Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

Obszarem przetwarzania danych osobowych Urzędu Gminy Stolno są pomieszczenia mieszczące się w budynku w miejscowości Stolno nr 112 zajmowane przez Urząd Gminy.

Do obszaru przetwarzania danych zalicza się wszystkie pomieszczenia służbowe budynku, w których dokonywane są wszelkiego rodzaju operacje na danych osobowych - tj. wpisywanie nowych informacji, ich modyfikowanie, usuwanie, kopiowanie różnymi sposobami, itd., oraz pomieszczenia, w których przechowywane są nośniki informacji zawierające wszelkie dane osobowe - jak serwery, szafy z dokumentami, szafy z nośnikami zawierającymi kopie zapasowe itp., a także pomieszczenia, w których przechowywany jest uszkodzony sprzęt komputerowy, nośniki informacji przeznaczone do likwidacji, jak również pomieszczenia archiwum Urzędu.

L.p.	Lokalizacja (adres)	Nr pokoju	Funkcja lokalizacji[1]	Zabezpieczenie fizyczne[2]
1.	Stolno, Stolno nr 112			
2.	Stolno, Stolno nr 112			
...				
n				

1. **(S)** pomieszczenie techniczne (serwerownia), **(PA)** – pomieszczenie archiwum, **(PK)** – pomieszczenie, w którym przechowywane są kopie bezpieczeństwa, **(WK)** – pomieszczenie, w którym wykonywane są kopie bezpieczeństwa, **(U)** – pomieszczenie, w którym pracownicy wprowadzają dane, **(AD)** – pomieszczenie administratora bazy danych
2. **(K)** – kraty w oknach, **(A)** – alarm, **(W)** – wzmocnione drzwi

Dane aktualne na dzień: ***2011r.***

Sporządził: .....

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Lp.	Zbiór danych	Forma (M/E) Wersja bazy danych[1]	Poziom zabezpieczeń[2] (W/PW/P/ND)	System informatyczny[3]	System operacyjny serwera Forma bazy danych[4]	Fizyczna lokalizacja[5]	Zawiera dane osób spoza organizacji (T/N)
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							
10.							
11.							
12.							
13.							
14.							
15.							

1. **(M)** – zbiór przetwarzany drogą manualną (wersja papierowa) / **(E)** – zbiór przetwarzany drogą elektroniczną (wersja bazy danych)
2. **(W)** wysoki / **(PW)** podwyższony / **(P)** podstawowy / **(ND)** nie dotyczy
3. nazwa zwyczajowa lub własna
4. rodzaj systemu operacyjnego np. Microsoft Windows 2003 Server / rodzaj bazy danych np. Microsoft SQL 2005 Server
5. pomieszczenie, w którym dane przetwarzane

Dane aktualne na dzień: ***2011r.***

Sporządził: .....

Wykaz zbiorów danych osobowych zarejestrowanych w GIODO

Lp.	Zbiór danych	Administrator zbioru	Data rejestracji zbioru	Nr księgi rejestrowej GIODO	Nr zgłoszenia zbioru w GIODO	Podstawa prawna do przetwarzania zbioru
1.		GMINA STOLNO, 86-212 Stolno, Stolno nr 112				
2.		GMINA STOLNO, 86-212 Stolno, Stolno nr 112				
3.		GMINA STOLNO, 86-212 Stolno, Stolno nr 112				
4.		GMINA STOLNO, 86-212 Stolno, Stolno nr 112				
5.		GMINA STOLNO, 86-212 Stolno, Stolno nr 112				
6.		GMINA STOLNO, 86-212 Stolno, Stolno nr 112				
7.		GMINA STOLNO, 86-212 Stolno, Stolno nr 112				
8.		GMINA STOLNO, 86-212 Stolno, Stolno nr 112				
9.		GMINA STOLNO, 86-212 Stolno, Stolno nr 112				

Dane aktualne na dzień: ..... *2011 r.*

Sporządził: .....

Zgłoszenie zbioru danych do rejestracji GIODO

/wzór/

ZGŁOSZENIE ZBIORU DANYCH DO REJESTRACJI GENERALNEMU INSPEKTOROWI OCHRONY DANYCH OSOBOWYCH

*☐ — zgłoszenie zbioru na podstawie art. 40 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.),

*☐ — zgłoszenie zmian na podstawie art. 41 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,

*☐ — zgłoszenie zbioru, w którym będą przetwarzane dane określone w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Nr .....

.....

(nadaje urzędnik Biura GIODO)

Część A. Wniosek

Wnoszę o wpisanie zbioru danych osobowych o nazwie:

.....

do Rejestru Zbiorów Danych Osobowych.

Część B. Charakterystyka administratora danych

1. Wnioskodawca (administrator danych):

.....

.....

(nazwa administratora danych i adres jego siedziby lub nazwisko, imię i adres miejsca zamieszkania wnioskodawcy oraz nr REGON)

2. Przedstawiciel wnioskodawcy, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych:

.....

.....

.....

(nazwa przedstawiciela administratora danych i adres jego siedziby lub nazwisko, imię i adres miejsca zamieszkania)

3. Powierzenie przetwarzania danych osobowych:

*☐ — administrator danych powierzył w drodze umowy zawartej na piśmie przetwarzanie danych innemu podmiotowi (art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych),

*☐ — danych przewiduje powierzenie przetwarzania danych innemu podmiotowi.

W przypadku powierzenia przetwarzania danych innemu podmiotowi podaj nazwę i adres siedziby lub nazwisko, imię i adres miejsca zamieszkania podmiotu, któremu powierzono przetwarzanie danych osobowych:

.....

.....

.....

*☐ *cd. w załączniku nr.....*

4. Podstawa prawna upoważniająca do prowadzenia zbioru danych:

*□ — zgoda osoby, której dane dotyczą, na przetwarzanie danych jej dotyczących,
*□ — przetwarzanie jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa

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

*□ *cd. w załączniku nr.....*

*□ — przetwarzanie jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
*□ — przetwarzanie jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego — w przypadku odpowiedzi twierdzącej, należy opisać te zadania:

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

*□ *cd. w załączniku nr.....*

*□ — przetwarzanie jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Część C. Cel przetwarzania danych, opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych

5. Cel przetwarzania danych w zbiorze:

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

*□ *cd. w załączniku nr.....*

6. Opis kategorii osób, których dane dotyczą:

.....
.....

7. Zakres przetwarzanych w zbiorze danych o osobach:

*□ — nazwiska i imiona,
*□ — imiona rodziców,
*□ — data urodzenia,
*□ — miejsce urodzenia,
*□ — adres zamieszkania lub pobytu,
*□ — numer ewidencyjny PESEL,
*□ — Numer Identyfikacji Podatkowej,
*□ — miejsce pracy,
*□ — zawód,
*□ — wykształcenie,
*□ — seria i numer dowodu osobistego,
*□ — numer telefonu.

8. Inne dane osobowe, oprócz wymienionych w pkt. 7, przetwarzane w zbiorze — należy *podać jakie:*

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

*□ *cd. w załączniku nr.....*

9. Dane przetwarzane w zbiorze:

a) ujawniają bezpośrednio lub w kontekście:

*☐ — pochodzenie rasowe,
*☐ — pochodzenie etniczne,
*☐ — poglądy polityczne,
*☐ — przekonania religijne,
*☐ — przekonania filozoficzne,
*☐ — przynależność wyznaniową,
*☐ — przynależność partyjną,
*☐ — przynależność związkową,
*☐ — stan zdrowia,
*☐ — kod genetyczny,
*☐ — nałogi,
*☐ — życie seksualne,

b) dotyczą:

*☐ — skazań,
*☐ — mandatów karnych,
*☐ — orzeczeń o ukaraniu,
*☐ — innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym

Jeśli nie zakreślono żadnej odpowiedzi, należy przejść od razu do pkt 11.

10. Podstawa prawna przetwarzania danych wskazanych w pkt 9:

*☐ — osoby, których dane dotyczą, będą wyrażać na to zgodę na piśmie,
*☐ — przepis szczególny innej ustawy zezwala na przetwarzanie bez zgody osoby, której dane dotyczą, jej danych osobowych — *w przypadku odpowiedzi twierdzącej, należy podać odniesienie do przepisu tej ustawy:*

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

*☐ *cd. w załączniku nr*.....

*☐ — przetwarzanie danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,
*☐ — przetwarzanie jest niezbędne do wykonania statutowych zadań kościoła, innego związku wyznaniowego, stowarzyszenia, fundacji lub innej niezarobkowej organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, a przetwarzanie danych dotyczy wyłącznie członków tej organizacji lub instytucji albo osób utrzymujących z nią stałe kontakty w związku z jej działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych — w przypadku odpowiedzi twierdzącej, należy podać, jakich:

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

*☐ *cd. w załączniku nr*.....

*☐ — przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,
*☐ — przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,
*☐ — przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem

lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych,

*☐ — przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą,

*☐ — przetwarzanie jest niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego, a publikowanie wyników badań naukowych uniemożliwia identyfikację osób, których dane zostały przetworzone,

*☐ — przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

Część D. Sposób zbierania oraz udostępniania danych

11. Dane do zbioru będą zbierane:

*☐ — od osób, których dotyczą,

*☐ — z innych źródeł niż osoba, której dane dotyczą,

12. Dane ze zbioru będą udostępniania:

*☐ — podmiotom innym niż upoważnione na podstawie przepisów prawa,

13. Odbiorcy lub kategorie odbiorców, którym dane mogą być przekazywane — *należy podać nazwę i adres siedziby lub nazwisko, imię i adres miejsca zamieszkania odbiorcy danych:*

.....

.....

.....

*☐ *cd. w załączniku nr*.....

14. Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego — *należy podać nazwę państwa:*

.....

.....

.....

*☐ *cd. w załączniku nr*.....

Część E. Opis środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36—39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

15. Zbiór danych osobowych jest prowadzony:

a) *☐ — centralnie

*☐ — w architekturze rozproszonej

b) *☐ ☐☐ — wyłącznie w postaci papierowej

*☐ — z użyciem systemu informatycznego

c) *☐ ☐ — z użyciem co najmniej jednego urządzenia systemu informatycznego służącego do przetwarzania danych osobowych połączonego z siecią publiczną np.: internetu

*☐ — bez użycia żadnego z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych połączonego z siecią publiczną np.: internetu

16. Zostały spełnione wymogi art.36-39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[1]:

a) *☐ — został wyznaczony administrator bezpieczeństwa informacji nadzorujący przestrzegania zasad ochrony przetwarzanych danych osobowych
*☐ — administrator danych sam wykonuje czynności administratora bezpieczeństwa informacji

b) *☐ — do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych

c) *☐ — prowadzona jest ewidencja osób upoważnionych do przetwarzania danych

d) *☐ — została opracowana i wdrożona polityka bezpieczeństwa

e) *☐ — została opracowana i wdrożona instrukcja zarządzania systemem informatycznym

f) inne środki, oprócz wymienionych w ppkt a-e, zastosowane w celu zabezpieczenia danych

.....

.....

.....

*☐ *cd. w załączniku nr*.....

Część F. Informacja o sposobie wypełnienia warunków technicznych i organizacyjnych, o których mowa w rozporządzeniu 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)

17. Zastosowano środki bezpieczeństwa na poziomie[2]:

*☐ — podstawowym,
*☐ — podwyższonym,
*☐ — wysokim.

.....
(data, podpis i pieczęć wnioskodawcy)

Objaśnienie:
* W przypadku odpowiedzi twierdzącej kwadrat zakreślić X
[1] Administrator danych prowadzący zbiór w systemie tradycyjnym (papierowym) zobowiązany jest do zastosowania środków określonych w pkt. 16 ppkt. a-d, a przypadku prowadzenia zbioru w systemie informatycznym, ponadto środka określonego w pkt 16 ppkt e.
[2] Należy wskazać odpowiedni poziom bezpieczeństwa określony w § 6 wymienionego rozporządzenia
Uwaga! (Dotyczy wyłącznie administratorów przetwarzających dane w systemach informatycznych):
– jeżeli wnioskodawca przetwarza dane wymienione w pkt. 9 zgłoszenia, należy zastosować środku przynajmniej na poziomie podwyższonym
– w przypadku gdy przynajmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną, należy zastosować środki bezpieczeństwa na poziomie wysokim
– w pozostałych przypadkach wystarczające jest zastosowanie środków bezpieczeństwa na poziomie podstawowym

Zgłoszenia można dokonać drogą elektroniczną, za pomocą programu komputerowego umożliwiającego jego prawidłowe wypełnienie, dostępne na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych - www.giodo.gov.pl

Rejestr upoważnień do przetwarzania danych osobowych*)

Lp.	Imię i Nazwisko	Komórka organizacyjna[1]	Data nadania upoważnienia	Data ustania upoważnienia	Nazwa identyfikatora[2]	Zakres upoważnienia[3] (nazwa zbioru)

*) upoważnienia do przetwarzania danych osobowych zarówno w systemach informatycznych jak i w sposób tradycyjny (manualnie)
1. Nazwa komórki organizacyjnej – (Referatu, samodzielne stanowiska)
2. dot. pracowników przetwarzających dane w systemach informatycznych
3. Skróty stosowane do określenia zakresu upoważnienia

Z – pełne prawa do zarządzania danymi
E – pełne prawa do edycji danych (w tym drukowania, archiwizowania, usuwania)
M – prawo do dodawania i modyfikacji danych
P – prawo do przeglądania danych
D – prawo do drukowania danych
A – prawo do wykonywania kopii archiwalnych
N – prawo do zakładania nowych kont

Dane aktualne na dzień: ..... ***2011 r.***

Sporządził: .....

Rejestr udostępnień danych osobowych

Lp.	Nazwa zbioru	Nazwa odbiorcy[1]	Data udostępnienia	Podstawa prawna[2]	Cel pozyskania danych osobowych	Zakres udostępnionych danych

1. dotyczy zarówno odbiorców uprawnionych na podstawie przepisów ustawy (obowiązek obligatoryjny), jak i nie mogących wykazać się prawną podstawą uzyskania danych (obowiązek fakultatywny).
2. akt prawny (nazwa, art.), z którego wynika udostępnienie danych osobowych

Opis struktury zbiorów danych

1. Aplikacja[1]:

Producent:

Wykaz osób posiadających dostęp do aplikacji przy wykorzystaniu hasła.

L.p.	Imię i Nazwisko	Uprawnienia[2]	Identyfikator
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

1) Nazwa aplikacji.
2) Skróty stosowane do określenia zakresu upoważnienia
Z – pełne prawa do zarządzania
E – pełne prawa do edycji danych (w tym drukowania, archiwizowania, usuwania)
N – prawo do zakładania nowych kont
M – prawo do dodawania i modyfikacji danych
P – prawo do przeglądania danych
A – prawo do wykonywania kopii archiwalnych

Wymagania bezpieczeństwa dotyczące rozwoju systemów i aplikacji

1. Przed opracowaniem, nabyciem lub istotną modyfikacją systemu informatycznego muszą zostać wyraźnie sprecyzowane wymagania w zakresie jego bezpieczeństwa.
2. Informatyk będący Administratorem Systemu Informatycznego w Urzędzie ustala standardy konfiguracyjne sprzętu komputerowego, które stanowią podstawę ustalania wymagań wobec dostawców sprzętu.
3. Wszelkie zamówienia muszą być zatwierdzone przez Administratorem Systemu Informatycznego Urzędu.
4. Istnieją szczegółowe zasady dotyczące bezpieczeństwa, wynikające z niniejszego dokumentu, które muszą być spełnione przez wszystkie wdrażane, rozwijane lub modyfikowane systemy informatyczne Urzędu.
5. Wybór Dostawcy jest regulowany osobnymi przepisami.
6. Projekt umowy na zakup bądź serwis oprogramowania powinien być zatwierdzony przez Administratora Systemu Informatycznego przed podpisaniem ostatecznej umowy.
7. W każdej specyfikacji powinny być wyraźnie określone funkcje i elementy pozwalające na zarządzanie oprogramowaniem (środki kontroli), które powinny być zawarte w każdej umowie.
8. Każda umowa powinna jednoznacznie określać kwestie własności oprogramowania i związanych z nimi praw autorskich.
9. Umowa musi zapewniać warunki i sposób świadczenia pomocy technicznej przez Wykonawcę, która powinna prowadzić efektywne rozwiązanie problemów związanych z danym systemem lub aplikacją w określonym w umowie czasie.
10. Odpowiedzialność za poprawne funkcjonowanie wdrażanych systemów i aplikacji spoczywa na Wykonawcy.
11. Nowe systemy powinny być poddane testom obciążeniowym, wydajnościowym oraz odpornościowym. Muszą wykazywać wydajność równą bądź przekraczającą aktualne potrzeby Urzędu.
12. Systemy informatyczne muszą umożliwiać rejestrowanie następujących danych:

- datę modyfikacji lub dodanie rekordu,
- nazwę użytkownika modyfikującego lub wprowadzającego rekord,
- kompletną historię modyfikacji rekordu.

13. Przed przekazaniem oprogramowania do użytkowania, osoby je opracowujące są zobowiązane usunąć wszystkie specjalne kanały dostępu tak, aby dostęp był możliwy jedynie z zastosowaniem zasad bezpieczeństwa Urzędu:
    - muszą być usunięty wszystkie nieudokumentowane funkcje pozwalające ominąć system zabezpieczeń.
    - muszą zostać usunięte wszystkie specjalne uprawnienia systemowe, ustanowione dla potrzeb prowadzenia prac wdrożeniowych, które nie są wymagane w środowisku produkcyjnym.
14. W celu zapewnienia ciągłości działania Urzędu w umowach z dostawcami musi pojawić się zapis gwarantujący Zamawiającemu bezwzględny dostęp do kodów źródłowych zakupionego oprogramowania nawet, jeśli nie było to przedmiotem umowy. Zapis regulujący przekazanie kodów źródłowych ochroni Urząd na wypadek upadłości lub likwidacji Dostawcy oprogramowania.
15. W oprogramowaniu produkcyjnym transakcje używane do celów kontrolnych, testowych, szkoleniowych lub innych celów nieprodukcyjnych powinny być odpowiednio oznakowane i/lub odseparowane od transakcji używanych w środowisku produkcyjnym.
16. Użytkownicy zobowiązani są do przekazywania bezpośrednio Informatykowi informacji o wszelkich nieprawidłowościach w funkcjonowaniu aplikacji i systemów.
17. Wykonawca musi dostarczyć Zamawiającemu dokumentację techniczną i użytkową dla każdej wdrażanej aplikacji i systemu.
18. Pracownikom firmy zewnętrznych, prowadzącym serwis aplikacji i systemów, dostęp do systemu produkcyjnego może być przyznany jedynie z uprawnieniami do odczytu i kopiowania. Każdorazowo dostęp pracowników firm zewnętrznych do systemu produkcyjnego musi zostać uzgodniony z Informatykiem,
19. Pracownicy zaangażowani w procedury serwisowe prowadzone w środowisku produkcyjnym nie mogą udostępniać systemu osobom spoza Urzędu bez poinformowania o tym fakcie Informatyka (Administratora Systemu Informatycznego).

20. Wszelkie zmiany w systemie produkcyjnym powinny być wprowadzane w sposób bezpieczny i gwarantujący ciągłość pracy Urzędu.
21. Wszelkie zmiany w systemie produkcyjnym muszą być wykonywane przy wiedzy i nadzorze Informatyka (Administratora Systemu Informatycznego).

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

PROCEDURA ADMINISTRACYJNO - TECHNICZNA		
1.	**Numer**	1
2.	**Wersja**	01
3.	**Nazwa**	**Rejestracja w systemie informatycznym nowego pracownika**
4.	**Odwołania do innych dokumentów**	*Instrukcja postępowania w sytuacji naruszenia systemu ochrony danych osobowych* stanowiąca załącznik nr 2 do *Polityki Bezpieczeństwa* Urzędu Gminy Stolno. *Procedura Administracyjno-techniczna nr 2 Przydzielenie hasła dla użytkownika.* *Procedura Administracyjno-techniczna nr 3 Zarządzanie hasłami.*
5.	**Status**	Obowiązująca
6.	**Data wprowadzenia**	
7.	**Data wygaśnięcia**	
8.	**Pracownik wdrażający**	Administrator Systemu Informatycznego
9.	**Zatwierdzający procedurę**	Wójt
10.	**Lista dystrybucyjna**	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego.

1. Po przeszkoleniu w zakresie BHP i ochrony danych osobowych bezpośredni przełożony (kierownik komórki organizacyjnej) zgłasza pracownika do systemu informatycznego przez wypełnienie dokumentu „*Karta zgłoszenia do systemu*".

2. „*Karta zgłoszenia do systemu*" składa się z IV części – wg załączonego wzoru
   - cz. I - wypełnia bezpośredni przełożony pracownika - imię i nazwisko, stanowisko, od kiedy ma mieć dostęp do systemu, na którym komputerze ma pracować, rodzaj oprogramowania, kogo zastępuje, podpis osoby wnioskującej;
   - cz. II - potwierdzenie o odbytym szkoleniu w zakresie ochrony danych osobowych i bezpieczeństwa systemu informatycznego - podpis osoby szkolonej i Administratora Bezpieczeństwa Informacji;
   - cz. III - wypełnia Administrator Systemu Informatycznego – nadanie loginu i hasła, przydzielenie poczty internetowej i intranetowej, data nadania, podpis;
   - cz. IV - potwierdzenie użytkownika o zapoznaniu się z instrukcją i poprawnością działania przydzielonej aplikacji.

3. Przydzielenie praw dostępu do systemu informatycznego wymaga od Administratora Systemu Informatycznego wykonania następujących czynności:

- odnotowania w ewidencji osób upoważnionych do przetwarzaniu danych osobowych,
- przedzielenia identyfikatora i nadania hasła startowego,
- przydzielenia w systemie informatycznym uprawnień na poziomie odpowiednim do zakresu wykonywanej pracy, zgodnie z wytycznymi zawartymi w cz. I *„Karty zgłoszenia do systemu"*
- przygotowania stacji roboczej, z uwzględnieniem nowego użytkownika.

4. Po zapoznaniu się z *„Instrukcją korzystania z systemu teleinformatycznego"*, sprawdzeniu poprawności działania nadanych haseł, użytkownik w obecności Administratora Systemu Informatycznego lub wyznaczonego informatyka podpisuje na *„Karcie zgłoszenia do systemu"* odbiór loginu i hasła (imię i nazwisko, data).

5. W przypadku zakładania nowych skrzynek pocztowych Administratora Systemu wysyła do użytkownika testową informacje w celu sprawdzenia poprawności działania konta.

6. *„Karta zgłoszenia do systemu"* przechowywana jest u Administratora Systemu Informatycznego w wydzielonym segregatorze.

KARTA

ZGŁOSZENIA DO SYSTEMU

Nr karty:.....*(nadaje Administrator Systemu Informatycznego)*

Część I

.....
Komórka organizacyjna

Stolno, dnia .....

Proszę o nadanie uprawnień do systemu pani / panu

.....
imię i nazwisko

.....
Stanowisko

.....
numer pokoju

W okresie od ..... do .....

Rodzaj aplikacji:
Standard:

- ☐ *Microsoft Word*
- ☐ *Microsoft Excel*
- ☐ *Open Office*
- ☐ *7 Zip (program do archiwizacji)*
- ☐ *Acrobat Reader*
- ☐ *Konto poczty wewnętrznej*
- ☐ *Konto do wewnętrznego serwisu intranetowego*

Niestandardowe:

- ☐ *dostęp do Internetu*
- ☐ *konto poczty zewnętrznej*
- ☐ *LEX - System Informacji Prawnej*
- ☐ *Microsoft PowerPoint (aplikacja do tworzenia prezentacji)*
- ☐ *Microsoft Access*
- ☐ *Inne:* .....
  .....

.....
data i podpis
Kierownika komórki organizacyjnej

Część II

Potwierdzam odbycie szkolenia w zakresie ochrony danych osobowych w oparciu o przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926, ze zm.), a także zachowania w tajemnicy każdej informacji uzyskanej w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, której ujawnienie mogłoby narazić na szkodę prawnie chroniony interes obywateli lub jednostki organizacyjnej.

.....
Data i podpis ABI

Część III

konto:.....

hasło (startowe):.....

Nazwa konta poczty wew:.....

Nazwa konta poczty zewn:.....

Nazwa konta intranetowego:.....

Inne:.....

Wyposażenie – zgodnie z metryka komputera

Inne:.....

.....
Data i podpis użytkownika

.....
data i podpis
Administratora Systemu Informatycznego

Cześć IV

Zapoznałem się z „Instrukcją korzystania z systemu teleinformatycznego"

.....
data i podpis użytkownika

PROCEDURA ADMINISTRACYJNO - TECHNICZNA		
1.	**Numer**	2
2.	**Wersja**	01
3.	**Nazwa**	**Przydzielenie hasła dla użytkownika**
4.	**Odwołania do innych dokumentów**	*Instrukcja postępowania w sytuacji naruszenia systemu ochrony danych osobowych* stanowiąca załącznik nr 2 do *Polityki Bezpieczeństwa* Urzędu Gminy Stolno. *Procedura Administracyjno-techniczna nr 1 Rejestracja w systemie nowego pracownika.* *Procedura Administracyjno-techniczna nr 3 Zarządzanie hasłami.*
5.	**Status**	Obowiązująca
6.	**Data wprowadzenia**	
7.	**Data wygaśnięcia**	
8.	**Pracownik wdrażający**	Administrator Systemu Informatycznego
9.	**Zatwierdzający procedurę**	Wójt
10.	**Lista dystrybucyjna**	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego.

1. Konto każdego użytkownika systemu zabezpieczone jest poprzez indywidualny, niezmienny identyfikator oraz hasło.
2. Przydzielenie hasła użytkownikowi następuje wg określonych zasad:
   - Pierwsze hasło zakładane jest podczas wprowadzania identyfikatora w systemie informatycznym,
   - Po założeniu hasła przez Administratora Systemu Informatycznego, użytkownik ma obowiązek zarejestrować się do systemu i zmienić hasło,
   - Hasło stanowi ciąg, co najmniej 8 znaków, musi zawierać wielkie i małe litery oraz cyfry i znaki specjalne,
   - Hasło musi mieć budowę pozwalającą użytkownikowi na zapamiętanie i jednocześnie nie może być łatwe do odgadnięcia. W tym celu należy unikać imion, dat urodzenia i innych kojarząc się z użytkownikiem określeń,
   - Hasła zapisane są przez system w postaci zaszyfrowanej

PROCEDURA ADMINISTRACYJNO - TECHNICZNA		
1.	**Numer**	3
2.	**Wersja**	01
3.	**Nazwa**	**Zarządzanie hasłami**
4.	**Odwołania do innych dokumentów**	*Instrukcja postępowania w sytuacji naruszenia systemu ochrony danych osobowych* stanowiąca załącznik nr 2 do *Polityki Bezpieczeństwa* Urzędu Gminy Stolno. *Procedura Administracyjno-techniczna nr 1 Rejestracja w systemie nowego pracownika.* *Procedura Administracyjno-techniczna nr 2 Przydzielenie hasła dla użytkownika.*
5.	**Status**	Obowiązująca
6.	**Data wprowadzenia**	
7.	**Data wygaśnięcia**	
8.	**Pracownik wdrażający**	Administrator Systemu Informatycznego
9.	**Zatwierdzający procedurę**	Wójt
10.	**Lista dystrybucyjna**	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego.

1. Hasła systemowe zakładane są dla zapobieżenia wykonywania czynności wychodzących poza uprawnienia zwykłego użytkownika (konfiguracja oprogramowania, konfiguracja sprzętu komputerowego, ustawienia BIOS),
2. Hasła systemowe zakładane i zmieniane są tylko przez Administratora Systemu Informatycznego,
3. Hasło systemowe stanowi ciąg, co najmniej 8 znaków, musi zawierać wielkie i małe litery oraz cyfry i znaki specjalne z wyjątkiem sytuacji, kiedy sprzęt lub oprogramowanie na to nie pozwalają.
4. Hasła systemowe mogą być wykorzystywane tylko i wyłącznie do celów związanych z konserwacją systemów informatycznych, a nie do bieżącej pracy.
5. Hasło użytkownika wykorzystywane jest podczas autoryzacji:
   - przy starcie systemu operacyjnego,
   - przy uruchamianiu aplikacji z kontrolą dostępu,
   - przy otwieraniu zabezpieczonych hasłem plików.
6. Każdy użytkownik systemu, posiadający własny identyfikator zobowiązany jest do ochrony haseł, którymi się posługuje.
7. Niedopuszczalne jest zapisywanie haseł na różnego rodzaju karteczkach, nalepkach bądź bezpośrednio na biurku czy monitorze,
8. Niedopuszczalne jest podawanie haseł do czyjejkolwiek wiadomości,

9. W przypadku ujawnienia hasła musi ono zostać niezwłocznie zmienione,
10. Hasło musi być zmieniane przynajmniej raz w miesiącu,
11. Jeżeli system nie wymusi zmiany hasła użytkownik sam zobowiązany jest do dokonania tej czynności.

PROCEDURA ADMINISTRACYJNO – TECHNICZNA		
1.	**Numer**	4
2.	**Wersja**	01
3.	**Nazwa**	**Usunięcie konta w systemie teleinformatycznym.**
4.	**Odwołania do innych dokumentów**	
5.	**Status**	Obowiązująca
6.	**Data wprowadzenia**	
7.	**Data wygaśnięcia**	
8.	**Pracownik wdrażający**	Administrator Systemu Informatycznego
9.	**Zatwierdzający procedurę**	Wójt
10.	**Lista dystrybucyjna**	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego.

Usunięcie konta w systemie informatycznym oznacza trwałe odebranie uprawnień użytkownikowi do systemu teleinformatycznego Urzędu Gminy Stolno.

Następuje w wyniku działań porządkujących Administratora Systemu Informatycznego prowadzonych w uzgodnieniu z Administratorem Bezpieczeństwa Informacji. Dopuszcza się usunięcie konta z systemu, które zostało przypadkowo, błędnie określone i nie było stosowane a także kont testowych.

PROCEDURA ADMINISTRACYJNO – TECHNICZNA		
1.	**Numer**	5
2.	**Wersja**	01
3.	**Nazwa**	**Blokada konta w systemie teleinformatycznym.**
4.	**Odwołania do innych dokumentów**	*Karta blokady / usunięcia blokady / usunięcia konta / zmiany hasła w systemie*
5.	**Status**	Obowiązująca
6.	**Data wprowadzenia**	
7.	**Data wygaśnięcia**	
8.	**Pracownik wdrażający**	Administrator Systemu Informatycznego
9.	**Zatwierdzający procedurę**	Wójt
10.	**Lista dystrybucyjna**	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego.

Blokada konta w systemie teleinformatycznym oznacza czasowe odebranie użytkownikowi wszelkich uprawnień do systemu.

Konto blokowane jest niezwłocznie przez Administratora Systemu Informatycznego na wniosek przełożonego pracownika lub Administratora Bezpieczeństwa Informacji.

1. Przełożony pracownika lub Administrator Bezpieczeństwa Informacji wypełnia cz. I „*Karty blokady / usunięcia blokady / usunięcia kont / zmiany hasła w systemie*" i potwierdza podpisem w cz. II „*Karty ...*"
2. Administrator Systemu Informatycznego, zgodnie z wytycznymi w części I dokumentu dokonuje zmiany w systemie polegającej na zablokowaniu konta. Po sprawdzeniu poprawności wykonania blokady podpisuje się na dokumencie.

KARTA BLOKADY / USUNIĘCIA BLOKADY / USUNIĘCIA KONTA / ZMIANY HASŁA W SYSTEMIE archiwizowana jest przez Administratora Systemu Informatycznego w wydzielonym segregatorze.

PROCEDURA ADMINISTRACYJNO – TECHNICZNA		
1.	**Numer**	6
2.	**Wersja**	01
3.	**Nazwa**	**Odblokowanie konta w systemie teleinformatycznym**
4.	**Odwołania do innych dokumentów**	*Karta blokady / usunięcia blokady / usunięcia konta / zmiany hasła w systemie*
5.	**Status**	Obowiązująca
6.	**Data wprowadzenia**	
7.	**Data wygaśnięcia**	
8.	**Pracownik wdrażający**	Administrator Systemu Informatycznego
9.	**Zatwierdzający procedurę**	Wójt
10.	**Lista dystrybucyjna**	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego.

Odblokowanie konta w systemie teleinformatycznym oznacza przywrócenie użytkownikowi uprawnień do systemu teleinformatycznego.

Odblokowanie konta związane jest z wcześniejszym zablokowaniem dostępu do systemu:

- na skutek planowanego działania (celowa blokada wynikająca z przesłanek urlop, choroba, naruszenie bezpieczeństwa danych, inne),
- w związku z trzykrotnym użyciem niepoprawnego hasła przy logowaniu na to samo konto,
- na skutek utraty ważności konta.

Konto odblokowywane jest niezwłocznie przez Administratora Systemu Informatycznego na wniosek pracownika potwierdzony przez przełożonego pracownika lub Administratora Bezpieczeństwa Informacji.

1. Pracownik wypełnia cz. I „*Karty blokady / usunięcia blokady / usunięcia konta / zmiany hasła w systemie*"

2. Bezpośredni przełożony lub ABI akceptuje wniosek w cz. II „*Karty ...*"

3. Po otrzymaniu „*Karty ...*" Administrator Systemu Informatycznego sprawdza parametry aktywności konta, odblokowuje konto a następnie nadaje hasło początkowe tzw. „startowe", które pracownik musi zmienić przy pierwszym zalogowaniu się do systemu.

4. O odblokowaniu konta Administrator Systemu Informatycznego powiadamia zainteresowanego pracownika.

KARTA BLOKADY / USUNIĘCIA BLOKADY / USUNIĘCIA KONTA / ZMIANY HASŁA W SYSTEMIE archiwizowana jest przez Administratora Systemu Informatycznego w wydzielonym segregatorze

PROCEDURA ADMINISTRACYJNO – TECHNICZNA		
1.	**Numer**	7
2.	**Wersja**	01
3.	**Nazwa**	**Zmiana hasła w systemie teleinformatycznym**
4.	**Odwołania do innych dokumentów**	*Karta blokady / usunięcia blokady / usunięcia konta / zmiany hasła w systemie*
5.	**Status**	Obowiązująca
6.	**Data wprowadzenia**	
7.	**Data wygaśnięcia**	
8.	**Pracownik wdrażający**	Administrator Systemu Informatycznego
9.	**Zatwierdzający procedurę**	Wójt
10.	**Lista dystrybucyjna**	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego.

Zmiana hasła dokonywana jest samodzielnie przez pracownika zgodnie z określonym harmonogramem. W pozostałych przypadkach (np.: użytkownik zapomni hasło, którym się posługiwał, system nie pozwala na samodzielną zmianę hasła) Administrator Systemu Informatycznego na wniosek pracownika nadaje hasło startowe.

1. Pracownik wypełnia cz. I „*Karty blokady / usunięcia blokady / usunięcia konta / zmiany hasła w systemie*"

2. Bezpośredni przełożony lub Administrator Bezpieczeństwa Informacji akceptuje wniosek w cz. II „*Karty ...*"

3. Na wniosek Administrator Systemu Informatycznego sprawdza parametry aktywności konta, w razie potrzeby odblokowuje konto a następnie ustala nowe hasło tzw. „startowe", które pracownik zobowiązany jest do zmiany przy pierwszym zalogowaniu się do systemu.

4. O zmianie hasła do konta Administrator Systemu Informatycznego powiadamia zainteresowanego pracownika.

KARTA BLOKADY / USUNIĘCIA BLOKADY / USUNIĘCIA KONTA / ZMIANY HASŁA W SYSTEMIE archiwizowana jest przez Administratora Systemu Informatycznego w wydzielonym segregatorze.

KARTA

BLOKADY / USUNIĘCIA BLOKADY / ZMIANY HASŁA / USUNIĘCIA KONTA W SYSTEMIE

Nr karty:.....*(nadaje Administrator Systemu Informatycznego)*

Część I

.....
Komórka organizacyjna

Stolno, dnia.....

Proszę o zablokowanie/odblokowanie/zmianę hasła/usunięcie konta w systemie*)

pani/pana .....

z powodu.....

od ..... do .....(dotyczy tylko zablokowania)

.....
data i podpis pracownika

Część II

Zatwierdzam zmiany zablokowania/odblokowania/zmiana hasła/usunięcia konta w systemie*).

.....
data i podpis
Kierownika komórki organizacyjnej / ABI

Cześć III

Zablokowanie/odblokowanie/zmiana hasła/usunięcie konta z systemu wykonano*)

Hasło startowe: .....(dotyczy tylko odblokowania konta i zmiany hasła)

.....
data i podpis pracownika

.....
data i podpis
Administratora Systemu Informatycznego

*)- niepotrzebne skreślić

PROCEDURA ADMINISTRACYJNO – TECHNICZNA		
1.	**Numer**	8
2.	**Wersja**	01
3.	**Nazwa**	**Modyfikacja uprawnień w systemie**
4.	**Odwołania do innych dokumentów**	
5.	**Status**	Obowiązująca
6.	**Data wprowadzenia**	
7.	**Data wygaśnięcia**	
8.	**Pracownik wdrażający**	Administrator Systemu Informatycznego
9.	**Zatwierdzający procedurę**	Wójt
10.	**Lista dystrybucyjna**	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego.

Dotyczy zmiany istniejących uprawnień w związku:

- ze zmianą oprogramowania
- z przekazaniem zasobów po osobie zwalnianej lub przechodzącej na inne stanowisko
- z przejęciem zasobów okresowo na czas nieobecności pracownika (urlop, choroba, delegacja)

1. Pracownik wypełnia część I „*Karty modyfikacji w systemie*"

2. Kierownik komórki organizacyjnej zatwierdza zmiany, jakie mają być wykonane w systemie - część II

3. Administrator Systemu Informatycznego dokonuje wymaganej zmiany. Po sprawdzeniu poprawności wykonania modyfikacji w systemie, podpisuje się na dokumencie - część III

4. „*Karty modyfikacji systemu*" archiwizowane są przez Administratora Systemu Informatycznego w wyznaczonym segregatorze.

KARTA

MODYFIKACJI W SYSTEMIE

Nr karty:.....*(nadaje Administrator Systemu Informatycznego)*

Część I

.....
Komórka organizacyjna

Stolno, dnia .....

Proszę o dodanie/usunięcie panu/pani.....

niżej zaznaczonych aplikacji niestandardowych:

☐ *dostęp do Internetu*

☐ *konto poczty zewnętrznej*

☐ *LEX - System Informacji Prawnej*

☐ *Microsoft PowerPoint (aplikacja do tworzenia prezentacji)*

☐ *Microsoft Access*

☐ *Inne:* .....

lub udostępnienia

☐ profilu stacji roboczej numer ..... przypisanej do osoby .....

☐ zasobów sieciowych osoby.....

Data obowiązywania: od.....

.....
data i podpis pracownika

Część II

Zatwierdzam modyfikację w systemie wymienioną w cz. I-szej.

.....
data i podpis
Kierownika komórki organizacyjnej

Cześć III

Modyfikację wykonano.

.....
data i podpis pracownika

.....
data i podpis
Administratora Systemu Informatycznego

PROCEDURA ADMINISTRACYJNO - TECHNICZNA		
1.	**Numer**	9
2.	**Wersja**	01
3.	**Nazwa**	**Zgłoszenie awarii działania sprzętu komputerowego**
4.	**Odwołania do innych dokumentów**	
5.	**Status**	Obowiązująca
6.	**Data wprowadzenia**	
7.	**Data wygaśnięcia**	
8.	**Pracownik wdrażający**	Administrator Systemu Informatycznego
9.	**Zatwierdzający procedurę**	Wójt
10.	**Lista dystrybucyjna**	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego.

Zgłoszenia awarii przyjmowane są pisemnie lub ustnie w zależności od złożoności awarii. Złożoność awarii jest określana podczas wstępnej rozmowy pracownika zgłaszającego awarię z ASI.

1. W przypadku awarii zgłaszanych pisemnie użytkownik wypełnia część I *„Karty zgłoszenia awarii działania sprzętu komputerowego"*

2. Użytkownik przekazuje Administratorowi sieci zgłoszenie awarii (część I)

3. Administrator Systemu Informatycznego przyjmuje zgłoszenie (wypełnia część II):
   - wpisuje datę przyjęcia zgłoszenia
   - wpisuje uwagi i wnioski (np. zgłoszenie do serwisu)
   - wpisuje datę zakończenia pracy i składa podpis

4. Dokument *„Karta zgłoszenia awarii"* przechowywana jest przez Administratora Systemu Informatycznego w odpowiednim segregatorze.

5. W przypadku zgłoszenia awarii w formie ustnej (awaria drobna) zostaje ona usunięta przez ASI.

KARTA

ZGŁOSZENIA AWARII

Nr karty:.....*(nadaje Administrator Systemu Informatycznego)*

Część I

..... Stolno, dnia .....

Komórka organizacyjna

Zgłaszam awarię:

☐- komputera:.....

(numer inwentarzowy, numer stacji)

☐- drukarki:.....

(numer inwentarzowy)

☐- programu:.....

Inne: .....

....

Stanowisko *numer pokoju* *nr telefonu*

.....

data i podpis osoby zgłaszającej

Część II

Zgłoszenie przyjęte:

Data przyjęcia:..... Data wykonania:.....

Uwagi i wnioski: .....

.....

.....

.....

.....

podpis

Administratora Systemu Informatycznego

PROCEDURA ADMINISTRACYJNO - TECHNICZNA		
1.	**Numer**	10
2.	**Wersja**	01
3.	**Nazwa**	**Dostęp użytkownika do systemu informatycznego poza godzinami urzędowania**
4.	**Odwołania do innych dokumentów**	
5.	**Status**	Obowiązująca
6.	**Data wprowadzenia**	
7.	**Data wygaśnięcia**	
8.	**Pracownik wdrażający**	Administrator Systemu Informatycznego
9.	**Zatwierdzający procedurę**	Wójt
10.	**Lista dystrybucyjna**	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego.

Standardowo w systemie informatycznym zdefiniowany jest dostęp zgodnie z godzinami pracy Urzędu (dotyczy systemów, które pozwalają na takowe ograniczenia dostępowe) tj. od poniedziałku do piątku 7,30 ÷ 15,15, z wyjątkiem wtorku, kiedy Urząd jest czynny w godz. 7,30 ÷ 16,30. Każda praca poza określonym terminem wymaga zgody Wójta Gminy Stolno lub bezpośredniego przełożonego i zmiany w systemie informatycznym z wyjątkiem komputerów przenośnych.

1. Bezpośredni przełożony pracownika wypełnia cześć I *„Kartę zmiany godzin pracy”* będącej załącznikiem do *Procedury nr 10.*
2. Po podpisaniu *„Karta ...”* przekazywana jest do Administratora Systemu Informatycznego.
3. Administrator Systemu Informatycznego, osoba zastępująca Administratora Systemu Informatycznego wprowadza zmiany w systemie informatycznym odnotowując ten fakt w cz. II.
4. *„Karta zmiany godzin pracy”* archiwizowana jest przez Administratora Systemu Informatycznego w segregatorze.

KARTA

ZMIANY GODZIN PRACY

Nr karty:.....*(nadaje Administrator Systemu Informatycznego)*

Część I

.....
Komórka organizacyjna

Stolno, dnia .....

Proszę o udostępnienie systemu informatycznego
pani/ panu .....
(imię i nazwisko)

.....	.....	.....
Stanowisko	*numer pokoju*	*nr telefonu*

W godzinach od ..... do .....

W okresie od ..... do .....

.....
data i podpis
Kierownik komórki organizacyjnej

Część II

Zmiana godzin pracy wykonana.

.....
Data i podpis informatyka

.....
data i podpis
Administratora Systemu Informatycznego

Część III

Anulowanic zlecenia.

PROCEDURA ADMINISTRACYJNO - TECHNICZNA		
1.	**Numer**	11
2.	**Wersja**	01
3.	**Nazwa**	**Przyjęcie do ewidencji nowego sprzętu informatycznego (komputery, drukarki, switche, skanery, serwery, itp)**
4.	**Odwołania do innych dokumentów**	*Procedura administracyjno – techniczna numer 12*
5.	**Status**	Obowiązująca
6.	**Data wprowadzenia**	
7.	**Data wygaśnięcia**	
8.	**Pracownik wdrażający**	Administrator Systemu Informatycznego
9.	**Zatwierdzający procedurę**	Wójt
10.	**Lista dystrybucyjna**	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego.

Każdy nowo zakupiony sprzęt informatyczny przed przekazaniem do eksploatacji należy zarejestrować w systemie ewidencji środków trwałych lub w ewidencji przedmiotów niematerialnych i w systemie finansowym.

1. Sprzęt oraz oprogramowanie przekazywane jest do Administratora Systemu Informatycznego wraz z fakturą (w przypadku przesyłek również z listem przewozowym).
2. Pracownik wymieniony w pkt. 1 po opisaniu dokumenty przekazuje do Referatu Planowania i Finansów w celu rejestracji.
3. Pracownik Referatu Planowania i Finansów rejestruje fakturę i podpisuje ją pod względem finansowym odwrotnej stronie, na której znajduje się:
   - Opis pod względem merytorycznym
   - Data
   - Podpis Administratora Systemu Informatycznego
   - Przeznaczenie każdej pozycji (w przypadku, gdy na fakturze jest zbiorcze zestawienie sprzętu, należy załączyć szczegółowe zestawienie – specyfikację sprzętu)
4. Na podstawie załączonego szczegółowego zestawienia, sprzęt informatyczny jest rejestrowany w Książce - Ewidencji Środków Trwałych lub nadawany numer inwentarzowy. Każdy sprzęt informatyczny musi mieć nadany indywidualny numer inwentarzowy zgodnie z przyjętymi w Urzędzie Gminy Stolno zasadami. Zestawienie zbiorcze sprzętu z przypisanymi numerami inwentarzowymi pozostaje w Referacie Planowania i Finansów.

5. Administrator Systemu Informatycznego wprowadza sprzęt informatyczny do „Ewidencji Sprzętu komputerowego, licencji i oprogramowania", zgodnie z Procedurą 12, dokonując zmian w ewidencji wyposażenia stanowiska w sprzęt informatyczny. Wszystkie karty gwarancyjne i licencje, protokoły naprawy, karty zgłoszenia do naprawy przechowywane są w wydzielonym segregatorze.

PROCEDURA ADMINISTRACYJNO - TECHNICZNA		
1.	**Numer**	12
2.	**Wersja**	01
3.	**Nazwa**	**Wyposażenie stanowiska pracy w sprzęt informatyczny**
4.	**Odwołania do innych dokumentów**	
5.	**Status**	Obowiązująca
6.	**Data wprowadzenia**	
7.	**Data wygaśnięcia**	
8.	**Pracownik wdrażający**	Administrator Systemu Informatycznego
9.	**Zatwierdzający procedurę**	Wójt
10.	**Lista dystrybucyjna**	Kierownicy komórek organizacyjnych, Administrator Bezpieczeństwa Informacji, Użytkownicy systemu informatycznego.

1. Każde stanowisko pracy powinno być wyposażone w „*Kartę wyposażenia stanowiska pracy*" w celu określenia jednoznacznej odpowiedzialności pracownika za powierzony sprzęt. Po skonfigurowaniu komputera i podłączeniu do sieci informatyk sprawdza poprawność logowania i zainstalowanego oprogramowania.
2. Administrator Systemu Informatycznego wypełnia część dokumentu dotyczącą sprzętu komputerowego.
3. Pracownik Referatu Planowania i Finansów – wypełnia część dokumentu dotyczącą pozostałego wyposażenia.
4. Pracownik przejmujący, sprawdza wyszczególniony sprzęt, zgodność numerów inwentarzowych, numerów fabrycznych i podpisuje odbiór.
5. „*Karta wyposażenia stanowiska pracy*" przechowywana jest przez Administratora Systemu Informatycznego.
6. Numer karty zapisany jest w ewidencji pracowników prowadzonej przez Administratora Systemu Informatycznego.
7. Przy zmianie w wyposażeniu wystawia się nową „*Kartę wyposażenia ...*" wypełniając tylko dodatkowy sprzęt. Na starej „*Karcie...*" odnotowuje się zdanie sprzętu.
8. Przy zwolnieniu pracownika lub przekazywania stanowiska innemu pracownikowi, pracownik Referatu Planowania i Finansów i Administrator Systemu Informatycznego odnotowuje zdanie sprzętu na odwrocie karty, podpisując zgodność zdawanego sprzętu.

KARTA

WYPOSAŻENIA STANOWISKA PRACY NR ...

z dnia .....

Imię i nazwisko: .....

Komórka organizacyjna: .....

Stanowisko: .....

Numer pokoju: .....

Stanowisko pracy wyposażone jest:

1. Stacja robocza

Lp.	Nazwa	Numer sprzętu	Numer inwentarzowy	Uwagi
1.	Stacja robocza			
2.	Monitor			
3.	Klawiatura			
4.	Mysz			
5.	Drukarka			
6.	UPS			
7.	Skaner			
8.				
9.				
10.				

2. Inne wyposażenie

Lp.	Nazwa	Numer fabryczny	Numer inwentarzowy	uwagi
1.	Telefon stacjonarny			
2.	Telefon komórkowy			
3.	Aparat fotograficzny			
4.				
5.				
6.				

.....
data i podpis pracownika zdającego

.....
data i podpis pracownika przyjmującego

PROCEDURA ADMINISTRACYJNO - TECHNICZNA		
1.	**Numer**	13
2.	**Wersja**	01
3.	**Nazwa**	**Postępowania w przypadku powzięcia zamiaru o planowanym rozwiązaniu umowy o pracę z pracownikiem Urzędu**
4.	**Odwołania do innych dokumentów**	*Procedura administracyjno – techniczna numer 4* *Procedura administracyjno – techniczna numer 5*
5.	**Status**	Obowiązująca
6.	**Data wprowadzenia**	
7.	**Data wygaśnięcia**	
8.	**Pracownik wdrażający**	Administrator Systemu Informatycznego
9.	**Zatwierdzający procedurę**	Wójt
10.	**Lista dystrybucyjna**	

1. W przypadku powzięcia zamiaru o planowanym rozwiązaniu umowy o pracę z pracownikiem pracującym w systemie informatycznym, bezpośredni przełożony wypełnia „*Kartę wyrejestrowania z systemu*".
2. Po wypełnieniu przełożony niezwłocznie przekazuje ją do Administratora Systemu Informatycznego, który niezwłocznie przystępuje do realizacji zgłoszenia.
3. Administrator Systemu Informatycznego informuje przełożonego pracownika, z którym ma być rozwiązana umowa o pracę, o wykonaniu zgłoszenia.
4. Zgłoszenie się do Administratora Systemu Informatycznego, zwalnianego pracownika z kartą obiegową stanowi podstawę do zablokowania konta a następnie trwałego usunięcia konta użytkownika systemu teleinformatycznego.

KARTA

WYREJESTROWANIA Z SYSTEMU

Nr karty:.....*(nadaje Administrator Systemu Informatycznego)*

Część I

.....
Komórka organizacyjna

Stolno, dnia .....

Proszę o cofnięcie uprawnień do systemu pani/ panu.....
(imię i nazwisko)

.....
Stanowisko

.....
numer pokoju

z dniem .....

.....
data i podpis
Kierownika komórki organizacyjnej

Część II

Realizacja zgłoszenia

Data przyjęcia:.....

Uwagi i wnioski: .....

.....
data i podpis
Administratora Systemu Informatycznego

Część III

Trwałe usunięcie konta

.....
data i podpis
Administratora Systemu Informatycznego

PROCEDURY AWARYJNE

Dla zachowania bezpieczeństwa przetwarzanych danych w Urzędzie pracownicy zobowiązani są do przestrzegania zasad określonego postępowania i zachowania się, przedstawionego w procedurach, w sytuacjach takich jak:

- **Naruszenie danych osobowych** **Procedura nr 1**
- **Zanik zasilania energetycznego** **Procedura nr 2**
- **Wystąpienie klęsk żywiołowych - pożar** **Procedura nr 3**
- **Wystąpienie klęsk żywiołowych - powódź** **Procedura nr 4**
- **Zalanie lub zatopienie pomieszczenia** **Procedura nr 5**
- **Wystąpienie zagrożenia terrorystycznego** **Procedura nr 6**

PROCEDURA AWARYJNA		
1.	**Numer**	1
2.	**Wersja**	01
3.	**Okoliczności stosowania procedury**	**W przypadku naruszenia danych osobowych**
4.	**Odwołania do innych dokumentów**	*Instrukcja postępowania w sytuacji naruszenia systemu ochrony danych osobowych* stanowiąca załącznik nr 2 do *Polityki Bezpieczeństwa* Urzędu Gminy Stolno.
5.	**Status**	Obowiązująca
6.	**Data wprowadzenia**	
7.	**Data wygaśnięcia**	
8.	**Pracownik wdrażający**	Administrator Bezpieczeństwa Informacji
9.	**Zatwierdzający procedurę**	Wójt
10.	**Lista dystrybucyjna**	

Wszelkie zauważone przez użytkowników zjawiska mogące naruszyć bezpieczeństwo stacji komputerowych, osób, sprzętu, oprogramowania, dokumentów lub bezpieczeństwa fizycznego muszą być niezwłocznie zgłoszone do Administratora Bezpieczeństwa Informacji/Administratora Systemu Informatycznego lub bezpośredniego przełożonego. Osoby te mają obowiązek określenia skali naruszenia bezpieczeństwa. Postępowanie jest określone w *Instrukcji postępowania w sytuacji naruszenia systemu ochrony danych osobowych* stanowiącej załącznik nr 2 do *Polityki Bezpieczeństwa* Urzędu Gminy Stolno.

PROCEDURA AWARYJNA		
1.	**Numer**	2
2.	**Wersja**	01
3.	**Okoliczności stosowania procedury**	**W przypadku zaniku zasilania**
4.	**Odwołania do innych dokumentów**	*Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczona dla użytkowników systemu* stanowiące załącznik nr 3 *do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.*
5.	**Status**	Obowiązująca
6.	**Data wprowadzenia**	
7.	**Data wygaśnięcia**	
8.	**Pracownik wdrażający**	Administrator Bezpieczeństwa Informacji
9.	**Zatwierdzający procedurę**	Wójt
10.	**Lista dystrybucyjna**	

Wobec braku oddzielnej (awaryjnej) linii zasilania energetycznego, która zasilałaby w energię elektryczną obiekt Urzędu w przypadku braku napięcia w linii głównej, serwer oraz kluczowe stanowiska komputerowe są zabezpieczone urządzeniem podtrzymującym zasilanie elektryczne (zasilacz awaryjny UPS podtrzymujący napięcie do 15 min.). Urządzenie to powinno pozwolić na prawidłowe i bezpieczne zakończenie pracy i zamknięcie systemu operacyjnego.

W przypadku długotrwałej awarii zasilania Wójt podejmuje decyzję w zakresie środków zaradczych i kontynuacji pracy Urzędu.

W przypadku wystąpieniu braku zasilania, pracownik przystępuje do bezpiecznego zakończenie pracy na stanowisku komputerowym zgodnie do zaleceń określonych w **Procedurach rozpoczęcia, zawieszenia i zakończenia pracy przeznaczonych dla użytkowników systemu** stanowiących *załącznik nr 3 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.*

	PROCEDURA AWARYJNA	
1.	**Numer**	3
2.	**Wersja**	01
3.	**Okoliczności stosowania procedury**	**W sytuacjach wystąpienia klęsk żywiołowych - pożar**
4.	**Odwołania do innych dokumentów**	*Instrukcja Bezpieczeństwa Pożarowego Urzędu Gminy Stolno*
5.	**Status**	Obowiązująca
6.	**Data wprowadzenia**	
7.	**Data wygaśnięcia**	
8.	**Pracownik wdrażający**	Administrator Bezpieczeństwa Informacji
9.	**Zatwierdzający procedurę**	Wójt
10.	**Lista dystrybucyjna**	

W przypadku wystąpienia klęski żywiołowej – pożaru, należy zastosować się do aktualnie obowiązujących szczegółowych instrukcji przeciwpożarowych i ewakuacyjnych Urzędu zawartych w Instrukcji Bezpieczeństwa Pożarowego budynku Urzędu Gminy Stolno, Stolno 112 oraz w niniejszej *Procedurze.*

1. Każdy, kto zauważy pożar obowiązany jest dostępnymi środkami niezwłocznie zawiadomić osoby znajdujące się w strefie zagrożenia pożarem w celu podjęcia działań alarmowych, ratowniczych czy ewakuacyjnych.
2. Należy **wezwać Straż Pożarną - tel. alarmowy 998 lub 112.** Po zgłoszeniu się dyżurnego spokojnym głosem podać następujące informacje:
   - przedstawić się - podając imię i nazwisko, nr telefonu, z którego prowadzi się rozmowę oraz informację o zdarzeniu,
   - adres i nazwę obiektu,
   - co się pali – pokój, na korytarzu, piętro, parter, itp.,
   - czy jest zagrożenie dla zdrowia i życie osób przebywających w obiekcie,
   - udzielić innych informacji na zadane pytania przez dyżurnego,
   - po udzieleniu wszystkich informacji wysłuchać zaleceń dyżurnego, co do dalszego zachowanie się i postępowania,
   - nie odkładać słuchawki telefonicznej do chwili potwierdzenia przyjęcia zgłoszenia.

Przyjmujący zgłoszenie może również potwierdzić zgłoszenie poprzez oddzwonienie.

3. W przypadku wystąpienia pożaru wszyscy pracownicy zobowiązani są do podjęcia działań zmierzających do jego likwidacji.
4. Jeżeli pozwalają na to warunki, równocześnie z alarmowaniem o niebezpieczeństwie należy przystąpić do gaszenia pożaru za pomocą podręcznego sprzętu gaśniczego będącego na wyposażeniu budynku w miejscach oznakowanych:
   - GAŚNIC śniegowych, proszkowych
   - HYDRANTU
5. Przed przystąpieniem do akcji gaśniczej, dla bezpieczeństwa ludzi i mienia, należy pamiętać o odłączeniu zasilania elektrycznego i dopływu gazu do miejsca zagrożenia.
6. Wszyscy, nie biorący udziału w gaszeniu zobowiązani są skierować się do najbliższej drogi ewakuacyjnej prowadzącej na zewnątrz budynku, oznakowanej znakami ewakuacyjnymi.
7. Wszyscy pracownicy zobowiązani są do udzielenia wzajemnej pomocy osobom, których życie i zdrowie zostało zagrożone pożarem.
8. Wszystkie działania ratowniczo-gaśnicze należy prowadzić tak, aby nie powstała panika osób będących w zagrożeniu.
9. Podczas prowadzonych działań ratowniczo-gaśniczych należy kierować się rozwagą w podejmowaniu decyzji.
10. Do czasu przybycia straży pożarnej działaniami ratowniczo gaśniczymi kieruje Wójt lub wskazana osoba energiczna i opanowana.

	PROCEDURA AWARYJNA	
1.	**Numer**	4
2.	**Wersja**	01
3.	**Okoliczności stosowania procedury**	**W sytuacjach wystąpienia klęsk żywiołowych – powódź**
4.	**Odwołania do innych dokumentów**	*Instrukcja Bezpieczeństwa Pożarowego dla obiektu przy ul. Wybickiego nr 38*
5.	**Status**	Obowiązująca
6.	**Data wprowadzenia**	
7.	**Data wygaśnięcia**	
8.	**Pracownik wdrażający**	Administrator Bezpieczeństwa Informacji
9.	**Zatwierdzający procedurę**	Wójt
10.	**Lista dystrybucyjna**	

W przypadku wystąpienia klęski żywiołowej – powódź, należy zastosować się do aktualnie obowiązujących szczegółowych instrukcji ewakuacyjnych Urzędu opracowanych przez pracownika Obrony Cywilnej Urzędu Gminy Stolno i ochrony przeciwpożarowej oraz zawartych w niniejszej *Procedurze*.

1. W przypadku wystąpienia powodzi wszyscy pracownicy zobowiązani są do podjęcia działań zmierzających do zminimalizowania jej skutków dla bytu Urzędu. W tym też celu wszelkimi, dostępnymi środkami należy powiadomić osoby znajdujące się w budynku.
2. Należy wyłączyć prąd w zagrożonej wodą części obiektu.
3. Następnie należy powiadomić dyżurnego straży pożarnej pod numerem ogólnokrajowego **telefonu alarmowego - 998 lub 112** przekazując w sposób wyraźny informacje:
   - przedstawić się - podając imię i nazwisko, nr telefonu, z którego prowadzi się rozmowę oraz informację o zdarzeniu,
   - adres i nazwę obiektu,
   - co zostało zalane – pokój, korytarz, parter, piwnica, itp.,
   - czy jest zagrożenie dla zdrowia i życie osób przebywających w obiekcie,
   - udzielić innych informacji na zadane pytania przez dyżurnego

- po udzieleniu wszystkich informacji wysłuchać zaleceń dyżurnego co do dalszego zachowanie się i postępowania
- nie odkładać słuchawki telefonicznej do chwili potwierdzenia przyjęcia zgłoszenia.

4. Ogólnie dostępnymi środkami, przedmiotami przystąpić do zabezpieczania obiektu przed dalszymi skutkami wody udzielając pomocy osobom zagrożonym, przystępując do ewakuacji zagrożonego mienia.
5. Przed przystąpieniem do akcji ratunkowej, dla bezpieczeństwa ludzi i mienia, należy pamiętać o odłączeniu zasilania elektrycznego do miejsca objętego zdarzeniem.
6. Podczas prowadzonych działań ratowniczych należy kierować się rozwagą w podejmowaniu decyzji.
7. Do czasu przybycia straży pożarnej działaniami ratowniczymi kieruje Wójt lub wskazana osoba energiczna i opanowana

Podstawową czynnością użytkowników w przedstawionych powyżej sytuacji jest zabezpieczenie nośników informacji i wyłączenie stacji komputerowej.

PROCEDURA AWARYJNA		
1.	**Numer**	5
2.	**Wersja**	01
3.	**Okoliczności stosowania procedury**	**W sytuacji wystąpienia zalania lub zatopienia pomieszczenia**
4.	**Odwołania do innych dokumentów**	*Akty prawa wewnętrznego*
5.	**Status**	Obowiązująca
6.	**Data wprowadzenia**	
7.	**Data wygaśnięcia**	
8.	**Pracownik wdrażający**	Administrator Bezpieczeństwa Informacji
9.	**Zatwierdzający procedurę**	Wójt
10.	**Lista dystrybucyjna**	

W przypadku wstąpienia zalania lub zatopienia pomieszczenia, w którym przetwarzane są dane osobowe wszyscy pracownicy Urzędu zobowiązani są do postępowania zgodnie z przepisami porządkowymi i aktami prawa wewnętrznego obowiązującymi w tym zakresie w Urzędzie.

W czasie godzin pracy Urzędu każdy pracownik, który zauważył wystąpienie zagrożenia natychmiast powiadamia o zdarzeniu kierownictwo Urzędu, przystępuje do zakończenia pracy na swoim stanowisku i podejmuje działania zabezpieczające dokumenty z przetwarzanymi danymi osobowymi.

Po otrzymaniu informacji osoba z kierownictwa Urzędu dąży do ustalenia, w szczególności:

- rodzaju awarii
- miejsca awarii.

Uzyskując informacje na powyższe pytania osoby te podejmują natychmiastowe przeciwdziałania zapobiegające skutkom awarii i powiadamia pracownika odpowiedzialnego za konserwację obiektu i odpowiedzialne specjalistyczne służby - Straż Pożarną.

Do czasu przybycia specjalistycznych służb, działaniami kieruje osoba z kierownictwa Urzędu. Po przybyciu do Urzędu służb specjalistycznych przedstawiciel kierownictwa

przekazuje kierowanie działaniami przedstawicielowi Straży Pożarnej składając relację z dotychczas podjętych czynności ograniczających skutki awarii.

Podstawową czynnością użytkowników w przedstawionych powyżej sytuacjach jest zabezpieczenie nośników informacji i wyłączenie stacji komputerowej.

	PROCEDURA AWARYJNA	
1.	**Numer**	6
2.	**Wersja**	01
3.	**Okoliczności stosowania procedury**	**W sytuacji wystąpienia zagrożenia terrorystycznego**
4.	**Odwołania do innych dokumentów**	*Formularz prowadzonej rozmowy z osobą informującą* stanowiącym załącznik do niniejszego dokumentu.
5.	**Status**	Obowiązująca
6.	**Data wprowadzenia**	
7.	**Data wygaśnięcia**	
8.	**Pracownik wdrażający**	Administrator Bezpieczeństwa Informacji
9.	**Zatwierdzający procedurę**	Wójt
10.	**Lista dystrybucyjna**	

Zagrożeniem terrorystycznym może być:

1. znalezienie podejrzanej paczki (przedmiotu)
2. otrzymanie podejrzanej przesyłki
3. otrzymanie telefonu o podłożonym ładunku wybuchowym
4. itp.

Stosownie do stanowiska pracy, miejsca pracy oraz zakresu obowiązków służbowych, pracownicy Urzędu powinni codziennie przed przystąpieniem do wykonywania czynności służbowych dokonać kontroli pomieszczeń służbowych pod kątem ukrycia podejrzanej paczki lub jakiegokolwiek podejrzanego przedmiotu. Wykonując te czynności należy szczególną uwagę zwrócić na kosze na śmieci, pomieszczenia ogólnodostępne jak np. toalety, gdyż do tych miejsc i przedmiotów w sposób niekontrolowany mają dostęp różne osoby spoza grona zatrudnionych pracowników.

W przypadku **znalezienia podejrzanego przedmiotu (paczki) w nietypowym miejscu w budynku Urzędu**, Kierownik komórki organizacyjnej niezwłocznie powiadamia o fakcie kierownictwo Urzędu podejmując jednocześnie czynności zabezpieczające miejsce znalezienia, uniemożliwiając do niego dostęp innym osobom. Informację taką należy niezwłocznie przekazać również do Dyżurnego Policji.

W sytuacji takiej nie należy:

- ulegać panice