**Zarządzenie Nr ADM/117/2019
Wójta Gminy Starogard Gdański**

z dnia 17 października 2019 r.

**w sprawie wprowadzenia Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy Starogard Gdański**

Działając w oparciu o Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) (Dz. Urz .UE L119 z 4 maja 2016 r.), ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000) oraz rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2016 r., poz. 113) zarządza się, co następuje:

**§ 1.**Wprowadza się Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy Starogard Gdański, stanowiący załącznik do Zarządzenia.

**§ 2.**Zarządzenie wchodzi w życie z dniem 17 października 2019 r.

|  |  |
| --- | --- |
|  | Wójt**Magdalena Forc-Cherek** |

Załącznik Nr 1 do zarządzenia Nr ADM/117/2019
Wójta Gminy Starogard Gdański
z dnia 17 października 2019 r.

**INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM
W URZĘDZIE GMINY STAROGARD GDAŃSKI**

**Rozdział 1.**
**Postanowienia ogólne**

**§ 1.**Celem Instrukcji jest określenie warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

**§ 2.**Ilekroć w niniejszym dokumencie jest mowa o :

1) **Urzędzie** – należy przez to rozumieć Urząd Gminy Starogard Gdański,83-200 Starogard Gdański ul. Sikorskiego 9

2) **Wójcie** – należy przez to rozumieć Panią Wójt Gminy Starogard Gdański

3) **Administratorze Danych (ADO)** – należy przez to rozumieć Panią Wójt Gminy

4) **Inspektor Ochrony Danych Osobowych (IOD)** – należy przez to rozumieć pracownika Urzędu wyznaczonego przez ADO do nadzorowania, przestrzegania zasad ochrony danych osobowych określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych,

5) **Administratorze Systemu Informatycznego (ASI)** – należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznego Urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony danych w systemach informatycznych,

6) **użytkowniku systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym Urzędu. Użytkownikiem może być pracownik Urzędu, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno – prawnej, osoba odbywająca staż, praktykę lub wolontariat w Urzędzie,

7) **pracowniku** – należy przez to rozumieć osobę zatrudnioną w Urzędzie na podstawie umowy o pracę, osobę wykonującą czynności na podstawie umowy cywilnoprawnej, stażystę, praktykanta lub wolontariusza,

8) **przetwarzaniu danych –** należy przez to rozumieć jakiekolwiek operacje wykonywane na danych osobowych, zgodnie z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679  z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2)

9) **identyfikatorze użytkownika** – należy przez to rozumieć ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

10) **ustawie** – należy przez to rozumieć ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych. (Dz. U. 2018 poz. 1000)

**Rozdział 2.**
**Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej
za te czynności.**

**§ 3.**Przetwarzać dane osobowe w systemach informatycznych mogą wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania danych osobowych.

**§ 4.**1. Za tworzenie, modyfikację i nadawanie uprawnień kontom użytkowników systemu odpowiada ASI.

2. ASI nadaje oraz modyfikuje uprawnienia w systemie informatycznym na podstawie pisemnego polecenia Wójta.

3. ASI prowadzi ewidencję użytkowników i uprawnień w systemie informatycznym, której wzór stanowi załącznik nr 2.

4. Karty uprawnień zawierające szczegółowe dane odnośnie przypisanych funkcji programów, w których przetwarzane są dane osobowe stanowią załącznik nr 3.

**§ 5.**1. Odbieranie uprawnień stosowane jest wyłącznie w uzasadnionych przypadkach.

2. Konta danego użytkownika systemu ulegają dezaktywacji w celu zachowania historii jego aktywności.

3. Dezaktywacja kont danego użytkownika następuje na podstawie pisemnego wniosku Wójta.

4. Naczelnicy zobowiązani są pisemnie informować IOD o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym, a w szczególności o konieczności wyrejestrowania użytkownika systemu lub ograniczenia jego uprawnień.

**§ 6.**Osoby upoważnione do przetwarzania danych osobowych obowiązane są do zachowania ich w tajemnicy. Tajemnica obowiązuje również po ustaniu zatrudnienia lub innego stosunku łączącego z Urzędem. Co stanowi Oświadczenie o poufności danych.

**Rozdział 3.**
**Stosowane metody i środki uwierzytelnienia oraz procedury związane z zarządzaniem
i użytkowaniem.**

**§ 7.**Konta będące jednocześnie identyfikatorem użytkownika, zakładane w systemach operacyjnych na stacjach roboczych są kontami o ograniczonych uprawnieniach i są chronione hasłami. Hasła do kont systemu o prawach administratora powinno znajdować się w zamkniętej kopercie w zamykanej na klucz szafie metalowej, do której dostęp mają:

- Wójt,

- Administrator Systemu Informatycznego,

- Inspektor Ochrony Danych.

Identyfikator (nazwa konta) użytkownika systemu nie może być zmieniany bez ważnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie. Zmiany identyfikatora dokonuje ASI.

**§ 8.**W przypadku awarii ASI dokonuje oceny sytuacji i podejmuje wszelkie niezbędne czynności w celu zachowania integralności danych oraz przywrócenia normalnego funkcjonowania systemów informatycznych.

**§ 9.**Hasło, którym zabezpieczony jest system operacyjny na stacji roboczej jak i programy (w tym platformy, serwisy internetowe, itp.) musi być zmieniane co 30 dni, licząc każdy dzień od czasu poprzedniej zmiany. Jeśli system operacyjny lub program (lokalny bądź sieciowy) nie oferuje automatycznego wymuszania zmiany hasła, użytkownik zobowiązany jest dokonać zmiany w sposób ręczny, zgodnie z harmonogramem czasowym opisanym powyżej. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.

Hasło tworzy się zgodnie z zasadami bezpieczeństwa, stosując tzw. mocne hasło.

- musi zawierać minimum 8 znaków

- musi zawierać co najmniej 1 cyfrę

- musi zawierać co najmniej jeden znak specjalny

- musi zawierać przynajmniej jedną dużą literę

Hasła nie mogą być do siebie podobne pod żadnym względem ani zawierać kolejnych numeracji poprzednich jego wersji (w okresie 6 miesięcy), np. hasło stworzone w styczniu brzmi: "R0Man01", a w lutym brzmi "R0Man02", itp. Takie praktyki jak wskazane w przykładzie są niedopuszczalne, ponieważ tworzą hasło w łatwy sposób możliwe do przewidywania (zgadnięcia).

Zasady tworzenia haseł, których bezwzględnie należy przestrzegać:

- nie należy używać identyfikatorów jako hasła (nawet ze zmianą wielkości liter lub pisane wspak).

- nie należy używać swojego imienia i nazwiska oraz nazw własnych.

- nie należy używać informacji związanych z własną osobą (pesel, numer telefonu itd.).

- nie należy używać samych cyfr lub samych liter.

Dodatkowo:

- haseł nie wolno udostępniać innym osobom, z wykluczeniem Administratora Danych, Administratora Systemów lub Inspektora Ochrony Danych

- zapisane hasło należy przechowywać w bezpiecznym miejscu, np. w szafie zamykanej na klucz.

W przypadku podejrzenia ujawnienia hasła lub innej koniecznej do jego zmiany sytuacji (wykluczając 30 dniowy obowiązek jego zmiany)

- należy poinformować Administratora Systemów i Ochrony Danych o takim fakcie

- zmienić hasło zgodne z zasadami tworzenia haseł.

Użytkownikowi nie wolno:

- wyrzucać wydruków zawierających dane osobowe do ogólnie dostępnych koszów na śmieci (wydruki zawierające dane osobowe mogą być niszczone tylko w niszczarce);

- pozostawiać wydruków, kopii dokumentów, zawierających dane osobowe w drukarkach, kserokopiarkach, skanerach;

- pozostawiać dokumentów na biurku po zakończonej pracy.

**§ 10.**Zabrania się korzystania w systemach, które to umożliwiają, opcji zapamiętania nazw użytkownika lub hasła.

**§ 11.**Oprogramowanie, w którym przetwarzane są dane osobowe posiada mechanizmy pozwalające na odnotowanie informacji dotyczących wykonywanych operacji na danych, chyba że producent oprogramowania nie uwzględnił takiego rozwiązania. W szczególności zapis ten powinien obejmować:

- rozpoczęcia i zakończenie pracy przez użytkownika systemu,

- operacje wykonywane na danych,

- nieudane próby dostępu do systemu informatycznego,

- nieudane próby wykonania operacji na danych,

- błędy w działaniu systemu informatycznego podczas pracy danego użytkownika,

- przesyłanie za pośrednictwem systemu danych innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu.

**§ 12.**System informatyczny posiada mechanizm zliczania nieudanych prób zalogowania się do systemu oraz blokadę konta użytkownika po wykryciu ośmiu nieudanych prób, chyba że producent oprogramowania nie uwzględnił takiego rozwiązania.

**Rozdział 4.**
**Sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania**

**§ 13.**W Urzędzie stosuje się ochronę antywirusową na każdej stacji roboczej centralnie zarządzana przez Administratora Systemów Informatycznych.

Oprogramowanie antywirusowe skonfigurowane jest w taki sposób, aby:

a. w cyklu dniowym system antywirusowy sprawdzał i aktualizował bazy sygnatur wirusowych,

b. przeprowadzana była kontrola wszystkich zewnętrznych elektronicznych wykorzystywanych nośników danych (magnetycznych, optycznych),

c. na bieżąco oprogramowanie skanowało wykorzystywane pliki, oraz podłączane nośniki zewnętrzne,

d. automatyczne skanowanie systemu stacji roboczej odbywało się przynajmniej raz w miesiącu.

**§ 14.**Na terenie Urzędu Gminy Starogard Gdański obowiązuje zakaz korzystania z wszelakiego rodzaju nośników komputerowych, z wykluczeniem tych, które zawarte są w ewidencji nośników będących w użyciu (wzór stanowi załącznik nr 4 do Instrukcji Zarządzania Systemem Informatycznym). Jeśli istnieje uzasadniona potrzeba wprowadzenia do użycia obcego nośnika, wymagana jest zgoda ASI.

Wszelkie nośniki winny być przechowywane w miejscu niedostępnym dla osób postronnych, zamkniętych na klucz. Zabrania się, bez zgody IOD lub ASI, wynoszenia nośników poza Urząd. Transport nośnika do innych jednostek odbywa się wyłącznie na odpowiedzialność użytkownika. W przypadku zagubienia, ujawnienia kradzieży, uszkodzenia mają zastosowanie zasady postępowania
w przypadkach awaryjnych, opisanych w instrukcji postępowania w sytuacji naruszenia danych osobowych w Urzędzie Gminy Starogard Gdański, uwzględniając zaistniałą sytuację.

**§ 15.**1. ASI przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach – nie rzadziej, niż co sześć miesięcy.

2. Kontrola antywirusowa przeprowadzana jest również na wybranej stacji roboczej w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.

**§ 16.**Połączenie lokalnej sieci komputerowej Urzędu z Internetem jest realizowane przy użyciu mechanizmów ochronnych (firewall) oraz kompleksowego systemu antywirusowego.

**Rozdział 5.**
**Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.**

**§ 17.**W celu rozpoczęcia pracy w systemie informatycznym użytkownik systemu:

1) loguje się do systemu operacyjnego, na swoje konto, wpisując swoje hasło dostępowe.

2) loguje się do programów wymagających dodatkowego wprowadzenia unikalnego identyfikatora i hasła.

 Zakończenie pracy odbywa się poprzez wylogowanie z używanych programów i zamknięcie ich, a następnie zamknięcie systemu operacyjnego – wyłączenie komputera.

**§ 18.**1. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy uniemożliwić osobom postronnym korzystanie z systemu informatycznego poprzez wylogowanie się z systemu operacyjnego.

2. W sytuacji, gdy w wyświetlane na monitorze dane może mieć wgląd osoba nieuprawniona należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran notebooka) w sposób uniemożliwiający wgląd w wyświetlaną treść.

3. Sposób szybkiego ukrywania zawartości ekranu polega na zablokowaniu systemu operacyjnego, poprzez jednoczesne wciśnięcie klawiszy **Logo Windows + L**.

**§ 19.**Nie dopuszcza się możliwości udostępniania swojego konta w systemie operacyjnym innym pracownikom, również upoważnionym.

**§ 20.**Każdy użytkownik systemu przed wyłączeniem komputera jest obowiązany zakończyć pracę uruchomionych programów. Niedopuszczalne jest wyłączanie komputera przed wylogowaniem się z programu komputerowego.

**§ 21.**Zawieszenie korzystania z systemu informatycznego może nastąpić losowo wskutek awarii lub planowo np. w celu konserwacji sprzętu. Planowe zawieszenie prac powinno być poprzedzone poinformowaniem użytkowników systemu Urzędu przez ASI na co najmniej 30 minut przed zawieszeniem.

**§ 22.**1. Użytkownik systemu informatycznego zobowiązany jest do powiadomienia ASI
w sytuacji:

a) podejrzenia naruszenia bezpieczeństwa systemu,

b) braku możliwości zalogowania się na swoje konto,

c) stwierdzenia fizycznej ingerencji w przetwarzane dane,

d) stwierdzenia użytkowania narzędzia programowego lub sprzętowego przez osoby nieupoważnione.

2. Na fakt naruszenia zabezpieczeń systemu mogą wskazywać:

a) nietypowy stan stacji roboczej np. brak zasilania, problemy z uruchomieniem,

b) wszelkiego rodzaju różnice w funkcjonowaniu systemu np. komunikaty informujące
o błędach, brak dostępu do funkcji systemu, nieprawidłowości w wykonywanych operacjach,

c) różnice w zawartości zbioru danych osobowych np. brak lub nadmiar danych,

d) inne nietypowe sytuacje.

3. Wszelkie usterki dotyczące działania systemów informatycznych i sprzętu komputerowego należy niezwłocznie zgłaszać do ASI lub IOD, w zależności od zaistniałej sytuacji.

**Rozdział 6.**
**Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania oraz sposób i miejsce ich przechowywania**

**§ 23.**Za systematyczne przygotowywanie kopii zapasowych odpowiada ASI.

**§ 24.**Dane z dziedzinowych systemów informatycznych (oprogramowania księgowego, kadrowego, płacowego, program do składek ZUS - Płatnik) są archiwizowane codziennie na dysk zewnętrzny oraz okresowo na nośnik zewnętrzny (płyty DVD) w częstotliwości raz na miesiąc.

Dodatkowo na stacjach roboczych użytkownik dokonuje kopii swoich danych na dysk zewnętrzny dostępny u naczelnika wydziału. Kopie te nie są obowiązkowe, jednak zalecane. W sytuacji, kiedy stan techniczny komputera uniemożliwia wykonywanie kopii, nie jest ona wdrażana. Jeśli tak się dzieje, użytkownik zgłasza fakt do Administratora Systemów Informatycznych w celu usunięcia usterki i wykonania kopii danych. W celu sprawnego przeprowadzania kopii oraz oszczędności miejsca na docelowym dysku archiwizacyjnym, nie są archiwizowane duże pliki, inne niż dane bazodanowe, np. zdjęcia, filmy, rysunki, duże pliki PDF, utwory muzyczne, pliki poczty elektronicznej (w przypadku klientów pocztowych, np. MS Outlook) itp. Gdy istnieje potrzeba wykonywania archiwizowania takich plików konieczne jest pisemne zgłoszenie faktu do ASI z opisem sytuacji i wskazaniu konkretnych plików lub katalogów przeznaczonych do archiwizacji. Dodatkowe kopie użytkowników nie są archiwizowane na nośnik zewnętrzny, sporządzany raz na miesiąc.

Każde kopie na nośnik zewnętrzny są przechowywane w metalowej szafie lub sejfie.

1. Kopie zapasowe baz danych wykonywane są codziennie w sieci komputerowej.

2. Kopie zapasowe wykonywane są na dyskach twardych stanowisk roboczych (lokalnie).

2. Dodatkowo dane zrzucane są codziennie na dysk zewnętrzny i przechowywane przez 90 dni.

3. Kopia zapasowa plików konfiguracyjnych serwera wykonywana jest raz w miesiącu i przechowywana na serwerze w odrębnym miejscu do tego przeznaczonym.

4. Raz w miesiącu dane z ostatniego dnia każdego tygodnia zapisywane są na płycie DVD.

**§ 25.**Okresową weryfikację kopii zapasowych pod kątem ich przydatności do odtworzenia danych przeprowadza ASI.

**§ 26.**Dane osobowe w postaci elektronicznej nie mogą być przechowywane na wymiennych nośnikach informacji, za wyjątkiem kopii zapasowych.

**§ 27.**1. Nośniki danych, na których zapisywane są dane osobowe i kopie zapasowe, przeznaczone do likwidacji, naprawy lub przekazania innemu podmiotowi nieuprawnionemu do otrzymywania danych osobowych, pozbawia się wcześniej zapisu tych danych.

2. Nośniki danych, na których zapisywane są kopie zapasowe, przeznaczone do likwidacji po usunięciu zapisów tych danych i sformatowaniu, niszczone są w sposób mechaniczny.

Wg Załącznika nr 5 Procedura niszczenia danych na nośnikach elektronicznych.

3. Wszelkie wydruki komputerowe z systemów informatycznych zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione w zamkniętych na klucz szafach biurowych, a po upływie ich ważności są niszczone przy użyciu niszczarek.

**Rozdział 7.**
**Sposób realizacji wymogów – udostępnianie**

**§ 28.**Dane osobowe przetwarzane w systemach informatycznych mogą być udostępniane wyłącznie osobom i podmiotom upoważnionym z mocy przepisów prawa.

**§ 29.**Udostępnienie danych osobowych przetwarzanych w systemie informatycznym nie może odbywać się drogą telefoniczną.

**§ 30.**Udostępnienie danych osobowych przetwarzanych w systemie informatycznym może nastąpić wyłącznie na zasadach określonych w Polityce Bezpieczeństwa Ochrony Danych Osobowych.

**§ 31.**IOD prowadzi wykazy udostępnianych danych osobowych przetwarzanych w systemach informatycznych zawierające co najmniej:

- datę przekazania danych,

- uzasadnienie potrzeby udostępnienia danych np. podstawę prawną,

- zakres udostępnionych informacji,

- odbiorcę danych osobowych.

**Rozdział 8.**
**Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.**

**§ 32.**1. Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta urządzenia .

2. Nieprawidłowości ujawnione w trakcie działań, o których mowa w ust. 1, powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy powiadomić IOD.

**§ 33.**1. Konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami autorów poszczególnych programów.

2. Osoby lub podmioty uprawnione do konserwacji lub naprawy baz danych niebędące pracownikami Urzędu winny przed przystąpieniem do tych czynności zawrzeć umowę o powierzeniu danych osobowych.

3. Prace wymienione w ust. 1 powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

**§ 34.**1. ASI prowadzi Dziennik systemu informatycznego, zgodnie ze wzorem określonym w *załączniku nr 1* do Instrukcji.

2. Wpisów do dziennika może dokonywać Wójt, IOD i ASI.

Załącznik Nr 1 do Załącznika Nr 1

*Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu informatycznego, a w szczególności:*

* *w przypadku awarii - opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski;*
* *w przypadku konserwacji systemu – opis podjętych działań, wnioski*

**DZIENNIK SYSTEMU INFORMATYCZNEGO UG Starogard gdański**

(wzór)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Lp.* | *Data i godzina* | *Opis zdarzenia* | *Podjęte działania / wnioski* | *Podpis* |
|  |  |  |  |  |

Załącznik Nr 2 do Załącznika Nr 1

**Ewidencja użytkowników i uprawnień w systemie informatycznym**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *Lp.* | *Nazwisko i imię* | *Data nadania uprawnień* | *Data modyfikacji uprawnień* | *Data odebrania uprawnień* | *Podpis administratora SI* |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Załącznik Nr 3 do Załącznika Nr 1

## NADANIE/ZMIANA/ODEBRANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

## Odebranie uprawnień w

**systemie informatycznym**

|  |  |  |
| --- | --- | --- |
| *Modyfikacja uprawnień**Nowy użytkownik* |  |  |

|  |  |
| --- | --- |
| **Imię i nazwisko użytkownika:** | **Komórka organizacyjna** |
|   |   |

Zakres uprawnień użytkownika w systemie informatycznym:

|  |  |
| --- | --- |
| SIDAS – Elektroniczny Obieg Dokumentacji[ ] przeglądanie [ ] zmiany [ ] drukowanie [ ] zakładanie i modyfikacja spraw[ ] wydruki raportów[ ] obsługa kancelarii[ ] uprawnienia naczelnika (dekretowanie pism, podgląd spraw pracowników, podpisywanie dok. Wychodzących certyfikatem kwalifikowanym)[ ] dodawanie interesantów[ ] konto na poziomie administratora[ ] Besti@ – Program do zarządzania Budżetem Jednostek Samorządu terytorialnegoŹródło: [ ] Ewidencja ludności[ ] Dowody[ ] PeseleBANKOWOŚĆ ELEKTRONICZNA – BS Starogard [ ] zestawienia płacowe na ekranie [ ] wprowadzanie zleceń[ ] kartoteka korekt [ ] wysyłanie zleceń[ ] pobieranie wyciągów[ ] kartoteka miesięcznych wynagrodzeń [ ] autoryzacja (podpisywanie) zleceń[ ] kartoteka wynagrodzeń pracowników  | Systemy dziedzinowe Radix:[ ] KADRY+ i PŁACE+ [ ] ELUD+[ ] FKB+ [ ] KASA +[ ] POGRUN+[ ] POST+ [ ] WIP+[ ] WYB+[ ] GOK+ [ ] Program Asseco Poland PŁATNIK (pełne uprawnienia)[ ] SHRIMP – portal pomocy DEMINIS [ ] WebEwid – portal geodezyjny[ ] CEIDG – portal ewidencji działalności gospodarczej.[ ] SL2014 – portal rozliczenia wniosków RPO[ ]BIP – Biuletyn Informacji Urzędu Gminy Starogard GdańskiInfrastruktura komputerowa:[ ] Dostęp do sieci Internet[ ] Pliki i dokumenty w systemie Office zawierających dane osobowe.[ ] …………………………………………[ ] …………………………………………[ ] …………………………………………[ ] ………………………………………… |

|  |  |
| --- | --- |
| Data nadania/odebrania uprawnień: | Podpis bezpośredniego przełożonego użytkownika systemu: |
| Nadany identyfikator(nazwa użytkownika): | Podpis ADO: |
| Nadany Identyfikator Sieciowy - IP komputera: | Podpis IOD: |
|  | Podpis ASI: |

Załącznik Nr 4 do Załącznika Nr 1

**Ewidencja elektronicznych nośników informacji wykorzystywanych w Urzędzie**

**(wzór)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| *Lp.* | *Oznaczenie nośnika* | *Nazwa nośnika* | *Data wpisania do ewidencji* | *Miejsce przechowywania nośnika* | *Podpis użytkownika* | *Uwagi/ data zwrotu* |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Przykładowe symbole nośników:

PD – pendrive (pamięć USB)

HDD -- dysk twardy

TK - telefon komórkowy

KP - karta pamięci

Oznaczenie nośnika:

*Kolejny numer nośnika/symbol nośnika /symbol placówki (np. 01/PD/UG)*

Załącznik Nr 5 do Załącznika Nr 1

**Procedura niszczenia danych na nośnikach elektronicznych i papierowych**

1. Podlegające likwidacji uszkodzone lub przestarzałe nośniki a szczególności twarde dyski z danymi osobowymi ze stacji roboczych i laptopów / pendrive / pamięci flash / dyski SSD / płyty DVD / telefony komórkowe / smartfony są niszczone w sposób fizyczny w tym również komisyjnie w/g Załącznika Protokół zniszczenia uszkodzonych nośników. Stosowana metoda niszczenia, to fizyczne niszczenie (pocięcie, nawiercenie, młotkowanie) wymontowanych nośników / przekazanie specjalistycznej firmie potwierdzone protokołem zniszczenia lub certyfikatem bezpieczeństwa firmy utylizacyjnej
2. Nośniki informacji zamontowane w sprzęcie IT a w szczególności twarde dyski muszą być wyczyszczone specjalistycznym oprogramowaniem zanim zostaną przekazane poza obszar organizacji (np. sprzedaż lub darowizna komputerów stacjonarnych / laptopów / smartfonów)
3. Dokumentacja papierowa niszczona jest w niszczarkach paskowych oraz tam, gdzie to wymagane w niszczarkach o podwyższonym standardzie
4. Dokumentacja papierowa niszczona jest za pośrednictwem firmy niszczącej dokumenty. Firma zobowiązana jest do wykazania się bezpieczną procedurą utylizacji (np. posiadać certyfikat ISO27001, nagrania z procesu transportu i utylizacji

.............................. dnia ..................r.

**Protokół nr ...............**

**zniszczenia uszkodzonych nośników komputerowych**

w Urzędzie Gminy w Starogardzie Gdańskim

Dnia ................... komisja powołana przez ..................................................................

 (data) (imię, nazwisko i stanowisko osoby powołującej komisję)

w składzie:

1. Przewodniczący ASI: .......................................
2. Członkowie: ........................................

 .....................................

dokonała trwałego zniszczenia nośników komputerowych:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| L.p. | Nazwa | Nr ewidencyjny  | Sposób zniszczenia  | Uwagi |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Dokonanie w/w czynności zostaje potwierdzone własnoręcznymi podpisami komisji:

................................................

................................................

............................................