WÓJT GMINY
Z A K R Z E W O
woj. kujawsko-pomorskie

ZARZĄDZENIE NR 75/2015
WÓJTA GMINY ZAKRZEWO
z dnia 12 listopada 2015 r.

w sprawie wdrożenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych

Na podstawie art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 z późn. zm.),

Wójt Gminy Zakrzewo
zarządza, co następuje:

Dział I
Polityka bezpieczeństwa

Rozdział 1
Założenia ogólne

§ 1. Polityka Bezpieczeństwa Urzędu Gminy w Zakrzewie zwana dalej „Polityką Bezpieczeństwa" określa wytyczne i kierunki działań, które podejmuje się w celu zapewniania bezpieczeństwa przetwarzanych danych osobowych oraz zapewnia wsparcie kierownictwa dla działań na rzecz bezpieczeństwa tych danych.

§ 2. Podstawę prawną Polityki Bezpieczeństwa stanowią:
1) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 z późn. zm.) i akty wykonawcze wydane na jej podstawie, w szczególności rozporządzenie 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. z 2004 r. Nr 100, poz. 1024);
2) Polskie Normy odnoszące się bezpieczeństwa informacji, w szczególności PN-ISO/IEC 27001, PN-ISO/IEC 27005;
3) umowy, których stroną jest Urząd Gminy w Zakrzewie lub Gmina Zakrzewo.

§ 3. Przetwarzając dane osobowe dokłada się szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia się, że dane:
1) przetwarza się zgodnie z prawem;
2) zbiera się dla oznaczonych, zgodnych z prawem celów i nie poddaje się dalszemu przetwarzaniu niezgodnemu z tymi celami;
3) są merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
4) przechowuje się w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

§ 4. Dane osobowe przetwarza się w celu realizacji zadań wynikających z aktów prawnych, w szczególności z:
1) ustawy z dnia 8 marca 1990 r. o samorządzie terytorialnym (Dz. U. z 2015 r., poz. 1515);
2) ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2014 r., poz. 1502 z późn. zm.).

2. Dane osobowe przetwarza się zarówno w tradycyjnej formie papierowej oraz w systemach informatycznych służących do przetwarzania tych danych.

§ 5. Politykę Bezpieczeństwa stosuje się do przetwarzania i zabezpieczania danych osobowych, na każdym etapie i w każdym obszarze, w szczególności w obszarze:

1) organizacji bezpieczeństwa danych;
2) bezpieczeństwa zasobów ludzkich;
3) zarządzania aktywami;
4) kontroli dostępu;
5) kryptografii;
6) bezpieczeństwa fizycznego i środowiskowego;
7) bezpieczeństwa eksploatacji;
8) bezpieczeństwa komunikacji;
9) pozyskiwania, rozwoju i utrzymania systemów informatycznych służących do przetwarzania danych osobowych;
10) relacji z innymi podmiotami i kontrahentami;
11) zarządzania incydentami bezpieczeństwa danych osobowych;
12) bezpieczeństwa danych osobowych w zarządzaniu ciągłością działania;
13) zgodności z przepisami prawnymi, umowami i innymi zasadami.

§ 6. Administratorem danych osobowych przetwarzanych przez Urząd Gminy w Zakrzewie jest Wójt Gminy.

§ 7. Przestrzeganie przepisów o ochronie danych osobowych przez osoby przetwarzające dane osobowe zapewnia administrator bezpieczeństwa informacji.

2. Zakres odpowiedzialności i uprawnienia administratora bezpieczeństwa informacji określa ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 z późn. zm.) oraz akty wykonawcze wydane na jej podstawie.

§ 8. Założenia Polityki Bezpieczeństwa znajdują konkretyzację w aktach prawa wewnętrznego Wójta Gminy.

§ 9. Ilekroć w Polityce Bezpieczeństwa jest mowa o:

1) ustawie, rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 z późn. zm.);
2) rozporządzeniu, rozumie się przez to rozporządzenie 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. z 2004 r., Nr 100, poz. 1024);

Rozdział 2
Cele

§ 10. 1. Celem strategicznym jest zapewnienie bezpieczeństwa danych osobowych, przez co rozumie się zachowanie poufności, integralności, rozliczalności i dostępności tych danych oraz zapewnienie przetwarzania danych zgodnego z przepisami o ochronie danych.

2. Cele w zakresie zapewnienia poufności, integralności i rozliczalności danych osobowych:

1) zabezpieczenie systemów informatycznych służących do przetwarzania danych osobowych przed zagrożeniam pochodzącymi z sieci publicznej, w szczególności nieuprawnionym dostępem;

2) zabezpieczenie urządzeń służących do przetwarzania danych osobowych przed działalnością szkodliwego oprogramowania;
3) zapewnienie kontroli przepływu informacji pomiędzy systemem informatycznym służącym do przetwarzania danych osobowych, a siecią publiczną oraz kontroli działań inicjowanych z sieci publicznej i tego systemu;
4) zabezpieczenie danych wykorzystywanych do uwierzytelniania użytkowników w systemach informatycznych służących do przetwarzania danych osobowych przed ujawnieniem osobie nieuprawnionej;
5) zabezpieczenie urządzeń przenośnych służących do przetwarzania danych osobowych i elektronicznych nośników tych danych, zawierających dane osobowe, w szczególności dane, o których mowa w art. 27 ust. 1 ustawy używanych poza obszarem, o którym mowa w § 4 pkt 1 rozporządzenia lub przekazywanych poza ten obszar przed nieuprawnionym dostępem, modyfikacją, usunięciem, zniszczeniem lub utratą;
6) zabezpieczenie urządzeń służących do przetwarzania danych osobowych i elektronicznych nośników tych danych zawierających dane osobowe, przeznaczonych do likwidacji, przekazania osobie lub podmiotowi nieuprawnionemu do przetwarzania danych oraz naprawy, przed dostępem osoby nieuprawnionej;
7) zabezpieczenie obszaru, o którym mowa w § 4 pkt 1 rozporządzenia przed dostępem osób nieuprawnionych na czas nieobecności w nim osoby dopuszczonej do przetwarzania danych osobowych;
8) zapewnienie rozliczalności przetwarzania danych osobowych przetwarzanych w systemach informatycznych służących do przetwarzania tych danych, odrębnie dla każdego użytkownika tych systemów;
9) zapewnienie zrozumienia obowiązków i odpowiedzialności za przetwarzanie i zabezpieczenie danych osobowych przez osoby dopuszczone do przetwarzania tych danych;
10) zabezpieczenie interesów Urzędu Gminy w Zakrzewie w razie zmiany lub zakończenia zatrudnienia osób dopuszczonych do przetwarzania danych osobowych;
11) zidentyfikowanie danych osobowych, zbiorów tych danych, a także urządzeń oraz programów służących do przetwarzania tych danych i zdefiniowanie właściwej odpowiedzialności za ich ochronę;
12) ograniczenie dostępu do danych osobowych i urządzeń służących do przetwarzania tych danych;
13) zapewnienie dostępu do danych osobowych i urządzeń służących do przetwarzania tych danych wyłącznie osobom uprawnionym;
14) zapobieżenie dostępu do danych osobowych oraz urządzeń i programów służących do ich przetwarzania przez osoby nieuprawnione;
15) wdrożenie oraz zapewnienie właściwego wykorzystania kryptograficznych środków zabezpieczenia danych osobowych;
16) rejestrowanie zdarzeń w systemach informatycznych służących do przetwarzania danych;
17) zapewnienie integralności systemów informatycznych służących do przetwarzania danych osobowych;
18) zarządzanie podatnościami technicznymi systemów informatycznych służących do przetwarzania danych osobowych;
19) zabezpieczenie dostępu do sieci komputerowych i sieci telekomunikacyjnych, w których przesyła się dane osobowe;
20) zabezpieczenie danych osobowych testowych;
21) zapewnienie bezpieczeństwa danych osobowych przekazywanych innym podmiot lub osobom;

22) wdrożenie poziomu bezpieczeństwa danych osobowych, których przetwarzanie powierzono Urzędowi Gminy w Zakrzewie;
23) zarządzanie incydentami bezpieczeństwa danych osobowych, w tym zgłaszaniem niezgodności;
24) zarządzanie bezpieczeństwem danych osobowych w ramach zarządzania ciągłością działania.

3 . Cele w zakresie zapewnienia dostępności danych osobowych:
1) zapewnienie prawidłowego działania systemów informatycznych służących do przetwarzania danych osobowych;
2) zapewnienie ciągłości działania urządzeń służących do przetwarzania danych osobowych w razie awarii zasilania lub zakłóceń w sieci zasilającej;
3) zapobieżenie uszkodzeniu lub utracie urządzeń służących do przetwarzania danych osobowych;
4) zapewnienie dostępności danych osobowych w razie ich uszkodzenia lub utraty;
5) zapewnienie dostępności urządzeń i programów służących do przetwarzania danych osobowych;
6) zminimalizowanie wpływu sprawdzeń, o których mowa w § 3 ust. 2 rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015 r., poz. 745).

Rozdział 3
Zagrożenia bezpieczeństwa danych osobowych

§ 11. Główne umyślne zagrożenia bezpieczeństwa danych osobowych:
1) przechwycenie danych osobowych na skutek zjawiska interferencji;
2) zdalne szpiegostwo przemysłowe;
3) podsłuch przez osobę nieuprawnioną;
4) zabranie nośników zawierających dane osobowe, w tym cyfrowych nośników tych danych przez osobę nieuprawnioną;
5) zabranie urządzeń służących do przetwarzania danych osobowych, zawierających te dane przez osobę nieuprawnioną;
6) odtworzenie danych osobowych z nośników danych, w szczególności elektronicznych nośników danych przeznaczonych do przekazania lub usunięcia uprzednio nie wymazanych;
7) ujawnienie danych osobowych;
8) zbieranie danych osobowych z niewiarygodnych źródeł, w szczególności od osoby, której dane nie dotyczą, nieważnych dokumentów oraz danych przekazywanych ustnie;
9) nieuprawniony dostęp do systemów informatycznych służących do przetwarzania danych osobowych;
10) wdrażanie niezweryfikowanych programów komputerowych, niezatwierdzonych przez administratora systemów informatycznych;
11) zniszczenie urządzeń i nośników zawierających dane osobowe;
12) używanie urządzeń i programów służących do przetwarzania danych osobowych niezgodne z przeznaczeniem, zasadami lub instrukcją producenta;
13) nieuprawnione powielanie danych osobowych;
14) użycie oprogramowania podszywającego się pod oprogramowanie wdrożone przez administratora danych do przetwarzania danych osobowych;
15) zniekształcenie danych osobowych;

16) przetwarzanie danych z naruszeniem przepisów o ochronie danych osobowych;
17) przetwarzanie danych osobowych w systemach informatycznych przy użyciu tożsamości innej osoby;
18) nieuprawnione działania użytkownika w systemie informatycznym służącym do przetwarzania danych osobowych;
19) zaniechanie obowiązków zabezpieczenia danych osobowych, w szczególności danych przetwarzanych w systemach informatycznych.

§ 12. Główne nieumyślne lub niezależne od człowieka zagrożenia bezpieczeństwa danych osobowych:
1) pożar;
2) zalanie;
3) zanieczyszczenie;
4) nieumyślne zniszczenie urządzeń i nośników zawierających dane osobowe;
5) awaria systemu chłodzenia urządzeń służących do przetwarzania danych osobowych, w szczególności awaria systemu zapewniającego właściwą temperaturę, nasłonecznienie i wilgotność pomieszczenia, w którym zlokalizowano serwer;
6) utrata zasilania w sieci zasilającej;
7) awarie urządzeń i programów służących do przetwarzania danych osobowych, w szczególności urządzeń telekomunikacyjnych;
8) promieniowanie elektromagnetyczne;
9) promieniowanie cieplne;
10) impuls elektromagnetyczny;
11) nieumyślne ujawnienie danych osobowych;
12) niewłaściwe działanie urządzeń i programów służących do przetwarzania danych osobowych;
13) nieumyślne przeciążenie systemu informatycznego służącego do przetwarzania danych osobowych spowodowane wyczerpaniem wolnych zasobów.

§ 13. Główne źródła zagrożeń bezpieczeństwa danych osobowych:
1) osoby dopuszczone do przetwarzania danych osobowych;
2) haker, cracker;
3) przestępca komputerowy;
4) szpieg przemysłowy;
5) terrostysta.

Rozdział 4
Kierunki działań

§ 14. 1. Cele określone w rozdziale realizuje się poprzez wdrożenie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych przed zagrożeniami określonymi w rozdziale trzecim, odpowiednich do zagrożeń i kategorii danych objętych ochroną.

2. Wyboru środków zapewniających ochronę przetwarzanych danych dokonuje się na podstawie analizy ryzyka.

3. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych określono w załączniku nr 1 do zarządzenia.

§ 15. Kierunki działania w celu zapewnienia poufności, integralności i rozliczalności:

1) ustanowienie struktury zarządzania bezpieczeństwem danych osobowych określającej odpowiedzialność za bezpieczeństwo tych danych;
2) rozdzielenie obowiązków i odpowiedzialności za bezpieczeństwo danych osobowych pozostających ze sobą w konflikcie;
3) uwzględnianie bezpieczeństwa danych osobowych w zarządzaniu projektami, niezależnie od ich rodzaju;
4) wdrożenie fizycznej zapory ogniowej zabezpieczającej systemy informatyczne służące do przetwarzania danych osobowych przed programami, których celem jest uzyskanie nieuprawnionego dostępu;
5) weryfikowanie przebiegu dotychczasowego zatrudnienia osób ubiegających się o zatrudnienie w kontekście ochrony danych osobowych zgodnie z właściwymi przepisami prawnymi, w tym z przepisami dotyczącymi weryfikowania wymierzonych kar;
6) uwzględnianie w umowach z osobami ubiegającymi się o zatrudnienie na stanowiska, na których niezbędne będzie przetwarzania danych osobowych, odpowiedzialności za przetwarzanie i zabezpieczanie tych danych;
7) zapoznanie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
8) wyciąganie konsekwencji wobec osób dopuszczających się naruszenia przepisów o ochronie danych osobowych, zasad Polityki Bezpieczeństwa i innych zasad przetwarzania i zabezpieczania tych danych, w tym w drodze postępowania dyscyplinarnego;
9) zidentyfikowanie danych osobowych, zbiorów danych osobowych oraz urządzeń i programów służących do ich przetwarzania, a także prowadzenie ewidencji tych zbiorów, urządzeń i programów; prowadzi się wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opis struktury zbiorów danych oraz opis sposobu przepływu danych pomiędzy systemami stanowiący załącznik nr 2 do zarządzenia;
10) przypisanie zbiorom danych osobowych, urządzeniom i programom służącym do przetwarzania danych osobowych osoby odpowiedzialnej za ich przechowywanie;
11) wdrożenie procedur przetwarzania danych osobowych;
12) zarządzanie urządzeniami przenośnymi i cyfrowymi nośnikami zawierającymi dane osobowe;
13) kontrola dostępu do danych oraz systemów informatycznych służących do ich przetwarzania;
14) zapewnienie osobom dopuszczonym do przetwarzania danych osobowych dostępu wyłącznie do sieci i usług sieciowych, do których są uprawnieni;
15) przydzielanie dostępu do danych osobowych użytkownikom systemów informatycznych służących do przetwarzania tych danych;
16) nadzór nad przydzielaniem i wykorzystywaniem prawa uprzywilejowanego dostępu do danych osobowych przetwarzanych w systemie informatycznym służącym do ich przetwarzania;
17) zarządzanie danymi służącymi do uwierzytelniania użytkownika w systemie informatycznym służącym do przetwarzania danych osobowych;
18) odbieranie praw dostępu;
19) ograniczenie dostępu do danych osobowych przetwarzanych w systemach informatycznych służących do ich przetwarzania;
20) bezpieczne logowanie do programów służących do przetwarzania danych osobowych oraz bezpiecznego wylogowania z tych programów;
21) zarządzanie hasłami;

22) nadzorowanie wykorzystania narzędzi programowych umożliwiających dostęp do danych osobowych przetwarzanych w systemach informatycznych służących do ich przetwarzania z pominięciem zabezpieczeń tych systemów;
23) ograniczenie i nadzorowanie dostępu do kodów źródłowych systemów informatycznych służących do przetwarzania danych osobowych;
24) stosowanie kryptograficznej ochrony danych osobowych;
25) zarządzanie kluczami kryptograficznymi;
26) fizyczne zabezpieczenie obszaru, o którym mowa w § 4 ust. 1 rozporządzenia, w szczególności pomieszczenia, w których znajduje się serwer, na którym przetwarza się dane osobowe oraz pomieszczenia, w którym przechowuje się kopie zapasowe zbiorów danych i programów służących do ich przetwarzania; prowadzi się wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarza się dane osobowe stanowiący załącznik nr 3 do zarządzenia.
27) lokalizowanie urządzeń służących do przetwarzania danych osobowych w sposób minimalizujący ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych;
28) wdrożenie urządzeń zapewniających nieprzerwane działanie systemów informatycznych służących do przetwarzania danych osobowych w razie awarii lub zakłóceń zasilania sieci zasilającej;
29) konserwacja urządzeń i programów służących do przetwarzania danych osobowych, zgodnie z zaleceniami producenta;
30) polityka czystego biurka i czystego ekranu;
31) wdrożenie procedur eksploatacyjnych systemów informatycznych służących do przetwarzania danych osobowych;
32) nadzorowanie zmian w systemach służących do przetwarzania danych osobowych;
33) monitorowanie wykorzystania zasobów serwerowych systemów informatycznych służących do przetwarzania danych osobowych;
34) wdrożenie zabezpieczeń wykrywających, zapobiegających i odtwarzających, służących do ochrony systemów informatycznych przed szkodliwym oprogramowaniem;
35) wykonywanie i testowanie kopii zapasowych zbiorów danych osobowych i programów służących do przetwarzania danych osobowych;
36) rejestrowanie zdarzeń systemów informatycznych służących do przetwarzania danych osobowych;
37) nadzorowanie instalacji oprogramowania w urządzeniach służących do przetwarzania danych osobowych;
38) wymiana informacji o podatnościach technicznych systemów informatycznych służących do przetwarzania danych osobowych;
39) zarządzanie bezpieczeństwem sieci teleinformatycznych;
40) stosowanie kryptograficznych środków ochrony wobec danych osobowych przesyłanych w sieci Urzędu Gminy w Zakrzewie oraz przekazywanych innym podmiotom w sieci publicznej.

Dział II
Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Rozdział 1

Procedury nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

§ 16. Konto użytkownika w systemie informatycznym tworzy administrator tego systemu na podstawie upoważnienia do przetwarzania danych osobowych, nadanego przez administratora danych.

§ 17. 1. Dla każdego użytkownika systemu nadaje się odrębny identyfikator i hasło.

2. Identyfikator nie podlega modyfikacjom.

3. Identyfikatora użytkownika, który utracił uprawnienia w systemie informatycznym nie przydziela się innemu użytkownikowi.

§ 18. Administrator systemu informatycznego nadaje użytkownikowi uprawnienia w systemie informatycznym w zakresie określonym w ewidencji osób upoważnionych do przetwarzania danych osobowych stanowiącej załącznik nr 4.

§ 19. 1. Uprawnienia użytkownika w systemie informatycznym modyfikuje lub odbiera administrator tego systemu na żądanie administratora bezpieczeństwa informacji lub administratora danych.

2. Administrator systemu informatycznego odbiera uprawnienia niezwłocznie po powzięciu wiadomości o zakończeniu zatrudnienia przez osobę, której konto dotyczy.

Rozdział 2

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

§ 20. Do uwierzytelnienia użytkownika w systemach informatycznych służących do przetwarzania danych osobowych stosuje się hasło.

§ 21. 1. Hasło do pierwszego uwierzytelnienia użytkownika w systemie informatycznym nadaje administrator tego systemu.

2. Administrator systemu informatycznego przekazuje hasło, o którym mowa w ust. 1 w sposób zapewniający zachowanie poufności tego hasła, osobiście lub drogą elektroniczną, w szczególności na adres poczty elektronicznej osoby, której hasło dotyczy.

3. Wobec hasła przekazywanego drogą elektroniczną stosuje się środki ochrony kryptograficznej.

4. Niezwłocznie po otrzymaniu hasła użytkownik loguje się do systemu i zmienia hasło, chyba że system nie posiada takiej funkcjonalności.

5. Użytkownik zachowuje hasło w tajemnicy.

§ 22. 1. Hasło służące do uwierzytelniania użytkownika w systemie informatycznym składa się z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

2. Hasło nie może zawierać wyrazów w sensie logicznym oraz cyfr składających się na ciąg znaków przypisanych użytkownikowi, w szczególności numeru ewidencyjnego PESEL, daty urodzenia.

§ 23. 1. Zmiana hasła służącego do uwierzytelniania użytkownika w systemie informatycznym następuje nie rzadziej niż co 30 dni.

2. Jeżeli system informatyczny nie wymusza zmiany hasła w terminie, o którym mowa w ust. 1, hasło zmienia użytkownik lub administrator tego systemu, jeżeli system tego wymaga.

3. Jeżeli hasło zmienia administrator systemu, hasło przekazuje się z zachowaniem § 21.

§ 24. Hasła stosowane do uwierzytelniania użytkowników w systemie informatycznym przechowuje się w postaci zaszyfrowanej.

§ 25. 1. Hasła administratorów systemów informatycznych stosowane do uwierzytelnienia ich w systemach informatycznych przechowuje administrator danych.

2. Administrator systemu informatycznego przekazuje kopertę zawierającą aktualne hasło służące do uwierzytelnienia go w systemie, niezwłocznie po każdej jego zmianie.

3. Nieaktualne hasło niszczy się w sposób uniemożliwiający jego odczyt.

§ 26. 1. Hasło służące do uwierzytelnienia administratora w systemie informatycznym używa się wyłącznie za zgodą administratora danych.

2. Z użycia hasła administratora systemu sporządza się notatkę, określającą w szczególności:
1) imię i nazwisko osoby, która użyła hasła;
2) data i godzina użycia hasła;
3) cel użycia hasła.

3. Administrator systemu informatycznego zmienia hasło służące do uwierzytelnienia go w systemie po każdym jego użyciu przez inną osobę.

Rozdział 3
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

§ 27. 1. Rozpoczęcie pracy w systemie informatycznym służącym do przetwarzania danych osobowych, użytkownik poprzedza oględzinami urządzeń składających się na ten system.
2. W trakcie oględzin użytkownik zwraca szczególną uwagę na:
1) ewentualne ślady ingerencji w obudowę urządzeń;
2) urządzenia peryferyjne podłączone do urządzeń;
3) urządzenia bezprzewodowe znajdujące się w miejscu pracy;
4) kable służące do transmisji danych.
3. W razie choćby podejrzenia nieuprawnionej ingerencji w system informatyczny użytkownik niezwłocznie zawiadamia administratora systemu informatycznego i zaprzestaje dalszych czynności, do czasu uzyskania zgody administratora systemu na dalszą pracę w systemie.

§ 28. Po uruchomieniu systemu służącego do przetwarzania danych osobowych, użytkownik sprawdza ten system na obecność oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu za pomocą narzędzi programowych zainstalowanych w tym celu.

§ 29. 1. Rozpoczęcie pracy w programie służącym do przetwarzania danych osobowych, użytkownik rozpoczyna od wprowadzenia nadanego mu identyfikatora i uwierzytelnienia tożsamości.

2. Wprowadzając identyfikator i hasło służące do uwierzytelnienia, użytkownik dochowuje szczególnej staranności w celu zachowania poufności tych danych.

3. Po zalogowaniu się do systemu użytkownik sprawdza datę i godzinę ostatniego logowania i próby logowania.

4. Jeżeli data i godzina ostatniego logowania, ostatniej próby logowania jest inna, niż ostatnia data i godzina logowania lub próby logowania się przez użytkownika, użytkownik niezwłocznie zawiadamia o tym administratora systemu informatycznego i zaprzestaje dalszej pracy w systemie, do czasu decyzji administratora systemu o możliwości wznowienia pracy w tym systemie.

§ 30. Zawieszenie pracy w systemie informatycznym służącym do przetwarzania danych osobowych polega na krótkotrwałej bezczynności w systemie, spowodowanej w szczególności opuszczeniem miejsca pracy.

2. Użytkownik systemu na czas bezczynności stosuje wygaszacz ekranu.

3. Wznowienie pracy następuje po przeprowadzeniu czynności określonych w § 29.

§ 31. 1. Zakończenie pracy w programie służącym do przetwarzania danych osobowych następuje poprzez wylogowanie się z tego programu.

2. Jeżeli użytkownik nie przewiduje dalszej pracy w systemie informatycznym wyłącza ten system.

Rozdział 4
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

§ 32. 1. Kopie zapasowe zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania tworzy administrator tego systemu.

2. Tworzy się kopię przyrostową oraz kopię całkowitą.

§ 33. 1. Kopie tworzy się na cyfrowym nośniku danych, odrębnym dla każdego systemu informatycznego zgodnie z harmonogramem określonym w załączniku nr 5 do zarządzenia.

2. Wobec danych osobowych znajdujących się na elektronicznym nośniku stosuje się kryptograficzne metody ochrony tych danych.

Rozdział 5
Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe, a także kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

§ 34. 1. Elektroniczne nośniki informacji zawierające dane osobowe, w tym nośniki zawierające kopie zapasowe, o których mowa w § 32 przechowuje administrator systemów informatycznych w sposób zapewniający zachowanie poufności i integralności tych danych.

2. Nośniki, o których mowa w ust. 1, administrator systemów informatycznych chroni przed dostępem, skopiowaniem, zabraniem przez osobę nieuprawnioną oraz przed zniszczeniem, w szczególności poprzez:
1) przechowywanie tych nośników w metalowej zabezpieczonej zamkiem szafie;
2) stosowanie wobec tych nośników kryptograficznej ochrony.

§ 35. 1. Dane osobowe znajdujące się na elektronicznych nośnikach przechowuje się nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania tych danych z zastrzeżeniem ust. 2.

2. Kopie zapasowe przyrostowe, o których mowa w § 32, przechowuje się do czasu utworzenia kopii całkowitej. Kopię zapasową całkowitą przechowuje się do czasu utworzenia kolejnej kopii całkowitej.

3. Administrator systemów informatycznych usuwa dane osobowe znajdujące się na elektronicznych nośnikach danych, niezwłocznie po ustaniu niezbędności przechowywania tych danych.

§ 36. 1. Elektroniczne nośniki informacji wykorzystuje się nie dłużej niż do czasu ich przydatności, określonego przez producenta lub dostawcę tych nośników.

2. Administrator systemów informatycznych, elektroniczne nośniki informacji, zawierające dane osobowe przeznaczone do:
1) likwidacji - pozbawia się uprzednio zapisu tych danych, a jeżeli nie jest to możliwe, uszkadza się te nośniki w sposób uniemożliwiający ich odczytanie;
2) naprawy - pozbawia się uprzednio zapisu tych danych w sposób uniemożliwiający ich odzyskanie lub naprawia się je pod osobistym nadzorem osoby upoważnionej przez administratora danych.

Rozdział 6
Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

§ 37. Na działalność oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, narażone są w szczególności:
1) serwer;
2) stacje robocze;
3) urządzenia przenośne;
4) elektroniczne nośniki danych.

§ 38. System informatyczny chroni się przed działalnością oprogramowania, o którym mowa w § 37 poprzez stosowanie fizycznej zapory ogniowej oraz oprogramowania antywirusowego.

§ 39. Administrator systemów informatycznych konfiguruje zabezpieczenia, o których mowa w § 38 w szczególności sposób:
1) zapewniający maksymalny poziom ochrony przed oprogramowaniem, o którym mowa w § 37;
2) uniemożliwiający użytkownikowi zmianę konfiguracji oraz choćby krótkotrwałe ich wyłączenie;
3) zapewniający sprawdzanie systemu przy każdym jego włączeniu oraz sprawdzanie elektronicznych nośników danych przy każdym jego użyciu;
4) zapewniający automatyczną aktualizację programu.

§ 40. Użytkownik systemu informatycznego, którego oprogramowanie wykryje oprogramowanie, o którym mowa w § 37, niezwłocznie zawiadamia administratora systemów informatycznych i zaprzestaje dalszej pracy w systemie, do czasu uzyskania zgody administratora na wznowienie pracy.

Rozdział 7

Sposób odnotowania informacji o odbiorcach, którym dane udostępniono.

§ 41. 1. Odnotowanie informacji o odbiorcach w zakresie określonym w § 7 ust. 1 pkt 4 rozporządzenia, którym dane osobowe udostępniono zapewnia każdy system informatyczny służący do przetwarzania tych danych.

2. Użytkownik systemu informatycznego, z którego udostępniono dane osobowe, odnotowuje niezwłocznie to udostępnienie.

Rozdział 8

Procedury wykonywania przeglądów i konserwacji systemów informatycznych oraz elektronicznych nośników informacji służących do przetwarzania danych osobowych.

§ 42. Przeglądy i konserwacje systemów informatycznych oraz elektronicznych nośników informacji służących do przetwarzania danych osobowych wykonuje się w celu zapewnienia ciągłości działania tych systemów i nośników.

§ 43. 1. Przeglądy i konserwacje wykonuje administrator systemu informatycznego lub za zgodą administratora danych inna osoba, w tym osoba nie zatrudniona w Urzędzie Gminy, nieupoważniona do przetwarzania danych.

2. Przeglądy i konserwacje wykonywane przez osobę inną niż administrator systemu informatycznego wykonuje się pod osobistym nadzorem tego administratora lub innej osoby wyznaczonej przez administratora danych.

§ 44. Przeglądy i konserwacje wykonuje się w zakresie i częstotliwości określonej w harmonogramie stanowiącym załącznik nr 6 do zarządzenia.

§ 46. Nadzór nad wykonaniem niniejszego zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 47. Traci moc:

1) Zarządzenie Nr 4/2006 Wójta Gminy Zakrzewo z dnia 9 lutego 2006 r. w sprawie wprowadzenia Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Zakrzewo
2) Zarządzenie Nr 6/2006 Wójta Gminy Zakrzewo z dnia 14 lutego 2006 r. w sprawie instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Zakrzewo.

§ 48. Zarządzenie wchodzi w życie z podpisania.

WÓJT

Artur Nenczak