Gminna Biblioteka Publiczna w Zakrzówku
ul. Żeromskiego 24 B, 23–213 Zakrzówek
tel/fax: (81) 821–50–36
biblioteka@zakrzowek.gmina.pl
www.gbp.zakrzowek.gmina.pl

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

GMINNEJ BIBLIOTEKI PUBLICZNEJ W ZAKRZÓWKU ORAZ FILII W STUDZIANKACH, SULOWIE I RUDNIKU DRUGIM

Wydanie: 02

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Administrator Danych: **Teresa Stankiewicz, Dyrektor Gminnej Biblioteki Publicznej w Zakrzówku** dnia 01 lutego 2015 r. zgodnie z **Rozporządzeniem 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 wdraża dokument o nazwie „**Instrukcja zarządzania systemem informatycznym**" zwany dalej „**Instrukcją**".

Zapisy tego dokumentu wchodzą w życie z dniem wdrożenia.

Ilekroć w **„Instrukcji"** jest mowa o:

1) **ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwaną dalej „ustawą";
2) **identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
3) **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
4) **sieci telekomunikacyjnej** – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)
5) **sieci publicznej** – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne;
6) **teletransmisji** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej
7) **rozliczalności** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
8) **integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
9) **raporcie** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
10) **poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
11) **uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 1.

Za przestrzeganie w Gminnej Bibliotece Publicznej w Zakrzówku zapisów **„Instrukcji"** odpowiedzialny jest **Administrator Danych** lub zgodnie z zapisem §2 „**Polityki Bezpieczeństwa**" wyznaczony **Administrator Bezpieczeństwa Informacji**.

§ 2.

W związku z tym, że w Gminnej Bibliotece Publicznej w Zakrzówku przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną, oraz uwzględniając kategorie przetwarzanych danych

i zagrożenia wprowadza się poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym na poziomie wysokim, a w związku z tym wprowadza się poniższe postanowienia:

I

Obszar, w który są przetwarzane dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne za zgodą Administratora Danych, Administratora Bezpieczeństwa Informacji lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

II

1) W systemie informatycznym służącym do przetwarzania danych osobowych, przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie nadane przez **Administratora Bezpieczeństwa Informacji**. Użytkownik przetwarzający dane po otrzymaniu upoważnienia oraz identyfikatora użytkownika i hasła jest zobowiązany niezwłocznie dokonać zmiany hasła oraz zachować je w tajemnicy.
2) Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni. Hasło nadane przez użytkownika musi składać się z co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
3) Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego poprzez zainstalowanie programu antywirusowego o nazwie *COMODO Antivirus*, poprzez zainstalowanie firewalla (zapory sieciowej), poprzez zabezpieczenie sieci radiowej odpowiedniej mocy uwierzytelnieniem.
2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego UPS.

IV

1) Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
2) W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
3) Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie wszystkich danych osobowych muszą być tworzone nie rzadziej niż raz na tydzień.
4) Kopie zapasowe:
   a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w zamkniętym pomieszczeniu nr 04 .
   b) usuwa się niezwłocznie po ustaniu ich użyteczności.

V

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych w tym stosuje hasła dostępu do komputera przenośnego oraz do plików, w których przetwarzane są dane osobowe.

VI

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

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

§ 3.

1) Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym – z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie – system ten zapewnia odnotowanie:
   a) daty pierwszego wprowadzenia danych do systemu;
   b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
   c) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
   d) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i kresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
   e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.
2) Odnotowanie informacji, o których mowa w ust – 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
3) Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust 1;
4) W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§ 4.

Po zakończeniu pracy w systemie informatycznym użytkownik ma obowiązek wylogować się z systemu. W przypadku braku czynności ze strony użytkownika w systemie informatycznym przez 30 min, system samoczynnie wyloguje użytkownika przetwarzającego dane osobowe.

§ 5.

Administrator Bezpieczeństwa Informacji ma obowiązek dokonywać przeglądów technicznych sprzętu informatycznego w przedsiębiorstwie oraz dbać o ich dobry stan techniczny. Zaleca się dokonywanie przeglądów okresowych co 30 dni oraz przeglądów generalnych raz na rok. W przypadku stwierdzenia usterek technicznych **Administrator Bezpieczeństwa Informacji** ma obowiązek niezwłocznie powiadomić o tym fakcie **Administratora Danych**.

§ 6.

W przypadku stwierdzenia przez **Administratora Bezpieczeństwa Informacji** uchybień dotyczących przetwarzania danych w przedsiębiorstwie powinien o tym fakcie niezwłocznie powiadomić **Administratora Danych** oraz wprowadzić takie zabezpieczenia i procedury, które w przyszłości wyeliminują takie zdarzenia.

§ 7.

W sprawach nieuregulowanych w niniejszej **„Instrukcji”** mają zastosowanie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przemarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzeni i systemy informatyczne służące do przetwarzania danych osobowych.

Podpis Administratora Danych Osobowych

….....

Podpis

Podpis Administratora Bezpieczeństwa Informacji

….....

Podpis