Załącznik nr 2 do Zarządzenia nr 20/12/2013 Prezydenta Miasta Lublin z dnia 13 grudnia 2013 r.
w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Lublin

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Lublin

Rozdział I
Podstawowe mechanizmy w jakie powinny być wyposażone urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

§ 1

Systemy informatyczne służące do przetwarzania danych osobowych powinny być wyposażone w mechanizmy:

1) rozliczalności, który pozwala jednoznacznie przypisać wykonanie określonych czynności przetwarzania konkretnej osobie upoważnionej;
2) integralności, który pozwala autoryzować czynności zmiany lub zniszczenia danych;
3) tworzenia raportu, który zawiera zakres i treść przetwarzanych danych;
4) uwierzytelniania, który weryfikuje deklarowaną tożsamość osoby upoważnionej.

Rozdział II
Procedury rozpoczęcia, zawieszenia i zakończenia pracy

§ 2

1. Rozpoczęcie pracy w systemie informatycznym następuje po zalogowaniu się do systemu informatycznego.
2. Logowanie do systemu informatycznego dokonywane jest za pomocą przydzielonego identyfikatora i hasła lub przyznanej karty kryptograficznej i kodu PIN.
3. Niedopuszczalne jest:
   1) zapisywanie hasła i przechowywanie go w miejscu, gdzie znajduje się stacja robocza lub w innym powszechnie dostępnym miejscu;
   2) udostępnianie hasła innej osobie;
   3) udostępnianie karty kryptograficznej lub kodu PIN innej osobie.
4. Oddalenie się od stacji roboczej poza pomieszczenie, w którym się ona znajduje, wymaga uprzedniego zablokowania stacji roboczej (w systemie Windows kombinacja klawiszy Windows + L). Wyjęcie karty kryptograficznej z czytnika powoduje automatyczne wylogowanie.
5. Zakończenie pracy na stacji roboczej wymaga wylogowania się z systemu informatycznego i wyłączenia komputera.

Rozdział III
Procedury nadawania i odbierania uprawnień do przetwarzania danych osobowych oraz rejestrowania i wyrejestrowywania tych uprawnień w systemach informatycznych

§ 3

1. Administrator systemu, przydzielając uprawnienia w systemie informatycznym, posługuje się słownikiem charakterystycznych dla danego zbioru czynności w celu określenia zakresu uprawnień w systemie w ramach zakresu upoważnienia.
2. Administrator systemu decyduje na podstawie rozporządzenia i stosuje dla zbioru danych osobowych właściwy poziom bezpieczeństwa:
   1) podstawowy – jeżeli przetwarzane są dane osobowe oraz żadne z urządzeń systemu informatycznego nie jest połączone z siecią publiczną;
   2) podwyższony – jeżeli przetwarzane są dane osobowe wrażliwe, wymienione w art. 27 ustawy oraz żadne z urządzeń systemu informatycznego nie jest połączone z siecią publiczną;
   3) wysoki – jeżeli przynajmniej jedno urządzenie systemu informatycznego jest połączone z siecią publiczną.
3. Procedury nadawania i cofania upoważnień do przetwarzania danych osobowych zostały szczegółowo opisane w załączniku nr 1 do Zarządzenia.

Rozdział IV
Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 4

1. W przypadku wystąpienia zbieżności identyfikatora z przyznanym już wcześniej, administrator systemu nadaje osobie upoważnionej inny identyfikator.
2. Pierwsze przydzielone hasło powinno być jednorazowe a po jego poprawnym użyciu system powinien automatycznie wymuszać wpisanie nowego hasła.
3. Hasła zmieniane są przez osoby upoważnione.
4. System powinien zapewniać:
   1) odrębny identyfikator dla każdego użytkownika z zastrzeżeniem, że identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie;
   2) jakość hasła, czyli zastosowanie odpowiedniej liczby znaków, w tym wielkich i małych liter, cyfr lub znaków specjalnych w zależności od poziomu bezpieczeństwa oraz jego zmianę co 30 dni.
5. Osoba upoważniona posiadająca hasło dostępu do systemu jest obowiązana zachować je w tajemnicy i nie ujawniać innym osobom.
6. System powinien wymuszać tworzenie haseł składających się z niepowtarzalnego zestawu co najmniej:
   1) sześciu znaków na poziomie bezpieczeństwa podstawowym;
   2) ośmiu znaków w tym dużych i małych liter, cyfr lub znaków specjalnych, na poziomach bezpieczeństwa podwyższonym i wysokim.

Rozdział V
Procedury tworzenia i przechowywania kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania oraz sposób, miejsce i okres przechowywania elektronicznych nośników danych

§ 5

1. Kopie zapasowe tworzone są:
   1) automatycznie przez system zarządzający serwerami, na specjalnie do tego celu przeznaczonych komputerach, macierzach, bibliotekach dyskowych lub taśmowych;
   2) przez administratora systemu na elektronicznych nośnikach danych.
2. Kopie zapasowe przechowuje się w pomieszczeniu, do którego dostęp mają jedynie osoby upoważnione.
3. Kopie zapasowe zaleca się przechowywać w innej lokalizacji niż ta, w której znajdują się zbiory danych.
4. Kopie zapasowe, pełne lub przyrostowe, tworzone są codziennie.
5. Przeznaczone do likwidacji elektroniczne nośniki danych pozbawia się wcześniej zapisu tych danych, a gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
6. Kopie zapasowe zawierające dane osobowe usuwa się niezwłocznie po ustaniu ich użyteczności, chyba że przepisy szczegółowe stanowią o ich dłuższym przechowywaniu.

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

§ 6

1. Systemy informatyczne chronione są przed działaniem szkodliwego kodu przez specjalistyczne oprogramowanie ochronne, zainstalowane na serwerach, stacjach roboczych i komputerach przenośnych.
2. Oprogramowanie ochronne sprawuje ciągły nadzór nad pracą systemu i zasobami danych osobowych na serwerach, komputerach przenośnych i stacjach roboczych, poprzez skanowanie dysków.
3. Oprogramowanie ochronne jest codziennie automatycznie aktualizowane przez pobieranie z serwerów producenta nowo dodanych definicji zagrożeń.
4. W przypadku wykrycia zagrożenia należy postępować zgodnie z zaleceniami wyświetlanymi przez oprogramowanie ochronne.
5. W przypadku, gdy samodzielne działania, podjęte przez użytkownika zgodnie z zaleceniami wyświetlanymi przez oprogramowanie ochronne, okażą się nieskuteczne, należy niezwłocznie skorzystać z pomocy serwisu Wydziału Informatyki i Telekomunikacji.
6. Elektroniczne nośniki danych i ich zawartość podlegają automatycznej kontroli przez oprogramowanie ochronne przy każdorazowym ich włączeniu do komputera.

Rozdział VII
Wymagania wobec systemu informatycznego przetwarzającego dane osobowe

§ 7

1. Systemy informatyczne powinny rejestrować:
   1) identyfikator osoby upoważnionej, przetwarzającej dane osobowe w systemie informatycznym i przypisywać tę czynności tylko jej;
   2) datę i czas zalogowania i wylogowania z systemu informatycznego;
   3) tożsamość stacji roboczej;
   4) nieudane i udane próby zalogowania się;
   5) wygaśnięcie czasu obowiązywania hasła dostępu do stacji roboczej.
2. Systemy informatyczne powinny zapewnić sporządzanie dla każdej osoby, której dane są przetwarzane w systemie informatycznym, raportu zawierającego:
   1) datę pierwszego wprowadzenia danych do systemu informatycznego;
   2) identyfikator osoby upoważnionej wprowadzającej te dane;
   3) źródła danych w przypadku zbierania danych nie od osoby, której one dotyczą;
   4) informacji o odbiorcach danych, którym dane osobowe zostały udostępnione o której mowa w art. 7 pkt 6 ustawy;
   5) dacie i zakresie udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
   6) sprzeciwu wobec przetwarzania danych osobowych o którym mowa art. 32 ust. 1 pkt 8 ustawy.
3. Rejestracja, o której mowa w ust. 1 następuje przez automatyczny zapis w systemie informatycznym.
4. Raport, o którym mowa w ust. 2 musi być zrozumiały dla przeciętnego odbiorcy, czyli powinien prezentować informacje w pełnym brzmieniu, poprzedzone nazwą opisową danego pola (nie w postaci kodowanej lub skróconej) oraz powinien generować dane tylko i wyłącznie jednej osoby.
5. Systemy informatyczne służące do przetwarzania danych osobowych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie nie muszą generować raportu, o którym mowa w ust. 2.
6. Systemy informatyczne, których dane wykorzystywane do uwierzytelniania są przesyłane w sieci publicznej muszą być chronione środkami kryptograficznej ochrony.

Rozdział VIII
Procedury wykonywania przeglądów i konserwacji systemów oraz elektronicznych nośników danych służących do przetwarzania danych osobowych

§ 8

1. Podmioty zewnętrzne mogą wykonywać przeglądy i konserwacje systemów informatycznych przy zachowaniu pełnej separacji danych osobowych od osób nie posiadających upoważnienia do przetwarzania, pod nadzorem administratora systemu lub w obecności osoby upoważnionej.
2. Elektroniczne nośniki danych przeznaczone do naprawy pozbawia się wcześniej

zapisu poprzez skasowanie danych programem trwale usuwającym pliki lub naprawia się je pod nadzorem osoby upoważnionej.
3. Elektroniczne nośniki danych nie nadające się do dalszego użytkowania pozbawia się wcześniej zapisu tych danych, a gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.

Rozdział IX
Przetwarzanie danych osobowych na komputerach przenośnych

§ 9

1. Decyzję o przetwarzaniu danych osobowych na komputerach przenośnych podejmuje zarządzający zbiorem po konsultacji ryzyka przetwarzania z dyrektorem IT.
2. Osoba upoważniona przetwarzająca dane osobowe przy użyciu komputera przenośnego jest zobowiązana do zachowania szczególnej staranności podczas jego transportu, przechowywania i użytkowania a zwłaszcza:
   1) do stosowania środków ochrony kryptograficznej wobec przetwarzanych danych osobowych;
   2) nie pozostawiania komputera przenośnego bez dozoru;
   3) nie instalowania bez wiedzy i zgody administratora systemu żadnego oprogramowania na komputerze przenośnym;
   4) nie udostępniania nikomu komputera oraz identyfikatora i hasła do systemu operacyjnego.
3. Przetwarzanie danych osobowych może odbywać się z użyciem zdalnego dostępu do sieci Urzędu Miasta Lublin poprzez szyfrowane połączenie pomiędzy komputerem użytkownika i siecią Urzędu Miasta Lublin. Podczas ustanawiania połączenia każda osoba upoważniona przechodzi proces uwierzytelnienia. Uwierzytelnienie następuje po identyfikacji, czyli zadeklarowaniu swojej tożsamości przez użytkownika przez podanie identyfikatora. Zadeklarowana, ale jeszcze niezweryfikowana, tożsamość jest potwierdzana w procesie uwierzytelnienia przez podanie hasła. Następnie osoba upoważniona przechodzi powtórne uwierzytelnianie podczas logowania do zbioru danych osobowych. Wydział Informatyki i Telekomunikacji rejestruje wszystkie zestawione w ten sposób połączenia.

Rozdzielnik:
1. Oryginał: Wydział Organizacji Urzędu.
2. Kopia użytkowa: www.bip.lublin.eu, intranet.