Załącznik Nr 1
do Zarządzenia Nr 68/2013
Wójta Gminy Szczecinek
z dnia 22 sierpnia 2013 r.

POLITYKA BEZPIECZEŃSTWA

w zakresie zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Szczecinek

Rozdział I

Postanowienia ogólne

1. Celem polityki bezpieczeństwa w zakresie zarządzania systemem informatycznym służącym do przetwarzania danych osobowych jest zapewnianie ochrony danych osobowych oraz określenie środków technicznych i organizacyjnych dla poufności przetwarzanych danych w Urzędzie Gminy Szczecinek.
2. Polityka bezpieczeństwa zawiera:
   1) Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.
   2) Wykaz zbiorów danych osobowych oraz programy zastosowane do przetwarzania tych danych.
   3) Opis struktury zbioru danych osobowych.
   4) Określenie środków technicznych i organizacyjnych dla zapewnienia poufności przetwarzania danych.

Rozdział II

Wykaz pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe w systemie informatycznym

L.p.	Pomieszczenia	Nazwa zbioru (bazy danych)	Rodzaj zabezpieczenia
1	2	3	4
1	Parter, p. nr 1	* ewidencja podatników * ewidencja nieruchomości * archiwalne dane z DOS-owych aplikacji FK - ZETO Koszalin	- system alarmowy, - systemy haseł, - zasilacze UPS, - odrębny VLAN (dla działu księgowości)

1	2	3	4
2.	Parter, p. nr 2	* ewidencja ludności PESEL i dowodów osobistych * stały rejestr wyborców * system ZMOKU	system alarmowy, okratowane okna, zamykane szafy, wzmocnione drzwi, systemy haseł, karty personalne, zasilacze UPS,
3.	Parter, p. nr 5	* ewidencja gruntów	system alarmowy, zamykane szafy, systemy haseł, kontrola adresu IP, zasilacze UPS,
4.	Parter, sekretariat	* system e-DOK	system alarmowy, zamykane szafy, systemy haseł, zasilacze UPS
5.	Parter, p. nr 9	* ewidencja podatników	system alarmowy, okratowane okna, systemy haseł, zasilacze UPS, odrębny VLAN,
6.	Parter, p. nr 10	* ewidencja podatników	system alarmowy, okratowane okna, systemy haseł, zasilacz UPS, odrębny VLAN,
7.	Parter, p. nr 11 oraz kasa	* ewidencja wniosków i decyzji w sprawie dodatków mieszkaniowych * ewidencja podatników, * ewidencje kadrowo - płacowe * program Płatnika	system alarmowy, okratowane okna, zamykane szafy, zasilacze UPS, odrębny VLAN,
8.	Piwnica	* serwer Novell Netware v. 4.11 * serwer Windows 2003 * serwer Linux SUSE	system alarmowy, wzmocnione drzwi, klimatyzacja, pełne zabezpieczenie zasilaczami UPS,
9.	1 piętro, p. nr 14	* dokumentacja kadrowa pracowników, * ewidencja kadrowa pracowników,	system alarmowy, zamykane szafy, wzmocnione drzwi, zasilacz UPS, odrębny VLAN,
10.	1 piętro, p. nr 16	- rozdzielnia - pomieszczenie zarządzające pracą sieci komputerowej.	system alarmowy, zamykane szafy, zasilacz UPS,
11.	2 piętro, p. nr 26	- ewidencje Gospodarki Odpadami	systemy haseł, zasilacz UPS, odrębny VLAN,

Wszystkie komputery są zabezpieczone licencjonowanym oprogramowaniem antywirusowym z centralną aktualizacją baz sygnatur z serwera znajdującego się w serwerowni.

Rozdział III

Wykaz zbiorów danych osobowych oraz programy zastosowane do przetwarzania danych osobowych

Lp.	Nazwa zbioru	Nazwa programu (systemu), sposób zabezpieczenia
1.	Ewidencja ludności PESEL i dowodów osobistych	SELWin, ver. 1.00.16.0025, identyfikator, hasło
2.	Stały rejestr wyborców	RWWin (moduł w SELWin), identyf., hasło
3.	Ewidencja podatników	FK - identyfikator, hasło
4.	Zbiór płacowy	Place - identyfikator, hasło
5.	Ewidencja wniosków i decyzji w sprawie dodatków mieszkaniowych	Dodatki v. 1.0.0 - identyfikator, hasło
6.	Ewidencja gruntów	EGB v.5 Win - identyfikator, hasło
7.	Ewidencja gruntów i budynków	TurboEWID - identyfikator i hasło, dostęp tylko przez internet i tylko z IP przydzielonych dla UG Szczecinek.
8.	Gospodarka Odpadami na terenie Miasta i Gminy	GOMiG – identyfikator, hasło

Rozdział IV

Spis programów przetwarzających zbiory danych osobowych wraz z producentami tych programów i wykorzystywanymi bazami danych

Lp.	Nazwa programu	Producent i rodzaj bazy danych
1	SELWin System Ewidencji Ludności pod Windows	ARAM ul.Belwederska 6a 00-762 Warszawa www.aram.com.pl Baza danych: MS SQL Serwer
2	RWWin Rejestr Wyborców pod Windows (moduł w programie SELWin)	jak wyżej
3	Gmina ver. 2 (Finanse i Księgowość)	ZETO Sp. z o.o. ul. 4 Marca 38, 75-708 Koszalin www.zeto.koszalin.pl baza danych: Serwer SUSE
4	Kadry i płace	jak wyżej

5	system Gmina FK (DOS) oparty o Novell Netware 4.11 (stary system bez aktualizacji – nie aktywny utrzymywany w celach archiwalnych w serwerowni UG)	jak wyżej
6	EGB v.5 Win Ewidencja Gruntów i Budynków wersja 5 pod Windows (system pasywny bez aktualizacji)	„GEOBAZA" Sp. z o.o. ul. Łokietka 10/2, 84-300 Lębork www.geobaza.com.pl Baza danych: Pervasive Database SQL V8 SP1
7	Turbo EWID dostęp przez przeglądarkę internetową,	GEOMATYKA - KRAKÓW S.C. ul. Mała Góra 30, 30-864 Kraków baza danych pobierana on-line ze Starostwa Powiatowego (aktualizacja na bieżąco)
8	eDOK - elektroniczny obieg dokumentów (WinSerwer 2003)	Sygnity SA Aleje Jerozolimskie 180, 02-486 Warszawa
9	GOMiG Gospodarka Odpadami na terenie Miasta i Gminy	ARISCO Sp. z o.o. ul. Nawrot 114 90-029 Łódź Baza: Firebird, wersja 2.1

Rozdział V

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

1. Zasady ogólne

1.1. Podstawowym sposobem zabezpieczenia danych i dostępu do nich jest system definiowania użytkowników, grup użytkowników oraz haseł. Są to zabezpieczenia programowe wmontowane w eksploatowane systemy uniemożliwiające dostęp do funkcji użytkowych systemu osobom nieupoważnionym.

1.2. Fizyczny dostęp do pomieszczeń, w których eksploatowane są systemy informatyczne, blokują wzmocnione drzwi i systemy alarmowe. Po godzinach urzędowania dozór budynku prowadzony jest przez firmę ochroniarską „SZABEL" Sp. z o.o. Koszalin, ul. Morska 11, oddział Szczecinek ul. Mickiewicza 2 (tel. 94 346-83-73).

1.3. Dodatkowe kopie bezpieczeństwa dla danych zarchiwizowanych z linuksowego serwera SUSE w całodobowej kopii są synchronizowane z urządzeniem QNAP w odrębnej lokalizacji – chroniąc w ten sposób dane na wypadek pożaru, zalania, wyładowań atmosferycznych czy też katastrofy budowlanej.

1.4. W pomieszczeniach, w których zainstalowany jest serwer sieci i komputery zawierające bazy danych lub mające dostęp do danych zainstalowanych jest system alarmowy.

1.5. Zagadnienia związane z ochroną danych i obowiązki stąd wynikające ujęte są w zakresach czynności pracowników (według załączonego wzoru).

1.6. Każdy pracownik Urzędu podpisuje oświadczenie (według załączonego wzoru).

1.7. Za całość polityki bezpieczeństwa odpowiada Administrator Danych Osobowych.

2. Zabezpieczenie magnetycznych nośników:

2.1. Podstawowe kopie bezpieczeństwa na nośnikach przechowywane są w szafach metalowych lub w sejfie. Kopie przechowywane awaryjne są w pokoju Nr 12 (pomieszczenie kasy) w szafie metalowej (sejfie), do którego klucz posiada pracownik odpowiedzialny za obsługę kasy Urzędu Gminy oraz w pokoju Nr 2 w szafie metalowej, do którego klucze posiada pracownik odpowiedzialny za obsługę bazy danych ewidencji ludności PESEL.

Dodatkowe kopie danych z systemów FK i Programu Płatnika (na wypadek pożaru, katastrofy itp.) przechowywane są na urządzeniu QNAP informatyka urzędu – zgodnie z umową o zdalnej replikacji danych.

2.2. Dostęp do nośników zawierających kopie danych mają tylko uprawnione osoby.

3. Zabezpieczenie danych kartotek papierowych:

3.1. Kartoteki papierowe znajdują się w szafach zamykanych na klucz. Klucze od szaf przechowywane są w szafie metalowej w pokoju Nr 12 (kasa).

4. Zabezpieczenie danych i dostępu do danych:

4.1. Zabezpieczenia organizacyjne:

a) Dostęp do danych mają tylko pracownicy wyznaczeni przez Administratora Danych. Administrator Bezpieczeństwa Informacji prowadzi ścisły rejestr tych pracowników obejmujący listę nazwisk użytkowników posiadających dostęp do danych łącznie z ich identyfikatorami w systemie, startowymi hasłami.
b) W pokojach, do których mają dostęp petenci, monitory ustawione są w ten sposób, by petenci nie widzieli zapisów na ekranie.
c) Częstotliwość tworzenia kopii awaryjnych określa instrukcja. Za wykonanie kopii archiwalnych odpowiedzialne są osoby określone w Instrukcji.

4.2. Zabezpieczenie programowe:

Programowym zabezpieczeniem przed dostępem do danych osób nieupoważnionych w sieci komputerowej są:

- system użytkowników
- system haseł z wymuszeniem zmiany hasła co 4 tygodnie,
- system dostępów do katalogów i wolumenów dyskowych
- system ograniczeń czasowych przy dostępie do sieci komputerowej

Administrator bezpieczeństwa informacji ma uprawnienia do definiowania w/w zabezpieczeń. Do aplikacji można wejść tylko wtedy, gdy zna się odpowiednią nazwę użytkownika i jego hasło dla danej aplikacji a także, gdy na stanowisku roboczym zainstalowane jest oprogramowanie klienckie umożliwiające komunikację z serwerem (tzw. klient sieci).

4.3. Zabezpieczenia dostępu do wydruków:

Wydruki zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp do nich osób postronnych.

4.4. Zabezpieczenia sieciowe:

a) sprzętowe:

W sieci komputerowej wyodrębniono kilka wirtualnych grup roboczych VLAN odseparowanych od siebie na poziomie warstwy drugiej modelu OSI za pomocą zarządzalnych przełączników Cisco Catalyst. Poprzez odrębne domeny broadcastowe każda z grup roboczych w pełni wykorzystuje dostępne pasmo sieci komputerowej, dzięki czemu praca w sieci jest efektywna. Grupy robocze nie widzą się wzajemnie w otoczeniu sieciowym.

b) logiczne:

Każda z grup roboczych ma odrębną adresację klasy **C** z puli prywatnej **192.168.x.x**. Na potrzeby urzędu wyodrębnia się 2 grupy:

UG_Acc - grupa ze statycznie skonfigurowanymi adresami IP, w skład tej grupy wchodzą komputery mające dostęp do serwera Linux SUSE (pokoje 1, 9, 10, 11, kasa, kadry, sekretariat, p.26).

default - pozostałe komputery (konfiguracja automatyczna z serwera DHCP).

c) bezprzewodowe:

Dostęp do sieci bezprzewodowej WiFi w budynku urzędu gminy jest możliwy tylko i wyłącznie przy spełnieniu następujących zabezpieczeń:

- SSID sieci jest niewidoczne (nie rozgłaszane) i znane tylko administratorowi,
- szyfrowanie transmisji jest minimum 128-bitowe, typ: WPA2 + AES,
- filtracja mac-adresów - dopuszczane do sieci bezprzewodowej są tylko te urządzenia, które są własnością urzędu gminy i które uprzednio administrator sprawdził i skonfigurował,
- adres IP zostaje przydzielony z puli przypisanej do VLAN-a **default**.

d) organizacyjne

- pomieszczenia dzierżawione przez jednostki podległe w budynku urzędu nie mają dostępu do grup roboczych **UG_Acc** oraz **default**, posiadają one odrębne VLAN-y:

GZWiK - grupa robocza Gminnego Zakładu Wodociągów i Kanalizacji,

GOPS - grupa robocza Gminnego Ośrodka Pomocy Społecznej,

UG_Ewidencja - grupa robocza stworzona na potrzeby systemu ZMOKU (pasywna)

- gniazdo sieci logicznej RJ-45 dostępne na korytarzu dla informatora PIAP jest zabezpieczone przed możliwością podłączenia innego urządzenia niż ten PIAP (blokada portu).
- ZEAS i ODR - posiadają własne routery i odrębne sieci którymi nie zarządza administrator urzędu.

5. Ochrona prawidłowej pracy programów w razie awarii zasilania.

Serwer sieci oraz komputery stacjonarne, na których są przetwarzane lub zapisywane dane osobowe są wyposażone w urządzenia podtrzymujące zasilanie. Serwery zlokalizowane w serwerowni dodatkowo są wyposażone w system automatycznego wyłączenia się (i zamknięcia systemu operacyjnego) w przypadku przedłużającego się zaniku zasilania, tuż przed całkowitym rozładowaniem się akumulatorów w UPS-ach.

Dopuszczalnym wyjątkiem konieczności braku posiadania zasilaczy UPS są komputery przenośne (typu laptop) posiadające własne baterie/akumulatory.

6. Ochrona prawidłowej pracy systemu informatycznego w razie awarii komunikacji w sieci komputerowej.

Komunikacja z serwerem w sieci odbywa się przez sieć komputerową opartą na technologii FastEthernet 100 MB/s z wykorzystaniem dwóch 48-portowowych przełączników. Serwery oraz każdy komputer (host) mają indywidualną komunikację z przełącznikami. Przełączniki wraz z awaryjnym źródłem zasilania (w postaci rackowych zasilaczy UPS) znajdują się szafach dystrybucyjnych w pokoju nr 16 (I piętro) oraz w serwerowni (piwnica) i spięte są ze sobą łączem światłowodowym o przepustowości 1 GB/s. Przy przedłużającym się braku napięcia zasilającego i całkowitym rozładowaniu zasilaczy UPS - konfiguracja przełączników Catalyst i routera Cisco (model 2811) nie zostanie utracona gdyż znajduje się w nieulotnej pamięci NVRAM.

Zbiory z danymi osobowymi, są pobierane i składowane na serwerach linux SuSE oraz Windows 2003 Serwer (eDOK). Stare dane przechowywane są w celach archiwalnych na wyłączonym z eksploatacji serwerze sieci Novell, który w każdej chwili może być uruchomiony.

7. Monitorowanie zabezpieczeń

7.1. Do monitorowania systemu zabezpieczeń, stosowanie do swego zakresu czynności zobligowany jest Administrator Bezpieczeństwa Informacji.

7.2. W ramach monitoringu należy przeprowadzać następujące działania:

a) okresowe sprawdzanie kopii bezpieczeństwa pod względem ich przydatności do odtwarzania danych,

b) kontrola zbiorów danych na nośnikach magnetycznych,

c) sprawdzanie częstotliwości zmian haseł,

d) przeprowadzanie symulowanych włamań.

8. System szkoleń

8.1. Szkolenie podstawowe dotyczące bezpieczeństwa danych obejmuje wszystkich pracowników Urzędu Gminy.

8.2. System szkoleń szczegółowych, prowadzonych indywidualnie, obejmuje pracowników zatrudnionych bezpośrednio przy przetwarzaniu danych osobowych.

8.3. Tematyka szkoleń obejmuje:

a) przepisy i instrukcje wewnętrzne Urzędu Gminy Szczecinek dotyczące ochrony danych archiwizacji zasobów i przechowywania nośników niszczenia wydruków i zapisów na nośnikach magnetycznych,

b) zakresy obowiązków pracowników związanych bezpośrednio z bezpieczeństwem danych i ochroną systemów na poszczególnych stanowiskach.

9. Konserwacja i naprawy sprzętu i oprogramowania

9.1. Wszelkie naprawy i konserwacje sprzętu i oprogramowania mogą odbywać się tylko w obecności osób uprawnionych. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać do naprawy dopiero po uzyskaniu zgody Administratora Bezpieczeństwa Informacji.

10. Połączenia z siecią zewnętrzną (Internet):

10.1 Wykonywane są tylko za pośrednictwem list dostępów, zapór ogniowych (tzw. firewalli) i translacji NAT realizowanej na routerze. Jednocześnie zabrania się dokonywania jakichkolwiek innych przyłączeń sieci Urzędu do sieci Internet.

Załącznik Nr 2
do Zarządzenia Nr 68/2013
Wójta Gminy Szczecinek
z dnia 22 sierpnia 2013 r.

INSTRUKCJA

zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Szczecinek.

§ 1.1. Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych określa:

1) sposób przydziału haseł dla użytkowników i częstotliwości ich zmiany oraz osoby odpowiedzialne za te czynności,
2) sposób rejestrowania i wyrejestrowywania użytkowników oraz osoby odpowiedzialne za te czynności,
3) procedury rozpoczynania i kończenia pracy,
4) metodę i częstotliwość tworzenia kopii awaryjnych,
5) metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz metodę ich usuwania,
6) sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków,
7) sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych,
8) sposób postępowania w zakresie komunikacji w sieci komputerowej.

2. Ilekroć w instrukcji jest mowa o administratorze – rozumie się przez to Administratora Bezpieczeństwa Informacji.

§ 2.1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, zwanego dalej „systemem" może uzyskać wyłącznie osoba (użytkownik) zarejestrowana w tym systemie przez administratora.

2. Rejestracja, o której mowa w ust.1, polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu, na podstawie upoważnienia wydanego przez administratora danych.

§ 3.1. Identyfikator użytkownika powinien składać się ze znaków (liter), jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych.

2. W przypadku zbieżności nadanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika, administrator bezpieczeństwa informacji nadaje inny identyfikator.

§ 4.1. Hasło powinno składać się z unikalnego zestawu co najmniej sześciu znaków, literowych, cyfrowych lub innych.

2. Hasło nie może być identyczne z identyfikatorem użytkownika, ani z jego imieniem lub nazwiskiem.

3. Zmiana hasła następuje nie rzadziej, niż co 30 dni.

4. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom.

§ 5.1. Wyrejestowania użytkownika z systemu informatycznego dokonuje administrator.

2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.

3. Wyrejestrowanie następuje poprzez:

1) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
2) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego jest:

1) nieobecność w pracy trwająca dłużej niż 21 dni kalendarzowe,
2) zawieszenie w pełnieniu obowiązków służbowych,
3) zwolnienie z pełnienia obowiązków służbowych.

5. Przyczyna trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.

§ 6.1. Rozpoczęcie pracy w systemie odbywa się poprzez:

1) przygotowanie stanowiska pracy,
2) włączenie stacji roboczej,
3) wprowadzenie swojego identyfikatora i hasła.

§ 7.1. Zakończenie pracy w systemie odbywa się poprzez:

1) zamknięcie aplikacji,
2) odłączenie się od zasobów systemowych,
3) zamknięcie systemu operacyjnego i wyłączenie stacji roboczej.

§ 8.1. Zabrania się użytkownikom pracującym w systemie:

1) udostępniania stacji roboczej osobom nie zarejestrowanym w systemie w trybie określonym w §1 ust.2 ,
2) udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z administratorem,
3) używania nielicencjowanego oprogramowania.

§ 9.1. Każdy przypadek naruszenia ochrony danych osobowych, a w szczególności:

1) naruszenia bezpieczeństwa systemu informatycznego,
2) stwierdzenia objawów (stanu urządzeń, sposobu działania programu lub jakości komunikacji w sieci), które mogą wskazywać naruszenie bezpieczeństwa,

podlega zgłoszeniu do administratora bezpieczeństwa informacji.

2. Administratorowi należy zgłosić w szczególności przypadki:

1) użytkowania stacji roboczej przez osobę nie będącą użytkownikiem systemu,
2) usiłowania logowania się do systemu (sieci) przez osobę nieuprawnioną,
3) usuwania, dodawania lub modyfikowania bez wiedzy i zgody użytkownika jego dokumentów,
4) przebywania osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe, w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych i bez zgody administratora danych osobowych, pozostawiania bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe,
5) udostępniania osobom nieuprawnionym stacji roboczej lub komputera przenośnego,
6) nie zabezpieczenia hasłem dostępu do komputera służącego do przetwarzania danych osobowych,
7) przechowywania kopii awaryjnych w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowanych na bieżąco,
8) przechowywania nośników informacji oraz wydruków z danymi osobowymi, nie przeznaczonymi do udostępniania, w warunkach umożliwiających do nich dostęp osobom nieuprawnionym.

3. Obowiązek dokonania zgłoszenia, o którym mowa w ust. 1 i 2 spoczywa na każdym pracowniku, który powziął wiadomość o naruszeniu ochrony danych osobowych.

4. W przypadku naruszenia integralności bezpieczeństwa sieciowego, obowiązkiem administratora jest natychmiastowe wstrzymanie udostępniania zasobów dla użytkowników i odłączenie serwerów od sieci.

5. Administrator ustala przyczyny naruszenia integralności bezpieczeństwa sieciowego.

6. Przywrócenie udostępniania zasobów użytkownikom może nastąpić dopiero po ustaleniu i usunięciu przyczyny naruszenia integralności bezpieczeństwa sieciowego.

§ 10.1. Kopie awaryjne (zapasowe) dla Rejestru Wyborców i systemów PESEL tworzy się z częstotliwością nie rzadziej niż raz na miesiąc, kopie z systemów finansowo-księgowych wykonuje się z automatu w każdy dzień powszedni.

2. Każdą kopię tworzy się pod odrębną nazwą powiązaną z datą utworzenia kopii,

3. Zabrania się przechowywania kopii awaryjnych (zapasowych) w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.

4. Administrator przegląda okresowo kopie awaryjne i ocenia ich przydatność do odtworzenia zasobów systemu w przypadku jego awarii.

5. Stwierdzenie utraty przez kopie awaryjne waloru przydatności do celu, o którym mowa w ust. 4, upoważnia administratora do ich zniszczenia bądź trwałego wykasowania.

§ 11.1. Sprawdzanie obecności wirusów komputerowych w systemie oraz ich usuwanie odbywa się przy wykorzystaniu licencjonowanego oprogramowania w oparciu o serwer dystrybucji aktualnych sygnatur i wersji oprogramowania.

2. Oprogramowanie, o którym mowa w ust.1, sprawuje ciągły nadzór (jest rezydentne) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.

3. Administrator w uzasadnionych przypadkach przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach.

§ 12.1. System i urządzenia informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczna, zabezpiecza się przed utratą danych osobowych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

2. Minimalne zabezpieczenie systemu i urządzeń informatycznych, o których mowa w ust.1, polega na wyposażeniu serwera (serwerów) oraz stacji roboczych w zasilacze awaryjne (UPS) o mocy nie mniejszej niż 500 VA.

§ 13.1. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać:

1) do naprawy,
2) podmiotowi uprawnionemu do otrzymania tych danych,
3) do likwidacji, dopiero po uprzednim uzyskaniu zgody administratora danych osobowych.

2. Urządzenia, o których mowa w ust.1, przed ich przekazaniem pozbawia się zapisu danych osobowych.

3. Jeżeli nie jest to możliwe, urządzenie to może być naprawiane wyłącznie pod nadzorem osoby upoważnionej przez administratora.

4. Jeżeli nie jest możliwe pozbawienie urządzenia, przekazywanego do likwidacji, zapisu danych osobowych, urządzenie – przed przekazaniem – uszkadza się w sposób uniemożliwiający odczytanie tych danych.

§ 14. Przeglądu i konserwacji systemu dokonuje administrator doraźnie, nie rzadziej niż raz na miesiąc.

§ 15.1. Bezpieczeństwo komunikacji w obrębie systemów przetwarzających dane osobowe, administrator zapewnia przy użyciu narzędzi w obrębie systemu.

2. W systemach działających sieciowo, na zasadzie udostępnienia zasobów na serwerze, administrator powinien uwzględniać dedykowane przyzwolenia dostępu.

§ 16.1. Przesyłanie danych osobowych w komunikacji wewnętrznej musi być oznaczone w sposób dostępny jedynie dla uprawnionych użytkowników i wyznaczony przez administratora przy użyciu narzędzi zabezpieczeń w obrębie systemu informatycznego.

2. W sytuacji, gdy dostępne narzędzia informatyczne nie będą wystarczające do działania w komunikacji wewnętrznej, administrator wyznacza sposób postępowania, mając w szczególności na uwadze ochronę danych osobowych.

§ 17. Przesyłanie danych osobowych poprzez sieć INTERNET odbywa się po uprzednim skonfigurowaniu oprogramowania przez administratora.

§ 18. Nośniki informatyczne zawierające dane osobowe powinny być opisane w sposób czytelny i zrozumiały dla użytkownika, a zarazem nie powinny ułatwiać rozpoznania zawartości przez osoby nieupoważnione.

§ 19.1. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione.

2. W pomieszczeniach, gdzie nie jest możliwe ograniczenie dostępu osób postronnych, monitory stanowisk dostępu do danych osobowych ustawia się w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

3. Ekrany monitorów stanowisk dostępu do danych osobowych są zaopatrzone w wygaszacze z ustawioną opcją wymagania hasła, które po upływie maksymalnie 3 minut nieaktywności użytkownika automatycznie wyłączają funkcję eksploatacji ekranu.

§ 20. Osoby użytkujące przenośne nośniki informatyczne, służące do przetwarzania danych osobowych, obowiązane są niezwłocznie informować na piśmie administratora o zakresie, rodzaju zbieranych danych osobowych oraz celu ich przetwarzania. Administrator może żądać usunięcia danych, co do których zachodzi uzasadnione podejrzenie, że nie są przetwarzane zgodnie z zasadami określonymi w przepisach o ochronie danych osobowych.

§ 21. Osoba przenosząca dane osobowe, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania nośników danych poza obszarem ochrony danych w celu zapobieżenia dostępowi do tych danych osobie nieuprawnionej

§ 22.

1. Użytkownik sporządzający wydruki, które zawierają dane osobowe jest odpowiedzialny za zachowanie szczególnej ostrożności przy korzystaniu z nich, a zwłaszcza za zabezpieczenie ich przed dostępem osób nie posiadających imiennego upoważnienia oraz nieuprawnionych do wglądu na podstawie indywidualnego zakresu czynności.

2. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

Lista pracowników i ich funkcje w systemie zabezpieczeń i przy przetwarzaniu danych osobowych

Lp.	Imię i nazwisko	Funkcja (zakres czynności i odpowiedzialności)
1.	**Janusz Babiński** **Wójt Gminy**	Administrator Danych Osobowych;
2.	**Mariusz Ratajczak** **Informatyk**	Administrator Bezpieczeństwa Informacji; Dostęp do serwerowni z serwerami, szafami dystrybucyjnymi i urządzeniem archiwizującym QNAP;
3.	**Adam Gonczarów** **Sekretarz Gminy**	Dane osobowe pracowników i kierowników gminnych jednostek organizacyjnych;
4.	**Bogusława Chojecka** **Inspektor UG**	Przetwarzanie bazy ewidencji ludności PESEL i dowodów osobistych; Wykonywanie kopii awaryjnych dla w/w bazy; Zabezpieczenie kluczy do szafy (sejfu) z kopiami awaryjnymi i bezpieczeństwa w pok. nr 2; Wymiana podstawowej kopii bezpieczeństwa w sejfie;
5.	**Małgorzata Zieleńczuk** **Inspektor UG**	jak wyżej
6.	**Angelika Wojtasik** **Inspektor UG**	Wprowadzanie treści do systemu eDok (Elektronicznego Obiegu Dokumentów), redagowanie treści w BiP urzędu, przetwarzanie bazy podatników opłaty śmieciowej, odbiór korespondencji w systemie e-PUAP
7.	**Kamila Wróbel** **Podinspektor UG**	Wprowadzanie treści do systemu eDok (Elektronicznego Obiegu Dokumentów), odbiór i wysyłka korespondencji w systemie e-PUAP. Odbiór i wysyłka korespondencji papierowej składanej przez petentów
8.	**Agnieszka Bielecka** **Podinspektor UG**	Zabezpieczenie kluczy do szafy z kopiami awaryjnymi i bezpieczeństwa w pok. nr 12 (kasa UG);
9.	**Mirosława Perska** **Skarbnik**	Przetwarzanie danych zbioru płacowego i wykonywanie kopii awaryjnych;
10.	**Danuta Padewska** **Inspektor UG**	Przetwarzanie danych zbioru płacowego, Przetwarzanie danych programu Płatnika, Przetwarzanie bazy ewidencji podatków;
11.	**Danuta Prokopowicz** **Inspektor UG**	Przetwarzanie bazy ewidencji wniosków i decyzji dodatków mieszkaniowych oraz wykonywanie kopii zapasowych;
12.	**Izabela Malinowska** **Podinspektor UG**	Przetwarzanie bazy ewidencji podatników;
13.	**Katarzyna Gajdzis** **Podinspektor UG**	Przetwarzanie bazy ewidencji podatników;

14.	**Katarzyna Sochacka** **Podinspektor UG**	Dostęp do bazy ewidencji gruntów;
15.	**Monika Święs** **Podinspektor UG**	Dostęp do bazy ewidencji gruntów i wykonywanie kopii awaryjnych;
16.	**Henryka Plesowicz** **Inspektor UG**	Przetwarzanie bazy ewidencji podatników i wykonywanie kopii awaryjnych;
17.	**Mariola Jaworska** **Inspektor**	Przetwarzanie bazy ewidencji podatników;
18.	**Michał Żandarski** **Podinspektor UG**	Przetwarzanie bazy ewidencji podatników;
19.	**Jolanta Maczyszyn** **Inspektor UG**	Przetwarzanie rejestru decyzji o warunkach zabudowy i zagospodarowania terenu;
20.	**Anna Skałecka** **Inspektor UG**	Przetwarzanie rejestru skarg i wniosków oraz danych osobowych pracowników;
21.	**Andrzej Leoniak** **Inspektor UG**	Przetwarzanie listy poborowych, wykazu przedpoborowych i rejestru przedpoborowych; Przetwarzanie wykazu żołnierzy rezerwy reklamowanych na wniosek i z urzędu; Przetwarzanie wykazu członków formacji obrony cywilnej; Przetwarzanie wykazu wykonawców, łączników i kurierów Akcji Kurierskiej; Przetwarzanie wykazu świadczeń osobistych na rzecz obrony i obrony cywilnej;
22.	**Irena Gogusz** **Inspektor UG**	Przetwarzanie ewidencji osób prowadzących działalność gospodarczą;
23.	**Teresa Mazur** **Inspektor UG**	Przetwarzanie papierowego archiwum zakładowego;
24.	**Monika Chmiel** **Podinspektor UG**	Przetwarzanie rejestru zezwoleń na wycinkę drzew;

Dodatkowy zakres obowiązków dla pracowników Urzędu Gminy Szczecinek

1. Pracownik zobowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania danych, zgodnie z obowiązującą w Urzędzie polityką bezpieczeństwa, regulaminami i instrukcjami wewnętrznymi, w tym m.in.:
   - chronić dane przed dostępem osób nieupoważnionych;
   - chronić dane przed przypadkowym lub nieumyślnym zniszczeniem, utratą lub modyfikacją;
   - chronić nośniki magnetyczne i wydruki komputerowe;
   - utrzymywać w tajemnicy powierzone hasła, częstotliwość ich zmian oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w Urzędzie;
   - archiwizować dane zgodnie z instrukcją technologiczną;
   - prowadzić niezbędną przewidziana instrukcję technologiczną, dokumentację pracy z systemem, archiwizowania danych, itp.

2. Zabrania się pod rygorem odpowiedzialności służbowej i karnej:
   - ujawnić dane – w tym dane osobowe zawarte w obsługiwanych systemach,
   - kopiować bazy danych lub ich części poza przewidzianymi instrukcją technologiczną, kopiami bezpieczeństwa,
   - przesyłać dane osobowe drogą elektroniczną,
   - przetwarzania danych w sposób inny niż opisany instrukcją technologiczną,

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

(Imię i Nazwisko Pracownika)

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

(Wójt Gminy Szczecinek)

Szczecinek dnia _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Urząd Gminy Szczecinek

ul. Pilska 3, 78-400 Szczecinek
woj. zachodniopomorskie
www.gminaszczecinek.pl

tel. (94) 37 432-48, -73, -85, -94
fax.(94) 37 420-08
e-mail: sekretariat@gminaszczecinek.pl

Szczecinek, 22.08.2012r.

OŚWIADCZENIE

(tekst oświadczenia podpisywanego przez pracowników
Urzędu Gminy Szczecinek oraz pracowników obsługi)

Ja niżej podpisany(a) ..... zobowiązuję się do zachowania tajemnicy danych osobowych, do których mam/będę miał dostęp w związku z wykonywaniem przeze mnie zadań służbowych i obowiązków pracowniczych w **Urzędzie Gminy Szczecinek**, zarówno **w trakcie obecnie wiążącego mnie stosunku pracy, stażu jak i po ustaniu zatrudnienia**.

Zobowiązuję się przestrzegać regulaminów, instrukcji i procedur obowiązujących w **Urzędzie Gminy Szczecinek** wiążących się z ochroną danych osobowych, a w szczególności nie będę bez upoważnienia służbowego wykorzystywał(a) danych osobowych ze zbiorów w **Urzędzie Gminy Szczecinek**.

Stwierdzam, że zostałem(am) przeszkolony(a) i zrozumiałem(am) treść definicji danych osobowych w rozumieniu art. 6 ustawy z dnia 29.08.1997r, o ochronie danych osobowych (tekst jednolity Dz. U z roku 2002 nr 101, poz. 926 z późn. zm.) oraz **aktów wykonawczych i instrukcji polityki bezpieczeństwa w Urzędzie Gminy Szczecinek**.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za naruszenie obowiązków pracowniczych w rozumieniu Kodeksu Pracy.

.....
podpis składającego oświadczenie

.....
przyjmujący oświadczenie

Wójt Gminy Szczecinek

ul. Pilska 3, 78-400 Szczecinek
woj. zachodniopomorskie
www.gminaszczecinek.pl

tel. (94) 37 432-48, -73, -85, -94
fax.(94) 37 420-08
e-mail: sekretariat@gminaszczecinek.pl

Szczecinek, 22.08.2013r.

UPOWAŻNIENIE

Działając na podstawie uprawnień nadanych mi w **Urzędzie Gminy** w sprawie ochrony danych osobowych oraz w oparciu o art. 37 ustawy o Ochronie Danych Osobowych (Dziennik Ustaw z 2002 r. Nr 101, poz. 926 z późn. zm.) upoważniam:

Pana / Panią .....

do przetwarzania danych/obsługi (niepotrzebne wykreślić):

- ☐ systemu informatycznego Gmina v.2 oraz urządzeń wchodzących w jego skład zlokalizowanych w Urzędzie Gminy Szczecinek służących do przetwarzania danych osobowych
- ☐ zawartych w bazie podatników systemu Gmina v.2
- ☐ zawartych w systemie elektronicznego obiegu dokumentów e-DOK
- ☐ systemu Płatnik służącego do sporządzania i wysyłki deklaracji dla ZUSu
- ☐ systemu GOMiG – dotyczącego opłaty za gospodarowanie odpadami,

na okres od 23.08.2013r do ustania z dniem 22.08.2014r

- ☐ identyfikator w e-Dok: .....

Wyżej wymieniona osoba została zapoznana z obecnie obowiązującymi przepisami dotyczącymi ochrony danych osobowych i dopuszczona jest do ich przetwarzania jedynie w zakresie określonym w Ustawie z dnia 29.08.1997r, o ochronie danych osobowych (tekst jednolity Dz. U. z roku 2002 nr 101, poz. 926) i wydanych do niej przepisach wykonawczych oraz w Zarządzeniu nr 68/2013 z dnia 22.08.2013r Wójta Gminy Szczecinek w sprawie określenia polityki bezpieczeństwa [...].

Wymieniona osoba została wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w **Urzędzie Gminy Szczecinek**.

Szczecinek, 23.08.2013r.
data

.....
Administrator Danych Osobowych