Załącznik nr 2
do Zarządzenia nr 17/2012
Burmistrza Miasta i Gminy Frombork
z dnia 22.03.2012r.

Urząd Miasta i Gminy Frombork,
Ul. Młynarska 5a,
14-530 Frombork

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Zgodnie z § 3 Rozporządzenia Ministra Sprawa 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), zwanego dalej „rozporządzeniem", wdraża się niniejszy dokument stanowiący „Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych", w celu stworzenia kompleksowych rozwiązań służących zapewnieniu bezpieczeństwa systemów informatycznych służących do przetwarzania danych.

Cel instrukcji

Celem wydania instrukcji jest realizacja zapisów Polityki Bezpieczeństwa przetwarzania danych osobowych obowiązującej w Urzędzie Miasta i Gminy we Fromborku oraz zaleceń § 5 rozporządzenia. Instrukcja ma charakter ***uniwersalny*** i precyzuje zagadnienia zarządzania ***wszystkimi*** systemami informatycznymi znajdującymi się w Urzędzie Miasta i Gminy we Fromborku.

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

1. Administrator danych (ADO):
   - Nadaje upoważnienie w zakresie dostępu do systemu informatycznego osobie, która w związku z wykonywanymi przez siebie obowiązkami będzie miała dostęp do danych osobowych w systemie,
   - Przekazuje wypełniony dokument w postaci papierowej:
     - 1 egz. do kadr- celem umieszczenia teczce akt osobowych
     - 1 egz. do osoby której upoważnienie dotyczy
     - 1 egz. do Administrator Bezpieczeństwa Informacji (ABI)

2. ABI:
   - Aktualizuje ewidencję osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym

3. Administrator Systemu Informatycznego (ASI):
   - Rejestruje użytkownika w systemie i nadaje mu określone uprawnienia oraz hasło

4. Użytkownik:
   - Uwierzytelnia się w systemie po podaniu identyfikatora oraz hasła uzyskanego od Informatyka
   - Użytkownik zmienia hasło na swoje, którego nie przekazuje nikomu i może rozpocząć pracę w aplikacji

5. Użytkownik jest wyrejestrowany z systemu informatycznego w każdym przypadku utraty przez niego uprawnień dostępu do danych osobowych, co ma miejsce w przypadku:
   - Ustania zatrudnienia
   - Zmiany zakresu obowiązków
   - Utraty uprawnienia
   - Informację pisemną o ustaniu zatrudnienia, zmianie zakresu obowiązków i utracie upoważnienia, przekazują kadry do ABI z chwilą ich zaistnienia

II. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzeniem i użytkowaniem:

1. W systemie informatycznym stosuje się uwierzytelnienia dwustopniowe; na poziomie:
   - Dostępu do stacji roboczej
   - Dostępu do aplikacji

2. Do uwierzytelnienia użytkownika w systemie na obu poziomach stosuje się hasła.
3. Hasło dostępu do stacji roboczej składa się, co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.
4. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
5. Hasło nie może być ujawnione nawet po utracie przez nie ważności.
6. Zmiana hasła do systemu następuje nie rzadziej, niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.
7. Dla każdej osoby upoważnionej instalowany jest odrębny identyfikator i hasło, tak, aby bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym mogła mieć tylko ta osoba, która poda właściwy identyfikator i hasło.
8. Identyfikator użytkownika jest wpisywany do ewidencji osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym wraz z zakresem upoważnienia oraz datą nadania uprawnień.
9. System zostanie zablokowany po trzykrotnej próbie nieudanego logowania się.

III. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu:

1. Rozpoczęcia pracy:
   - Uruchomienie komputera w systemie podając hasło
   - Uruchomić komputer i zalogować się podając swój identyfikator dostępu do stacji

roboczej
- Uruchomić aplikację, wpisując swój identyfikator i hasło dostępu - uzależnione od programu
- Rozpocząć pracę

2. Procedura zawieszenia pracy w systemie:
   - Przy każdym opuszczeniu stanowiska komputerowego, dopilnować, aby na ekranie nie były wyświetlone dane osobowe
   - Przed opuszczeniem miejsca pracy na dłuższy czas użytkownik obowiązany jest poczekać, aż zaktywizuje się wygaszacz ekranu

3. Procedura zakończenia pracy w systemie:
   - Zarchiwizować dane
   - Zamknąć aplikację
   - Zamknąć system
   - Wyłączyć monitor i drukarkę

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

1. W cyklu cotygodniowym kopie wykonywane są w serwerze oraz na odrębnym stanowisku komputerowym pełniącym funkcję archiwum.
2. W cyklu miesięcznym kopie zapisywane są na płytach cd.
3. W razie potrzeby kopie zapasowe wykonywane są przez użytkowników aplikacji na płytach lub innych nośnikach pamięci w cyklu codziennym.
4. ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.

V. Sposób, miejsce i okres przechowywania:

1. Wydruki archiwalne lub bieżące przechowywane mogą być wyłącznie w pomieszczeniach uniemożliwiających dostęp do nich przez osoby nieupoważnione.
2. Wydruki, zawierające dane osobowe, należy zniszczyć przez pocięcie w niszczarce nie później niż po upływie 3 dni, po ich wykorzystaniu chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania.
3. Za bezpieczeństwo danych zapisanych w komputerach przenośnych oraz w innych urządzeniach przenośnych w całości odpowiada użytkownik komputera lub urządzenia przenośnego.
4. Po zakończeniu pracy przez użytkowników systemu, elektroniczne nośniki informacji są przechowywane w zamykanych na klucz szafach biurowych lub szafach pancernych.
5. Przeznaczone do likwidacji elektroniczne i optyczne nośniki informacji, mogące zawierać dane osobowe, pozbawia się w sposób trwały zapisu tych danych, a w przypadku gdy nie jest to możliwe, niszczy lub uszkadza się w sposób trwale uniemożliwiający ich odczytanie, nie później niż po upływie 3 dni.
6. Za skasowanie zbędnych danych lub zniszczenie zbędnych nośników elektronicznych odpowiedzialny jest ASI.
7. Kopie zapasowe zbioru danych osobowych przechowywane są w serwerowni.

8. Dostęp do serwerowni mają tylko upoważnieni pracownicy, tj. ABI i ASI oraz Burmistrz Gminy.
9. Kopie zapasowe przechowuje się przez okres:
   - dzienne - przez siedem dni,
   - tygodniowe -do końca następnego tygodnia,
   - miesięczne -dwunastu miesięcy następujących po miesiącu sporządzenia kopii, dopuszcza się dłuższy okres przechowywania, o ile pozwalają na to warunki,
10. Dane osobowe zapisane w formie papierowej inne niż wydruki z systemu (pisma, ankiety itp.) są przechowywane na podobnych zasadach, co wydruki.
11. W przypadku konieczności przekazywania elektronicznych lub optycznych nośników informacji zawierających dane osobowe podmiotom zewnętrznym w sytuacjach nie związanych z wykonywanymi działaniami służbowymi, nośniki te pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie.
12. W przypadku konieczności przekazywania elektronicznych lub optycznych nośników informacji zawierających dane osobowe podmiotom zewnętrznym w sytuacjach nie związanych z wykonywanymi działaniami służbowymi oraz brakiem możliwości pozbawienia się wcześniej zapisanych na nich danych, na czas przekazania sporządza się stosowną umowę powierzenia danych osobowych.

VI. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego lub inna ingerencja w ten system.

1. Nadzór nad instalowaniem nowego oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawuje ASI.
2. Oprogramowanie zastosowane w systemach informatycznych automatycznie monitoruje występowanie wirusów w trakcie załączania lub wczytywania danych z zewnętrznych nośników informacji.
3. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
4. Czynności związane z ochroną antywirusową systemu informatycznego wykonuje ASI, wykorzystując w trakcie pracy moduł programu antywirusowego z aktualną bazą antywirusową.
5. ASI ma obowiązek zgłaszać na piśmie ADO wszelkie potrzeby lub zauważone niedociągnięcia w zakresie zapewnienia bezpieczeństwa systemu informatycznego.
6. O każdorazowym wykryciu wirusa przez oprogramowanie antywirusowe użytkownik obowiązany jest niezwłocznie poinformować ABI lub ASI.
7. W przypadku, gdy system zabezpieczeń wskazuje zaistnienie zagrożenia, użytkownicy są zobowiązani bezzwłocznie powiadomić o tym fakcie ASI, który po jego usunięciu sprawdza system i przywraca go do pełnej funkcjonalności.
8. ASI jest odpowiedzialny za aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku:
   - Sieci lokalnej
   - Stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej

9. Ochrona systemu informatycznego używanego w urzędzie polega na:
   - Ochronie przez identyfikator,
   - Ochronie za pomocą hasła,
   - Przydzielaniu praw,
10. Bezwzględnie zakazuje się użytkownikom samowolnego korzystania z prywatnych lub pochodzących ze źródła innego niż miejsce pracy nośników informacji (magnetycznych, optycznych, urządzeń podłączanych do stacji roboczych). Korzystanie z takich nośników może mieć miejsce wyłącznie po uzyskaniu zgody ASI, po uprzednim sprawdzeniu nośnika informacji przez ASI pod względem bezpieczeństwa dla systemu informatycznego.
11. Bezwzględnie zabrania się użytkownikom łamania lub obchodzenia zabezpieczeń systemów informatycznych. O każdym przypadku znalezienia luki w zabezpieczeniach użytkownik ma obowiązek powiadomić ABI oraz ASI.

VII. Zasady i sposób odnotowania w systemie informacji o udostępnianiu danych osobowych.

1. W komórce organizacyjnej w której przetwarzane są dane osobowe prowadzi się rejestr. W niektórych aplikacjach możliwe jest odnotowanie informacji o odbiorcach danych z tego systemu.
2. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
   - Osoby, której dane dotyczą,
   - Osoby użytkowania systemu lub innej osoby upoważnionej do przetwarzania danych osobowych w urzędzie,
   - Przedstawiciela, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych,
   - Podmiotu, któremu powierzono przetwarzanie danych,
   - Organów państwowych lub organów samorządu terytorialnego, któremu dane są udostępnione w związku z prowadzonym postępowaniem.
3. Odnotowanie obejmuje informacje o:
   - Nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane,
   - Zakresie udostępniania danych,
   - Dacie udostępniania
4. Udostępnianie danych osobowych może nastąpić wyłącznie na pisemną prośbę odbiorcy danych
5. Nadzór nad prawidłowością odnotowywania w systemie ww. informacji sprawuje ABI.

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

1. O przeprowadzonych przeglądach i konserwacjach systemu każdorazowo informowany jest ABI, który może nadzorować przebieg prac.
2. Przeglądu i konserwacji sprzętu w sieci informatycznej, systemów informatycznych i nośników informacji dokonuje stosownie do potrzeb ASI w porozumieniu z ABI.
3. Za terminowość przeprowadzania przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.

4. Bezwzględnie zabronione jest samodzielne dokonywanie przez użytkowników napraw sprzętu informatycznego, wymiana jego podzespołów oraz wykonywanie innych czynności nie związanych bezpośrednio z jego eksploatacją lub nie dopuszczonych do wykonywania przez producenta sprzętu w instrukcji obsługi.
5. Użytkownik ma obowiązek niezwłocznie powiadomić ABI o wszelkich nieprawidłowościach i awariach sprzętu informatycznego, mogących prowadzić do próby naruszenia lub naruszenia bezpieczeństwa danych osobowych.
6. Sprawdzanie poprawności działania programów i narzędzi programowych przeprowadza się w następujących przypadkach:
   - Zmiany wersji oprogramowania serwera plików
   - Zmiany wersji oprogramowania stanowiska komputerowego użytkownika systemu
   - Zmiany systemu operacyjnego serwera plików
   - Zmiany systemu operacyjnego stanowiska komputerowego użytkownika systemu
   - Wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji
   - lub modyfikacji systemu.
7. Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych. Sprawdzanie powinno obejmować:
   - Poprawność logowania się do systemu w zależności od posiadanych uprawnień (zasymulować pracę wszystkich typów uprawnień użytkownika)
   - Poprawność działania wszystkich elementów aplikacji (menu, zestawienia, formularze, raporty)
8. Poprawność funkcjonowania aplikacji polega na symulacji działania wykonujące następujące operacje:
   - Wprowadzania danych osobowych;
   - Edytowania danych osobowych;
   - Wyszukiwania danych osobowych;
   - Wydruku danych osobowych
9. Przegląd przeprowadza projektant nowego systemu w obecności ASI.
10. Za prawidłowość przeprowadzania przeglądów i konserwacji systemu odpowiada ASI.
11. Konserwację oprogramowania przeprowadza się po zgłoszeniu przez użytkownika systemu potrzeby wprowadzenia zmian pozwalających utrzymać funkcjonalność systemu w dynamicznie zmieniającym się środowisku pracy.
12. Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych na podobnych zasadach jak ma to miejsce w przypadku przeglądu oprogramowania