieszczeniu, w którym przetwarzane są dane, osoby postronne mogą znajdować się tylko za zgodą i w obecności użytkownika informacji.
2) Należy chronić ekrany stacji roboczych (ustawienie monitora uniemożliwiające podgląd) oraz wydruki znajdujące się na biurku i w otwartych szafach przed osobami postronnymi.
3) Monitory stacji roboczych wyposażone są we włączające się po 15 minutach, od przerwania pracy, wygaszacze ekranu. Wznowienie wyświetlenia następuje po wprowadzeniu odpowiedniego hasła.
4) Zakazuje się robienia kopii całych zbiorów danych przez użytkowników informacji. Całe zbiory danych i informacji mogą być kopiowane tylko przez Administratora Systemów

Informatycznych lub automatycznie przez system, z zachowaniem procedur ich ochrony.

5) Jednostkowe dane mogą być kopiowane na zewnętrzne nośniki magnetyczne, optyczne. Nośniki te są przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane.
6) Przesyłanie danych pocztą elektroniczną może odbywać się tylko w postaci zaszyfrowanej.
7) Zakazuje się wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej.
8) Użytkownicy informacji zobowiązani są do odpowiednio częstego robienia kopii roboczych przetwarzanych danych i informacji, na których się właśnie pracuje, aby zapobiec ich utracie.

VII. Procedury tworzenia kopii zapasowych zbiorów oraz programów i narzędzi programowych służących do ich przetwarzania

1) Administrator Systemów Informatycznych prowadzi rejestr wykonywanych kopii, sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność (wzór – **załącznik nr 4**).
2) W celu sprawdzenia poprawności wykonywanych kopii Administrator Systemów Informatycznych poddaje testowi wybraną kopię. Próba polega na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość odczytania danych.
3) Administrator Bezpieczeństwa Informacji na wniosek Administratora Systemów Informatycznych zatwierdza wykaz informacji chronionych. Dane te oraz dane przechowywane w pamięci stacji roboczych i serwerów sieciowych archiwizowane są w cyklu określonym przez Administratora Systemów Informatycznych na odpowiednich nośnikach informatycznych.
4) Administratorzy Informacji dokonują oceny danych przechowywanych w pamięci stacji roboczych pod kątem ich ważności dla obsługi interesantów oraz funkcjonowania referatów i Urzędu Gminy w Brudzeniu Dużym, kwalifikują je jako informacje chronione oraz zobowiązują pisemnie użytkowników informacji (pracowników) do ich kopiowania w sposób określony w pkt.5, 6, 7 i 8 (wzór – **załącznik nr 6**).
5) Użytkownicy są zobowiązani do wykonywania kopi zapasowych swoich danych przechowywanych w pamięci stacji roboczych/serwera oraz programów i narzędzi programowych, w sposób określony przez Administratora Systemów Informatycznych oraz Administratorów Informacji (użytkownicy powinni przyjąć zasadę codziennego sporządzania kopii wszystkich danych, które uległy zmianie tego dnia).
6) Dopuszcza się tworzenie kopii zapasowych (archiwalnych) na innych, oddzielnych nośnikach informacji.
7) Kopie zapasowe, o których mowa, wyżej tworzy się:
   a) codziennie – na koniec dnia kopię wszystkich danych, które uległy zmianie tego dnia,
   b) raz w tygodniu – na koniec tygodnia kopie wszystkich danych bez względu czy uległy zmianie czy nie,
8) Nośniki zawierające kopie zapasowe należy oznaczać jako *„Kopia zapasowa tygodniowa/miesięczna”* wraz z podaniem daty sporządzenia.
9) Dostęp do kopii zapasowych posiada Administrator Systemów Informatycznych oraz Administrator Bezpieczeństwa Informacji.
10) Kopie czasowe tworzy się na oddzielnych nośnikach informatycznych zgodnie z zasadami określonymi w Rozdziale VI, pkt.5, p.pkt 3) Polityki Bezpieczeństwa Informacji.

VIII. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane oraz wydruków i kopii zapasowych

1. Elektroniczne nośniki informacji

1) Dane w postaci elektronicznej przetwarzane w systemach informatycznych, zapisane na dyskietkach, dyskach magnetooptycznych, dyskach twardych, pendrivach itp. nie mogą

być wynoszone poza siedzibę Urzędu Gminy Brudzeń Duży bez zgody Administratorów Informacji.

Fakt przetwarzania danych poza siedzibą Urzędu Gminy Brudzeń Duży musi być odnotowany w prowadzonej ewidencji (wzór – **załącznik nr** 7).

2) Wymienne, elektroniczne nośniki informacji przechowywane są w pokojach stanowiących obszar przetwarzania danych, określonych w Zarządzeniu Nr 159 /2008 Wójta Gminy Brudzeń Duży z dnia 10 grudnia 2008 roku w sprawie Polityki Bezpieczeństwa w Urzędzie Gminy w Brudzeniu Dużym. Po zakończeniu pracy są zabezpieczane w zamykanych w szafach biurowych lub kasetkach.
3) Z danych przetwarzanych w pamięci stacji roboczych oraz komputerów przenośnych muszą być bezwzględnie wykonywane kopie zapasowe na odpowiednich nośnikach informacji, zgodnie z procedurami określonymi w Polityce Bezpieczeństwa i Instrukcji Zarządzania Systemami Informatycznymi.
4) Dane w postaci elektronicznej należy usunąć z nośnika informacji w sposób uniemożliwiający ich ponowne odtworzenie, nie później niż po upływie 3 dni, po wykorzystaniu tych danych chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania. O usunięciu danych decyduje Administrator Informacji.
5) Wymienne elektroniczne nośniki danych powinny być oznaczone w sposób określony w Zarządzeniu Nr 159 /2008 Wójta Gminy Brudzeń Duży z dnia 10 grudnia 2008 roku w sprawie Polityki Bezpieczeństwa w Urzędzie Gminy w Brudzeniu Dużym.
6) W przypadku uszkodzenia lub zużycia nośnik, zawierający dane, należy zniszczyć fizycznie w taki sposób, by nie można było odczytać jego zawartości (w niszczarce służącej do niszczenia nośników, przecięcia lub przełamania).
7) Nośniki wielorazowego użytku, takie jak dyski twarde, dyskietki, płyty CD - RW, DVD - RW, można wykorzystać ponownie do celów przechowywania kopii bezpieczeństwa, po uprzednim usunięciu ich zawartości.
8) Urządzenia, dyski oraz inne elektroniczne nośniki informacji przeznaczone do likwidacji muszą być pozbawione zapisów lub trwale uszkodzone w sposób uniemożliwiający odczytanie z nich danych. Likwidacja prowadzona jest zgodnie z obowiązującymi w Urzędzie Gminy przepisami dotyczącymi gospodarki środkami trwałymi oraz wartościami niematerialnymi.
9) Urządzenia, dyski oraz inne elektroniczne nośniki informacji przeznaczone do przekazania podmiotowi nieuprawnionemu do przetwarzania danych na nich zawartych muszą być wcześniej pozbawione zapisu tych danych w sposób uniemożliwiający ich odzyskanie.
10) Urządzenia, dyski lub inne elektroniczne nośniki informacji przeznaczone do naprawy muszą być pozbawione danych w sposób uniemożliwiający ich odzyskanie lub być naprawiane pod nadzorem Administratora Systemów Informatycznych.

2. Kopie zapasowe

1) Kopie zapasowe, wykonywane zgodnie z procedurą określoną w punkcie VII, p.pkt.3-5, zbiorów danych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w kasie pancernej. Każde wydanie i przyjęcie kopii jest odnotowywane w rejestrze.
2) Zabronione jest przechowywanie kopii zapasowych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.
3) Dostęp do szafy, w której są przechowywane kopie zapasowe, mają tylko osoby upoważnione, tj. Administrator Bezpieczeństwa Informacji, Administrator Systemów Informatycznych oraz Inspektor ds. obronnych, obrony cywilnej i zarządzania kryzysowego.
4) Kopie zapasowe likwiduje się niezwłocznie po ustaniu ich przydatności i użyteczności.

3. Wydruki

1) Wydruki zawierające dane są przechowywane w zamkniętych szafach, w pokojach

stanowiących obszar przetwarzania danych, określonych w Zarządzeniu Nr 159/2008 Wójta Gminy Brudzeń Duży z dnia 10 grudnia 2008 roku w sprawie Polityki Bezpieczeństwa Informacji w Urzędzie Gminy w Brudzeniu Dużym.

2) Wydruki zawierające dane należy zniszczyć przez pocięcie w specjalnym urządzeniu /niszczarce/ nie później niż po upływie 3 dni, po ich wykorzystaniu chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania. O zniszczeniu wydruków decyduje Administrator Informacji.

4. Dane wejściowe do systemu

1) Dane zapisane w formie papierowej, innej niż wydruki z systemów (pisma, ankiety, formularze itp.), są przechowywane na tych samych zasadach jak wydruki.
2) Formularze zgody z podpisami osób, których dotyczą dane przetwarzane w systemach, przechowywane są w pokojach stanowiących obszar przetwarzania danych, określonych w Zarządzeniu Nr 159 /2008 Wójta Gminy Brudzeń Duży z dnia 10 grudnia 2008 roku w sprawie Polityki Bezpieczeństwa Informacji w Urzędzie Gminy w Brudzeniu Dużym.
3) Z danymi zapisanymi w formie elektronicznej należy postępować w sposób opisany w rozdziale VI, pkt.5 Polityki Bezpieczeństwa Informacji.

IX. Środki ochrony systemów przed złośliwym oprogramowaniem, w tym wirusami komputerowymi i nieuprawnionym dostępem

1. Ochrona antywirusowa

1) Za ochronę antywirusową odpowiada Administrator Systemów Informatycznych. Do jego obowiązków należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów, dokonywanych przez oprogramowanie antywirusowe.
2) Sprawdzanie obecności wirusów komputerowych w systemach informatycznych oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych.
3) Użytkownik jest obowiązany zawiadomić Administratora Systemów Informatycznych o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.
4) W celu ochrony przed wirusami komputerowymi używanie nośników danych (dyskietki, dyski optyczne itp.) spoza Urzędu Gminy jest dopuszczalne dopiero po uprzednim sprawdzeniu ich przy pomocy programu antywirusowego. Jeżeli stanowisko użytkownika nie jest wyposażone w program antywirusowy, nośnik danych należy przekazać do sprawdzenia przez Administratora Systemów Informatycznych.
5) W przypadku stwierdzenia obecności wirusów komputerowych w systemie należy postępować w sposób opisany w **punkcie XIII.**
6) Użytkownik systemu na stanowisku komputerowym, importujący dane do systemu informatycznego jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów.

2. Ochrona przed nieautoryzowanym dostępem, bezpieczeństwo i zasady pracy w sieci komputerowej

1) Urządzenia systemu informatycznego służącego do przetwarzania danych ważnych dla obsługi interesantów i funkcjonowania Urzędu Gminy nie mogą być połączone z siecią Internet. Listę urządzeń i systemów połączonych z siecią Internet zatwierdza Administrator Bezpieczeństwa Informacji na wniosek Administratora Systemów Informatycznych.
2) Na stanowiskach komputerowych mających dostęp do Internetu musi być zainstalowane oprogramowanie antywirusowe oraz zainstalowany program Firewall.
3) Korzystanie z Internetu jest możliwe tylko w przypadku, jeżeli jest to niezbędne do wykonywania obowiązków służbowych.
4) Zabronione jest otwieranie załączników poczty elektronicznej nieznanego typu lub pochodzące z podejrzanej korespondencji.

5) Zasoby informatyczne takie jak foldery, drukarki udostępnia Administrator Systemów Informatycznych.
6) Użytkownik nie może zmieniać adresu IP oraz innych parametrów urządzeń komunikacji sieciowej.
7) Użytkownik informacji jest zobowiązany do ścisłego przestrzegania zasad pracy w sieci określonych w Polityce Bezpieczeństwa i Rozdziale V, pkt. 1. Instrukcji Zarządzania Systemami Informatycznymi.

X. Zasady i sposób odnotowywania w systemach informacji o udostępnieniu danych

1) Udostępnienie danych może nastąpić wyłącznie na wniosek odbiorcy danych zgodnie z zasadami określonymi w Polityce Bezpieczeństwa.
2) Odbiorcą danych jest każdy, komu udostępnia się dane, z wyłączeniem:
   - ✓ osoby, której dane dotyczą,
   - ✓ osoby użytkownika systemu lub innej osoby upoważnionej do przetwarzania danych w Urzędzie Gminy,
   - ✓ przedstawiciela, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych,
   - ✓ podmiotu, któremu powierzono przetwarzanie danych,
   - ✓ organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
3) Odnotowanie obejmuje informacje o:
   a) nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane,
   b) zakresie udostępnianych danych,
   c) dacie udostępnienia,
4) Obowiązek odnotowania ww. informacji spoczywa na użytkowniku informacji (pkt. VI ust. 7 Polityki Bezpieczeństwa) .
5) Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.
6) Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnieniu danych należy umieścić w raporcie, a raport przekazać tej osobie.
7) W przypadku braku możliwości odnotowywania przez system informatyczny udostępnienia danych, informację o tym należy zamieścić w ewidencji udostępniania danych prowadzonej w formie papierowej lub elektronicznej (wzór - **załącznik 8**).
8) Bezpośredni nadzór nad udostępnianiem danych sprawuje Administrator Informacji. Natomiast nadzór nad prawidłowością udostępniania danych sprawuje Administrator Bezpieczeństwa Informacji.

XI. Procedury wykonywania naprawy urządzeń oraz przeglądów i konserwacji systemów, w tym elektronicznych nośników informacji służących do przetwarzania danych

O przeprowadzanych przeglądach i konserwacjach systemu, w każdym przypadku informowany jest Administrator Bezpieczeństwa Informacji, który może być przy nich obecny.

Kontrole i testy przeprowadzane przez Administratora Bezpieczeństwa Informacji mogą obejmować zarówno dostęp do zasobów systemów, jak i profile oraz uprawnienia poszczególnych użytkowników.

1. Przeglądy i konserwacja urządzeń

1) Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu.
2) Ocenie podlegają: stan techniczny urządzeń (komputery, serwery, UPS-y, itp.), stan okablowania budynku w sieć logiczną, spójność baz danych.
3) Nieprawidłowości ujawnione w trakcie przeglądów i konserwacji powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić Administratora Bezpieczeństwa Informacji.

4) Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada Administrator Systemów Informatycznych.

2. Przegląd programów i narzędzi programowych

1) Przeglądu pliku zawierającego raport dotyczący działania aplikacji bądź systemu (log systemowy) dokonuje Administrator Systemów Informatycznych nie rzadziej niż raz na miesiąc. Zapisy logów systemowych są przeglądane przez Administratora Systemów Informatycznych każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.
2) Przeglądu i sprawdzenia poprawności zbiorów danych dokonuje użytkownik przy współudziale Administratora Systemów Informatycznych.
3) Przegląd programów i narzędzi programowych przeprowadzany jest w następujących przypadkach:
   a) zmiany wersji oprogramowania stanowiska komputerowego użytkownika systemu,
   b) zmiany systemu operacyjnego stanowiska komputerowego użytkownika systemu,
   c) wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modyfikacji systemu.
4) Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych. Sprawdzenie powinno obejmować:
   a) poprawność logowania się do systemu w zależności od posiadanych uprawnień (zasymulować pracę wszystkich typów uprawnień użytkownika),
   b) poprawność działania wszystkich elementów aplikacji (menu, zestawienia, formularze, raporty),
   c) poprawność funkcjonalną systemu symulując działania wszystkich grup użytkowników wykonując następujące operacje:
      ✓ wprowadzanie danych,
      ✓ edytowanie danych,
      ✓ wyszukiwania danych,
      ✓ wydruk danych.
5) Przegląd przeprowadza projektant systemu w obecności Administratora Systemów Informatycznych.
6) Za prawidłowość przeprowadzenia przeglądu programów i narzędzi programowych systemów odpowiada Administrator Systemów Informatycznych.

3. Zarządzanie oprogramowaniem systemowym i użytkowym

1) Nośniki informatyczne zakupionego oprogramowania operacyjnego, narzędziowego i aplikacyjnego przechowywane są w chronionym i zabezpieczonym przed nieuprawnionym dostępem miejscu.
2) Administrator Systemów Informatycznych prowadzi rejestr oprogramowania z określeniem użytkowników, którym zostało ono udostępnione (wzór rejestru - **załącznik nr 3**).
3) Użytkownik może korzystać z udostępnionego oprogramowania jedynie w celu wykonywania obowiązków służbowych.
4) Zabronione jest wykonywanie przez użytkownika jakichkolwiek instalacji oprogramowania bez zgody Administratora Systemów Informatycznych.
5) Użytkownikowi nie wolno dokonywać jakichkolwiek zmian w konfiguracji systemu operacyjnego.

4. Konserwacja oprogramowania

1) Konserwację oprogramowania przeprowadza się po zgłoszeniu przez użytkownika systemu potrzeby wprowadzenia zmian pozwalających utrzymać funkcjonalność systemu w dynamicznie zmieniającym się środowisku pracy.
2) Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych, na testowej bazie danych, na podobnych zasadach jak ma to miejsce w przypadku przeglądu oprogramowania.

3) Konserwacja przeprowadzana jest w obecności Administratora Systemów Informatycznych.

5. Naprawa urządzeń

1) Naprawa urządzeń komputerowych oraz zmiany w systemach informatycznych przeprowadzane są pod nadzorem Administratora Systemów Informatycznymi.
2) Naprawa urządzeń oraz zmiany w systemach informatycznych wykonywane przez serwisanta w siedzibie Urzędu Gminy mogą być prowadzone tylko zgodnie z zasadami określonymi w **rozdziale VI, pkt. 3** Polityki Bezpieczeństwa Informacji.
3) Naprawy urządzeń poza siedzibą Urzędu Gminy mogą być dokonywane po spełnieniu warunków określonych w **rozdziale VI, pkt. 3** Polityki Bezpieczeństwa Informacji.

XII. Przetwarzanie danych w zbiorach doraźnych

1) Dostęp do danych odbywa się poprzez aplikacje. Gdy zachodzi potrzeba zapisania danych w innym formacie np. dane do raportu w postaci pliku arkusza kalkulacyjnego, można tego dokonać w doraźnym zbiorze danych pod warunkiem, że zapisane dane będą należycie chronione, tj.:
   a) uniemożliwi się dostęp do danych osobom nieuprawnionym,
   b) uniemożliwi się zmianę danych, a tym samym sfałszowanie informacji pochodzących z systemu,
   c) zabezpieczy się bezpośredni dostęp do danych hasłem.
2) Doraźny zbiór danych należy usunąć z nośnika danych, na którym został utworzony lub zniszczyć nośnik, nie później niż 3 dni po wykorzystaniu danych. O usunięciu danych lub nośnika decyduje Administrator Informacji.
3) Dane w zbiorach doraźnych mogą być przetwarzane wyłącznie w pokojach stanowiących obszar przetwarzania danych.
4) W przypadku stwierdzenia lub podejrzenia nieuprawnionego dostępu do danych w zbiorze należy niezwłocznie zawiadomić Administratora Bezpieczeństwa Informacji oraz postępować zgodnie z procedurą określoną w **Rozdziale XIII.**

XIII. Postępowanie w przepadku stwierdzenia naruszenia zasad bezpieczeństwa przetwarzanych danych w systemach informatycznych

1) Domniemanie, przesłanka czy fakt wskazujące na naruszenie zasad ochrony danych, a zwłaszcza stan różny od ustalonego w systemie informatycznym, jest dla użytkownika podstawą do podjęcia natychmiastowego działania.
2) O sytuacji odbiegającej od normy, w szczególności o przesłankach naruszenia lub podejrzenia naruszenia zasad ochrony danych w systemie informatycznym, użytkownik zobowiązany jest natychmiast poinformować Administratora Informacji oraz Administratora Systemów Informatycznych, a zwłaszcza o:
   a) naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła),
   b) częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień,
   c) braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera,
   d) wykryciu wirusa komputerowego,
   e) zauważeniu elektronicznych śladów próby włamania do systemu informatycznego,
   f) znacznym spowolnieniu działania systemu informatycznego,
   g) podejrzeniu próby kradzieży sprzętu komputerowego lub dokumentów zawierających dane,
   h) zmianie położenia sprzętu komputerowego,
   i) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub szaf.
   j) stanie urządzeń (brak zasilania, problemy z uruchomieniem),
   k) stanie systemu zabezpieczeń obiektu (urządzenia alarmowe itp.),
   l) stanie aktywnych urządzeń sieciowych i pozostałej infrastruktury informatycznej,

m) faktach świadczących o działaniu systemu poza dozwolonym czasem pracy,
n) przebywaniu osób nieuprawnionych w obszarze przetwarzania danych.

3) Do czasu przybycia na miejsce Administratora Systemów Informatycznych użytkownik stwierdzający naruszenie przepisów lub stan mogący mieć wpływ na bezpieczeństwo danych i systemu zobowiązany jest do możliwie pełnego udokumentowania zdarzenia (np. zapisania treści komunikatów), celem precyzyjnego określenia przyczyn i ewentualnych skutków naruszenia obowiązujących zasad, a w szczególności:
   a) niezwłocznego podjęcia czynności niezbędnych dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnienia w działaniu również ustalenia jego przyczyn lub sprawców,
   b) rozważenia wstrzymania bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   c) zaniechania dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
   d) zastosowania się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku,
   e) przygotowania opisu incydentu,
   f) nie opuszczania bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia Administratora Systemów Informatycznych.
4) Stwierdzenie przez Administratora Systemów Informatycznych naruszenia zasad ochrony danych wymaga natychmiastowego powiadomienia Administratora Bezpieczeństwa Informacji oraz podjęcia natychmiastowych działań poprzez:
   a) usunięcie uchybień (wymiana niesprawnego zasilacza awaryjnego, usunięcie wirusów z systemu komputerowego, itp.),
   b) zastosowanie dodatkowych środków zabezpieczających zgromadzone dane,
   c) wstrzymanie przetwarzania danych do czasu usunięcia awarii systemu informatycznego.
5) Administrator Bezpieczeństwa Informacji po otrzymaniu zawiadomienia powinien niezwłocznie:
   a) przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych,
   b) podjąć działania chroniące system przed ponownym naruszeniem,
   c) w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport naruszenia bezpieczeństwa systemu informatycznego, a następnie niezwłocznie przekazać go Administratorowi Danych.
6) Administrator Bezpieczeństwa Informacji w uzgodnieniu z Administratorem Systemów Informatycznych może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.
7) W przypadku odtwarzania danych z kopii zapasowych Administrator Systemów Informatycznych obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu (dotyczy to zwłaszcza przypadków infekcji wirusowej).
8) Administrator Danych po zapoznaniu się z raportem naruszenia bezpieczeństwa systemu informatycznego podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych czynności zapewniających bezpieczeństwo systemu informatycznego lub zastosowaniu środków ochrony fizycznej.
9) Administrator Bezpieczeństwa Informacji i Administrator Systemów Informatycznych zobowiązani są do informowania Administratora Danych o awariach systemu informatycznego, stwierdzonych przypadkach naruszenia Instrukcji Zarządzania Systemami Informatycznymi przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego korzystania ze sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.

Uwaga: Procedurę naruszenia zasad bezpieczeństwa przetwarzanych danych w systemach informatycznych stosuje się odpowiednio w przypadku naruszenia zasad bezpieczeństwa przetwarzanych danych w systemie tradycyjnym

XIV. Postanowienia końcowe

1) W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
2) Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do zapoznania się, przed dopuszczeniem do przetwarzania danych, z niniejszą instrukcją oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści.
3) Osobie upoważnionej do przetwarzania danych i informacji Administrator Bezpieczeństwa Informacji przekazuje wyciąg z Instrukcji Zarządzania Systemami Informatycznymi, przygotowany z uwzględnieniem jej stanowiska (obowiązków).
4) Niezastosowanie się do procedur określonych w niniejszej instrukcji przez pracowników upoważnionych do przetwarzania danych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym na podstawie Kodeksu Pracy.
5) Osoby naruszające zasady i procedury określone w Instrukcji Zarządzania Systemami Informatycznymi będą pociągnięte do odpowiedzialności karnej, na podstawie art. 51-52 ustawy oraz art. 266 Kodeksu Karnego.

Instrukcja Zarządzania Systemami Informatycznymi wchodzi w życie z dniem 10 grudnia 2008 roku.

Dokumenty powiązane:

Zarządzenie Nr 159 /2008 Wójta Gminy Brudzeń Duży z dnia 10 grudnia 2008 roku w sprawie Polityki Bezpieczeństwa w Urzędzie Gminy w Brudzeniu Dużym.

Administrator
SEKRETARZ GMINY
Barbara Błaszkiewicz
Bezpieczeństwa Informacji

Załączniki:

Załącznik nr 1 - Imienny Dokument Uprawnień

Załącznik nr 2 - Rejestr zmian hasła użytkownika systemu/programu

Załącznik nr 3 - Rejestr udostępnionego oprogramowania

Załącznik nr 4 - Rejestr kopii zapasowych (bezpieczeństwa danych)

Załącznik nr 5 – Raport naruszenia bezpieczeństwa danych/systemu informatycznego w Urzędzie Gminy w Brudzeniu Dużym

Załącznik nr 6 - Rejestr wykonywanych kopii zapasowych w Urzędzie Gminy w Brudzeniu Dużym

Załącznik nr 7 - Ewidencja przetwarzania danych poza siedzibą Urzędu Gminy w Brudzeniu Dużym

Załącznik nr 8 - Ewidencja udostępniania danych

Załącznik nr 1

Imienny Dokument Uprawnień

<table>
<tr><td colspan="2">□ Nowy użytkownik</td><td colspan="2">□ Modyfikacja uprawnień</td><td>□ Odebranie uprawnień</td></tr>
<tr><td colspan="3">Imię i nazwisko użytkownika:</td><td colspan="2">Referat:</td></tr>
<tr><td colspan="3">Stanowisko:</td><td>Pokój nr:</td><td>Telefon nr:</td></tr>
<tr><td colspan="3">Nazwa systemu/programu</td><td colspan="2">Zakres uprawnień</td></tr>
<tr><td colspan="3" rowspan="2">1.

Login:</td><td colspan="2">forma papierowa □ przetwarza dane osobowe
□ zbieranie □ przechowywanie
□ zmienianie □ usuwanie
□ opracowywanie □ przekazywanie
□ kopiowanie</td></tr>
<tr><td colspan="2">forma elektroniczna □ przetwarza dane osobowe
□ zbieranie □ przechowywanie
□ zmienianie □ usuwanie
□ opracowywanie □ przekazywanie
□ kopiowanie</td></tr>
<tr><td colspan="3" rowspan="2">2.

Login:</td><td colspan="2">forma papierowa □ przetwarza dane osobowe
□ zbieranie □ przechowywanie
□ zmienianie □ usuwanie
□ opracowywanie □ przekazywanie
□ kopiowanie</td></tr>
<tr><td colspan="2">forma elektroniczna □ przetwarza dane osobowe
□ zbieranie □ przechowywanie
□ zmienianie □ usuwanie
□ opracowywanie □ przekazywanie
□ kopiowanie</td></tr>
<tr><td colspan="3" rowspan="2">3.

Login:</td><td colspan="2">forma papierowa □ przetwarza dane osobowe
□ zbieranie □ przechowywanie
□ zmienianie □ usuwanie
□ opracowywanie □ przekazywanie
□ kopiowanie</td></tr>
<tr><td colspan="2">forma elektroniczna □ przetwarza dane osobowe
□ zbieranie □ przechowywanie
□ zmienianie □ usuwanie
□ opracowywanie □ przekazywanie
□ kopiowanie</td></tr>
<tr><td colspan="5">Zasady zastępstwa i/lub okres ważności uprawnień:</td></tr>
<tr><td colspan="2">Administrator Informacji Data i podpis:</td><td colspan="3">Administrator Systemów Informatycznych Data i podpis:</td></tr>
<tr><td colspan="2">Upoważnienie Nr...../...</td><td colspan="3">Administrator Bezpieczeństwa Informacji Data i podpis:</td></tr>
</table>

Załącznik nr 2

Rejestr zmian hasła użytkownika systemu/programu

System/program : .....

Użytkownik : .....

Identyfikator : .....

Data rejestracji : .....

Data wyrejestrowania : .....

Lp.	Data	Przyczyna zmiany	Podpis Administratora Systemów Informatycznych	Podpis użytkownika informacji	Uwagi
1	2	3	4	5	6

Załącznik nr 8

EWIDENCJA UDOSTĘPNIANIA DANYCH
w systemie .....

Lp.	Nazwa i adres podmiotu któremu udostępniono dane	Data udostępnienia	Zakres udostępnionych danych	Login / imię i nazwisko użytkownika informacji udostępniającego dane
1	2	3	4	5

EWIDENCJA UDOSTĘPNIANIA DANYCH
w Urzędzie Gminy Brudzeń Duży

Lp.	Nazwa i adres podmiotu któremu udostępniono dane	Data udostępnienia	Zakres udostępnionych danych	Nazwa zbioru, rejestru, programu	Login / imię i nazwisko użytkownika informacji udostępniającego dane
1	2	3	4	5	6