Załącznik Nr 2
do Zarządzenia Wójta Gminy Turośl
z dnia 29 grudnia 2016 roku

INSTRUKCJA

Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych

SPIS TREŚCI:

I. Postanowienia ogólne.

W Urzędzie Gminy Turośl obowiązuje **wysoki poziom bezpieczeństwa systemu informatycznego**, ponieważ co najmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.

1. Instrukcja Zarządzania Systemami Informatycznymi jest dokumentem regulującym zasady oraz procedury zarządzania i administrowania Systemami Informatycznymi Urzędu Gminy Turośl. Instrukcja obejmuje swoim zakresem wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemach informatycznych.
2. Celem procedury jest określenie wymagań bezpieczeństwa dla sprzętu i oprogramowania eksploatowanego w Urzędzie Gminy.
3. Sprzęt służący do przetwarzania danych osobowych składa się z komputerów stacjonarnych klasy PC oraz serwerów.
4. Użytkownik korzystający z komputera przenośnego jest zobowiązany do zachowania szczególnej ostrożności podczas transportu komputera oraz nie może udostępniać komputera osobom nieupoważnionym.
5. Sieć komputerowa służąca do przetwarzania danych osobowych posiada zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu komputerowego (zasilanie sieci musi być stabilizowane, np. poprzez zastosowanie zasilaczy stabilizowanych, UPS, itp.).
6. Główne węzły są podtrzymywane przez UPS zapewniający odpowiedni czas pracy systemu.
7. Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają licencje.
8. Administrator Systemu Informatycznego odpowiada za wyposażenie systemu informatycznego w mechanizmy uwierzytelniania użytkownika oraz sprawuje kontrolę dostępu do danych osobowych przez osoby upoważnione.
9. Ekrany monitorów są wyposażone w wygaszacze zabezpieczone hasłem, które aktywują się automatycznie po upływie określonego czasu od ostatniego użycia komputera.
10. Ekrany monitorów są ustawione w taki sposób, żeby w miarę możliwości uniemożliwić odczyt wyświetlanych informacji osobom nieupoważnionym.

II. Procedura nadawania uprawnień do przetwarzania danych, rejestrowanie tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

Celem procedury jest zapewnienie użytkownikom odpowiednich uprawnień do przetwarzania danych osobowych, aby zredukować zagrożenie nieuprawnionego dostępu do danych osobowych i utraty poufności. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych każdy pracownik musi zostać zapoznany przez bezpośredniego przełożonego lub IBT z przepisami dotyczącymi ochrony danych osobowych, otrzymać upoważnienie a na dowód przeszkolenia złożyć stosowne oświadczenie.

PROCEDURA NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH:

1. Administrator Danych Osobowych (ADO - Wójt):
   1) nadaje/odbiera pracownikowi upoważnienie do przetwarzania danych w systemach/aplikacjach eksploatowanych w Urzędzie Gminy w związku z wykonywanymi przez niego zadaniami,
   2) zgłasza do IBT/AST potrzebę nadania/odebrania uprawnień w systemie informatycznym na wymaganym poziomie.
2. Inspektor Bezpieczeństwa Teleinformatycznego (IBT - Sekretarz):
   1) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych zgodnie z załącznikiem nr 2,
   2) zleca IST założenie użytkownika w systemie i nadanie mu koniecznych uprawnień.
3. Administrator Systemu Teleinformatycznego (IST – informatyk):
   1) generuje login i hasło spełniające kryteria poziomu zabezpieczeń,
   2) wprowadza odpowiednią konfigurację w systemie/programie komputerowym
4. Wyrejestrowanie użytkownika z systemu informatycznego realizuje AST po zaakceptowaniu przez IBT wniosku o cofnięcie upoważnienia do przetwarzania danych osobowych
5. Powyższe zasady nadawania/odbierania uprawnień dostępu do wszystkich systemów/aplikacji eksploatowanych w Urzędzie Gminy obowiązują wszystkich pracowników.

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

1. Naczelną zasadą bezpieczeństwa systemów/aplikacji i sieci jest ochrona informacji przed nieuprawnionym dostępem, ujawnieniem, przypadkowym lub nieautoryzowanym zniszczeniem lub modyfikacją danych. Stosowanie zasad uwierzytelniania użytkowników systemów/aplikacji ma bezpośredni wpływ na zachowanie poufności, rozliczalności oraz integralności danych.
2. W systemach/aplikacjach informatycznych stosuje się uwierzytelnienie, na poziomie:
   1) dostępu do systemu operacyjnego,
   2) dostępu do aplikacji,
   3) dostępu do komputera (hasło na poziomie biosu).
3. Do uwierzytelnienia użytkownika w systemie/aplikacji na obu poziomach używa się identyfikatorów i haseł:
   1) stosowanie unikalnych identyfikatorów użytkownika zapewnia bezpieczeństwo i realizuje zasady rozliczalności w systemach (rejestrowane w logach systemów),
   2) zasada ta ma na celu przypisanie w sposób jednoznaczny wszelkich działań w systemie konkretnemu użytkownikowi (nie dopuszcza się, aby użytkownik korzystał z kont: administrator, gość, a także z konta innego użytkownika),
   3) ograniczenie dostępu do informacji jedynie do kręgu użytkowników uprawnionych (autoryzowanych) wymaga przyjęcia odpowiednio dobranej polityki stosowania haseł.
4. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów bądź innych bezpośrednio kojarzących się z użytkownikiem.

III.1 Zasady przydziału haseł

1) Pierwsze hasło dla użytkownika ustala i przydziela AST,
2) użytkownik systemu niezwłocznie (po nadaniu hasła przez ASI), ustala swoje, znane tylko jemu hasło,
3) hasło składa się z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

4) zmiana hasła przez użytkownika powinna następować nie rzadziej niż co 30, dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.,
5) użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło dostępu,
6) hasło nie może być ujawnione nawet po utracie przez nie ważności,
7) hasła mają charakter poufny, stanowią tajemnicę służbową – są znane tylko jego właścicielowi,
8) zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom,
9) hasła w bazie są zapisywane w systemie w postaci szyfrowanej,
10) hasła w stosunku, do których zaistniało podejrzenie o ich ujawnieniu podlegają bezzwłocznie zmianie,
11) Jeśli system to umożliwia, po przekroczeniu 5 prób logowania system blokuje dostęp do systemu informatycznego na poziomie danego użytkownika,
12) Jest zabronione zapamiętywanie haseł w programach/przeglądarkach.

III.2 Procedura zarządzania środkami uwierzytelniania

1. W celu zarządzania metodami oraz środkami uwierzytelniania mają zastosowanie „Procedura uwierzytelniania użytkownika w systemie informatycznym" oraz „ Procedura rejestrowania/wyrejestrowania użytkownika z systemu informatycznego".
    1) Procedura uwierzytelniania użytkownika w systemie informatycznym.
        a) Niepowtarzalny identyfikator oraz pierwsze hasło jest przydzielone użytkownikowi przez Administratora Bezpieczeństwa Teleinformatycznego po nadaniu uprawnień do przetwarzania danych osobowych.
        b) Bezpośredni dostęp do danych użytkownik uzyskuje po podaniu identyfikatora i właściwego hasła.
    2) Procedura rejestrowania/wyrejestrowania użytkownika z systemu informatycznego.
        a) Użytkownicy systemu informatycznego są niezwłocznie rejestrowani lub wykreślani z rejestru, gdy uzyskują lub tracą prawo dostępu do systemu,

b) Identyfikator po wyrejestrowaniu użytkownika zostaje zablokowany przez Administratora Bezpieczeństwa Teleinformatycznego.
c) Identyfikator po wyrejestrowaniu użytkownika nie jest przydzielany innej osobie.

IV Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego

Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utratą poufności w sytuacji, gdy użytkownik rozpoczyna, przerywa lub kończy pracę w systemie informatycznym przetwarzającym dane osobowe.

1. Procedura rozpoczęcia pracy:
   1) uruchomić komputer, podać hasło BIOS(jeśli dotyczy),
   2) zalogować się podając własny identyfikator i hasło dostępu, uruchomić wybrany system/aplikację podając własny identyfikator i hasło dostępu.
2. Procedura zawieszenia pracy w systemie/aplikacji:
   1) przy każdorazowym opuszczeniu stanowiska komputerowego, należy dopilnować, aby na ekranie nie były wyświetlane informacje lub dane osobowe, poprzez zablokowanie komputera (wylogowanie z profilu lub uruchomienie wygaszacza ekranu).
   2) Każdy użytkownik ma obowiązek stosowania wygaszacza ekranu (ustawionego na max. 10 min.) zabezpieczonego hasłem lub wylogowania się z systemu.
3. Procedura zakończenia pracy w systemie:
   1) zamknąć system/aplikację,
   2) zamknąć system operacyjny komputera i zaczekać na jego wyłączenie,
   3) wyłączyć monitor
   4) sprawdzić, czy elektroniczne nośniki informacji zawierające dane osobowe nie zostały pozostawione w komputerze lub bez odpowiedniego zabezpieczenia.
4. Użytkownik w pełnym zakresie odpowiada za powierzony mu sprzęt komputerowy i wykonywane czynności aż do momentu rozliczenia ze sprzętu komputerowego.

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

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych,
2. Za proces tworzenia kopii zapasowych odpowiada AST,
3. W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych użytkownicy systemu informatycznego zobowiązani są do centralnego przechowywania kopii danych, tak aby możliwe było ich łatwe zabezpieczenie poprzez wykonanie kopii zapasowych,
4. Kopie zapasowe informacji przechowywanych w systemie informatycznym przetwarzającym dane osobowe tworzone są w następujący sposób:

a) Częstotliwość tworzenia kopi zapasowych jest zależna od częstotliwości aktualizacji/wprowadzenia zmian w bazach danych:

- w cyklu dobowym, poza godzinami pracy, za pomocą automatycznych skryptów, wykonywane są lokalne kopie baz danych umieszczone na serwerach (kopie lokalne)

- w cyklu dobowym, w godzinach pracy, za pomocą automatycznych lub uruchamianych ręcznie skryptów wykonywane są kopie baz danych umieszczonych na komputerach użytkowników;

- w cyklu tygodniowym wykonywane są kopie na nośnikach zewnętrznych;

- kopie programów, w których zmiany są dokonywane jedynie sporadycznie w ciągu miesiąca, mogą być wykonywane odpowiednio w cyklach tygodniowych, dwutygodniowych lub miesięcznych np.: Płatnik, Sputnik Środki Trwałe, Druki IPS, itp..

b) W przypadku programów z własnymi (wbudowanymi) bazami danych, tworzona jest kopia zapasowa programu przetwarzającego te dane,

c) Kopie zapasowe należy wykonywać przed aktualizacją programu lub zmianą jego wersji.

d) Użytkownicy we własnym zakresie odpowiadają za kopie zapasowe wytworzonych przez siebie dokumentów

5. Wydruki i dokumenty papierowe zawierające dane osobowe przechowywane są wyłącznie w zamykanych szafach.
6. Osoba zatrudniona przy przetwarzaniu danych osobowych sporządzająca wydruk zawierający dane osobowe ma obowiązek na bieżąco sprawdzać przydatność wydruku w wykonywanej pracy, a w przypadku jego nieprzydatności – niezwłocznie wydruk zniszczyć.
7. Elektroniczne nośniki informacji z danymi osobowymi są oznaczane i przechowywane w zamykanych szafach znajdujących się w Urzędzie Gminy, do którego dostęp mają wyłącznie upoważnieni pracownicy.
8. Fizyczna likwidacja zniszczonych lub niepotrzebnych elektronicznych nośników informacji z danymi osobowymi odbywa się w sposób uniemożliwiający odczyt danych osobowych.
9. Do tworzenia kopii zapasowych wykorzystywane są dedykowane do tego celu urządzenia wchodzące w skład systemu informatycznego na nośnikach wymiennych adekwatnych do rodzaju urządzenia,
10. Nośniki kopii zapasowych, które zostały wycofane z użycia, jeżeli jest to możliwe, należy pozbawić zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych lub podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika, w sposób uniemożliwiający odczytanie zapisanych na nich danych.

VI. Sposób, miejsce i okres przechowywania

1. Elektroniczne nośniki informacji zawierające dane osobowe:
   1) dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne,
   2) nośniki danych osobowych oraz wydruki powinny być przechowywane w zamkniętych szafach wewnątrz obszaru przeznaczonego do przetwarzania danych osobowych i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar,
   3) przekazywanie nośników danych osobowych i wydruków poza urząd powinno odbywać się za wiedzą IBT,
   4) w przypadku, gdy nośnik danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie danych z nośnika
   5) jeżeli wydruk danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki dokumentów,
2. Zasady przechowywania kopii
   1) kopie zapasowe na nośnikach danych są przechowywane w metalowej szafie , znajdującej się w pokju nr 16,
   2) dostęp do metalowej szafy mają tylko upoważnieni pracownicy, tj. ADO/AST(ASI)/IST
   3) gdy kopia zapasowa nie jest dłużej potrzebna, należy przeprowadzić jej zniszczenie lub usunięcie danych z nośnika,
5. Maksymalny czas przechowywania nośników danych wynosi trzy miesiące.
6. Kopie zapasowe starsze niż 3 miesiące powinny być w zależności od nośnika wymazywane lub niszczone w sposób uniemożliwiający ich odczyt.
7. W przypadku konieczności przechowywania kopii zapasowych przez okres dłuższy niż 3 miesiące, wszystkie kopie zapasowe zbiorów danych osobowych, aplikacji przetwarzających dane osobowe oraz danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, których to dotyczy muszą być okresowo (co najmniej raz na pół roku) sprawdzane pod względem ich dalszej przydatności. Czynności te wykonuje AST,

VII. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia

Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:

- załączniki do poczty elektronicznej,
- przeglądane strony internetowe,
- pliki i aplikacje pochodzące z nośników wymiennych uruchamiane i odczytywane na stacji roboczej.

1. Ochrona antywirusowa

1) za ochronę antywirusową odpowiada AST,
2) oprogramowanie antywirusowe jest instalowane/konfigurowane przez AST na wszystkich stanowiskach komputerowych:
   a) rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) powinien być stale włączony,
   b) antywirusowy skaner ruchu internetowego musi być stale włączony,
   c) monitor zapewniający ochronę przed wirusami makr w dokumentach MS Office musi być stale włączony,
   d) skaner poczty elektronicznej musi być stale włączony.
4) aktualizacja oprogramowania antywirusowego odbywa się w sposób automatyczny dla wszystkich komputerów zainstalowanych w sieci,
5) instalacja oprogramowania antywirusowego oraz jego aktualizacja na komputerach niepodłączonych do sieci, odbywa się nie rzadziej niż raz w tygodniu i jest wykonywana przez AST,
6) system antywirusowy powinien mieć ustawione automatyczne skanowanie nośników wymiennych (pendrive, dyskietki 3,5'' , płyty CD)
7) użytkownik systemu na stanowisku komputerowym, importujący dane do systemu informatycznego, jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów i szkodliwego oprogramowania.
8) oprogramowanie na komputerach może być zainstalowane wyłącznie przez AST,

9)pracownicy nie są uprawnieni do instalacji jakiegokolwiek oprogramowania bez odpowiedniej zgody IBT/AST. W przypadku zainstalowania takiego oprogramowania bez odpowiedniej akceptacji pracownik ponosi odpowiedzialność porządkową i prawną.

10)pracownicy mogą używać połączenia z Internetem jedynie w celach służbowych,

11)pracownicy nie mają prawa przekazywać za pośrednictwem sieci komputerowej do stron trzecich jakichkolwiek danych osobowych bez wiedzy ADO/IBT,

12)pracownicy nie mogą ściągać i wysyłać za pośrednictwem sieci komputerowej plików wykonywalnych i instalacyjnych.

13)Użytkownicy systemu informatycznego zobowiązani są do skanowania zawartości nośników wymiennych odczytywanych na stacji roboczej pod względem potencjalnie niebezpiecznych kodów – przy każdym odczycie,

W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy administrator systemu teleinformatycznego powinien podjąć działania zmierzające do usunięcia zagrożenia.

W szczególności działania te mogą obejmować:

1) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,
2) odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,
3) samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z zewnętrznymi ekspertami.

2. Ochrona przed awarią zasilania

1) system, w którym przetwarzane są dane osobowe powinien posiadać mechanizmy pozwalające zabezpieczyć je przed ich utratą lub zmianą spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej,

2) dane osobowe przetwarzane w systemie chroni się stosując filtry zabezpieczające przed skutkami spadku napięcia oraz urządzenia podtrzymujące zasilanie do momentu poprawnego zapisania danych i wylogowania się użytkownika z systemu.

VII. Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 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)

1. System informatyczny musi posiadać mechanizm uwierzytelniający użytkownika, wykorzystujący identyfikator i hasło. Powinien także posiadać mechanizmy pozwalające na określenie uprawnień użytkownika do korzystania z przetwarzanych informacji (np. prawo do odczytu danych, modyfikacji istniejących danych, tworzenia nowych danych, usuwania danych),
2. System informatyczny powinien posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych, w szczególności zapis ten powinien obejmować:
   1) daty pierwszego wprowadzenia do systemu,
   2) identyfikatora użytkownika wprowadzającego dane,
   3) źródła danych w przypadku zbierania danych nie od osoby której one dotyczą,
   4) rozpoczęcie i zakończenie pracy przez użytkownika systemu,
   5) operacje wykonywane na przetwarzanych danych, a w szczególności ich dodanie, modyfikację oraz usunięcie,
   6) przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu,
   7) nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
   8) błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

Zapis działań użytkownika uwzględnia:

- identyfikator użytkownika,
- datę i czas, w którym zdarzenie miało miejsce,
- rodzaj zdarzenia,
- określenie informacji, których zdarzenie dotyczy (identyfikatory rekordów).
- w ramach możliwości technicznych system informatyczny powinien posiadać mechanizmy pozwalające na automatyczne powiadomienie Administratora Bezpieczeństwa Informacji lub osoby przez niego uprawnionej o zaistnieniu zdarzenia

krytycznego (mogącego mieć krytyczne znaczenie dla bezpieczeństwa przetwarzanych danych osobowych),

- ponadto system informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem:
  - identyfikatora osoby, której dane dotyczą,
  - osoby przesyłającej dane,
  - odbiorcy danych,
  - zakresu przekazanych danych osobowych,
  - daty operacji,
  - sposobu przekazania danych.

1. Dla każdego systemu, w którym przetwarzane są dane osobowe, prowadzony jest Rejestr, w którym odnotowywane są informacje o odbiorcach danych z tego systemu (o ile występuje dla danego systemu proces udostępniania danych).
2. W systemie/aplikacji użytkowanych do przetwarzania danych osobowych są zapisywane informacje o logowaniach użytkowników (logi).
3. Odbiorcą danych jest każdy, komu udostępnia się dane:
   a) osoby, której dane dotyczą,
   b) podmiotu, któremu powierzono przetwarzanie danych,
   c) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
4. Odnotowanie obejmuje informacje o:
   a) nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane,
   b) zakresie udostępnianych danych,
   c) dacie udostępnienia.
5. Obowiązek odnotowania ww. informacji w Rejestrze spoczywa na użytkowniku systemu udostępniającemu dane.
6. Odnotowanie informacji w Rejestrze powinno nastąpić niezwłocznie po udostępnieniu danych.
7. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
8. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

VIII. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

Prace serwisowe prowadzone w tym zakresie mogą być wykonywane wyłącznie przez pracowników lub przez upoważnionych przedstawicieli wykonawców zewnętrznych znajdujących się w towarzystwie pracowników.

Przed rozpoczęciem prac serwisowych przez osoby zewnętrzne konieczne jest potwierdzenie tożsamości serwisantów. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

- likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie:
- `przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
- naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

1. Dla zachowania ciągłości pracy i bezpieczeństwa danych przeprowadza się przegląd i konserwację platformy sprzętowej, na której eksploatowany jest system/aplikacja.
2. Przeglądy i konserwacja urządzeń:
   1) przeglądy i konserwacja urządzeń wchodzących w skład platformy sprzętowej dla danego systemu/aplikacji powinny być wykonywane w terminach określonych przez producenta sprzętu,
   2) jeśli producent nie przewidział dla danego urządzenia potrzeby dokonywania przeglądów eksploatacyjnych, lub też nie określił ich częstotliwości, to o dokonaniu przeglądu oraz sposobie jego przeprowadzenia decyduje AST,
   3) przegląd i konserwacja urządzeń, może być wykonana na żądanie przełożonego AST,
   4) czynności, o których mowa w ppkt a) i b) wykonuje AST co najmniej jeden raz na kwartał,
   5) nieprawidłowości ujawnione w trakcie przeglądów bądź konserwacji, powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane.

3. Przegląd systemów/aplikacji i narzędzi programistycznych przeprowadzany jest w celu sprawdzenia poprawności działania i wykonywany jest w następujących przypadkach:
   1) zmiany wersji oprogramowania systemu/aplikacji,
   2) zmiany systemu operacyjnego platformy sprzętowej, na której eksploatowany jest system/aplikacja,
   3) wykonania zmian w systemie/aplikacji spowodowanych koniecznością naprawy lub modyfikacji systemu.
4. Przed dokonaniem zmian w systemie/aplikacji należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych, na testowej bazie danych. Sprawdzenie powinno m.in. obejmować:
   1) poprawność logowania się do systemu w zależności od posiadanych uprawnień (zasymulować pracę wszystkich typów uprawnień użytkownika),
   2) poprawność działania funkcjonalności systemu/aplikacji sprawdzonej na różnego typu danych,
   3) poprawność działania wszystkich elementów aplikacji (menu, zestawienia, formularze, raporty, itp.).
5. Za prawidłowość przeprowadzenia procesu przeglądu i konserwacji systemu/aplikacji odpowiada AST.
6. Konserwację systemu/aplikacji przeprowadza się w obecności użytkownika.

Załącznik nr 1
do Instrukcji Zarządzania
Systemami Informatycznymi

Data nadania upoważnienia: .....

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie § 15 ust. 2 Regulaminu Organizacyjnego Urzędu Gminy Turośl stanowiącego załącznik do Zarządzenia Nr 33/03 Wójta Gminy Turoś;l z dnia 24 listopada 2003 roku, w związku z art. 37 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. 2002 r. Nr 101, poz. 926) oraz działem I ppkt. g Polityki Ochrony Danych Osobowych w Urzędzie Gminy w Turośli.

1. Upoważniam Panią/Pana .....
(imię i nazwisko upoważnianego)

zatrudnioną/-ego na stanowisku .....
do dostępu do następujących danych osobowych zawartych w zbiorach:
– .....
– .....
– .....
(zakres upoważnienia: wskazanie kategorii danych, które może przetwarzać określonaw upoważnieniu osoba, lub rodzaj czynności lub operacji, jakich może dokonywać na danych osobowych)

2. Identyfikator w systemie operacyjnym: .....
3. Identyfikator w programie: .....

4. Okres trwania upoważnienia: .....
(okres obowiązywania upoważnienia)

Wystawił: .....
(podpis administratora lub osoby reprezentującej administratora)

5. Osoba upoważniona do przetwarzania danych objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Data i podpis osoby upoważnionej: .....

mgr Piotr Niedbała

Załącznik nr 2
do Instrukcji Zarządzania
Systemami Informatycznymi

EWIDENCJA

OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Numer i data nadania upoważnienia	Upoważnienie ważne do dnia	Zakres/Nazwa zbioru danych	Nazwa systemu informatycznego	Identyfikator nadany w systemie	Identyfikator nadany w systemie operacyjnym