**ZARZĄDZENIE Nr 19/2019**
**DYREKTORA ZARZĄDU LOKALI MIEJSKICH**
**z dnia 12 marca 2019 r.**

**w sprawie wprowadzenia Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Zarządzie Lokali Miejskich**

Na podstawie § 9 ust. 2 pkt. 4 regulaminu organizacyjnego stanowiącego załącznik do zarządzenia Nr 9609/VII/18 Prezydenta Miasta Łodzi z dnia 24 października 2018 r. w sprawie zatwierdzenia regulaminu organizacyjnego jednostki budżetowej o nazwie Zarząd Lokali Miejskich

**zarządzam, co następuje:**

§ 1. Wprowadzam do stosowania w Zarządzie Lokali Miejskich Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, która stanowi załącznik do niniejszego zarządzenia.

§ 2. Naruszenie zasad określonych w niniejszej Instrukcji przez pracowników Zarządu może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.

§ 3. Naruszenie zasad określonych w niniejszej Instrukcji przez osoby fizyczne i podmioty, z którymi Zarząd zawarł umowę może być potraktowane jako nienależyte wykonanie umowy w rozumieniu Kodeksu cywilnego.

§ 4. Traci moc Zarządzenie Nr 14/2018 Dyrektora Zarządu Lokali Miejskich z dnia 25 maja 2018 r. w sprawie wprowadzenia Instrukcji Zarządzania Systemami Informatycznymi Służącymi do Przetwarzania Danych Osobowych obowiązującej w Zarządzie Lokali Miejskich.

§ 5. Zarządzenie wchodzi w życie z dniem wydania, z mocą od dnia 1 marca 2019 r.

**p.o. DYREKTORA**
**ZARZĄDU LOKALI MIEJSKICH**

**Andrzej Chojnacki**

Załącznik
do Zarządzenia nr 19/2019
Dyrektora ZLM
z dnia 12 marca 2019 r.

**Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Zarządzie Lokali Miejskich**

**Postanowienia ogólne**

§ 1. Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Zarządzie Lokali Miejskich, zwana dalej Instrukcją, określa sposób zarządzania systemami informatycznymi, wykorzystywanymi do przetwarzania danych osobowych w Zarządzie Lokali Miejskich .

§ 2. Instrukcja służy zabezpieczeniu danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 3. Celem Instrukcji jest zapewnienie takiego stopnia bezpieczeństwa danych osobowych, który odpowiadałby ryzyku, w rozumieniu art. 32 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016).

§ 4. Ilekroć w Instrukcji jest mowa o:
1) Zarządzie – należy przez to rozumieć Zarząd Lokali Miejskich (ZLM);
2) Dyrektorze – należy przez to rozumieć Dyrektora Zarządu Lokali Miejskich;
3) Administratorze Danych (ADO) – należy przez to rozumieć Dyrektora Zarządu Lokali Miejskich;
4) administratorze systemów informatycznych (ASI) – należy przez to rozumieć powołaną przez ADO osobę na niniejsze stanowisko;
5) Administratorze lokalnym ePUAP – należy przez to rozumieć administratora zarządzającego kontem ePUAP w Zarządzie;
6) haśle – należy przez to rozumieć ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;
7) identyfikatorze – należy przez to rozumieć ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
8) integralności danych – należy przez to rozumieć właściwość zapewniającą, że dane osobowe nie zostały zmienione, usunięte lub zniszczone w sposób nieautoryzowany;
9) odbiorcy danych – należy przez to rozumieć każdego, komu udostępnia się dane osobowe, z wyłączeniem:
   a) osoby, której dane dotyczą,
   b) osoby upoważnionej do przetwarzania danych,
   c) przedstawiciela, o którym mowa w art. 27 RODO,
   d) podmiotu przetwarzającego, o którym mowa w art. 28 RODO,
   e) organów publicznych, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z przepisami prawa;
10) IOD – należy przez to rozumieć inspektora ochrony danych tj. osobę wyznaczoną przez

ADO, która będzie realizowała zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych;

11) poufności danych – należy przez to rozumieć właściwość zapewniającą, że dane nie są udostępniane lub ujawniane nieupoważnionym podmiotom;
12) podmiocie przetwarzającym – należy przez to rozumieć podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawartej zgodnie z art. 28 RODO;
13) raportach – należy przez to rozumieć przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
14) RODO – należy przez to rozumieć rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych, w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
15) rozliczalności – należy przez to rozumieć właściwość zapewniającą, że podejmowane działania mogą być przypisane w sposób jednoznaczny konkretnej osobie lub podmiotowi;
16) sieci publicznej – należy przez to rozumieć publiczną sieć telekomunikacyjną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017, poz. 1907 z późn. zm.);
17) serwisancie – należy przez to rozumieć firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego;
18) SIAD – należy przez to rozumieć system informatyczny administratora danych tj. sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych;
19) ustawie – należy przez to rozumieć obowiązującą ustawę o ochronie danych osobowych;
20) uwierzytelnianiu – należy przez to rozumieć działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
21) upoważnionym – należy przez to rozumieć osobę, która posiada upoważnienie do przetwarzania danych osobowych nadane przez Administratora Danych zgodnie z art. 29 ogólnego rozporządzenia;
22) użytkowniku – należy przez to rozumieć upoważnionego, któremu nadano identyfikator i przyznano hasło;
23) IZSI – należy przez to rozumieć niniejszą Instrukcję zarządzania systemami informatycznymi;
24) PBDO – należy przez to rozumieć Politykę Bezpieczeństwa Danych Osobowych obowiązującą w Zarządzie Lokali Miejskich wraz ze zmianami;
25) ZSI DOM5 – należy przez to rozumieć zintegrowany system informatyczny zawierający w sobie zbiory danych osobowych.

§ 5. W celu zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku, ADO wdraża odpowiednie środki techniczne i organizacyjne, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Obejmują one m.in.: mechanizmy kontroli dostępu do danych, stosowanie oprogramowania antywirusowego, czy stosowanie bezpiecznych haseł.

§ 6. Oceniając adekwatność stosowanych środków uwzględnia się stan wiedzy technicznej, koszt wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

§ 7. Ocena adekwatności stosowanych środków w celu zapewnienia bezpieczeństwa systemu informatycznego dokonywana jest zgodnie z procedurami określonymi w PBDO.

§ 8. Ogólny opis środków zastosowanych w celu zapewnienia bezpieczeństwa systemu zawiera opis zasobów danych osobowych, będących załącznikiem do PBDO.

**Nadawanie uprawnień i wyrejestrowywanie użytkowników**

§ 9. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie użytkownik upoważniony do przetwarzania danych osobowych, zarejestrowany w tym systemie przez ASI na wniosek kierownika Wydziału ds. Kadr lub IOD.

§ 10. Rejestracja użytkownika, o której mowa w § 9, polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do ewidencji użytkowników systemu prowadzonej przez ASI.

§ 11. ASI przekazuje do Wydziału ds. Kadr informację o identyfikatorze, który został nadany użytkownikowi.

§ 12.1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje ASI, na wniosek IOD lub kierownika Wydziału ds. Kadr.

2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.

3. Wyrejestrowanie następuje poprzez:

1) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe);
2) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4. Wyrejestrowanie czasowe musi nastąpić w przypadku:

1) nieobecności użytkownika w pracy trwającej dłużej niż 30 dni kalendarzowych (system ZSI DOM 5 automatycznie po tym terminie wymusza zmianę hasła);
2) zawieszenia w pełnieniu obowiązków służbowych;
3) zwolnienia ze świadczenia pracy/odsunięcia od wykonywania czynności służbowych.

5. Wyrejestrowanie czasowe może nastąpić w przypadku:

1) wypowiedzenia umowy o pracy;
2) wszczęcia postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych;

6. Wyrejestrowanie trwałe następuje w przypadku rozwiązania lub wygaśnięcia stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

§ 13.1. O przyznaniu pracownikowi uprawnień do potwierdzania, przedłużania i unieważniania profili zaufanych ePUAP przez administratora lokalnego ePUAP decyduje ADO.

2. Procedura nadawania przez Administratora lokalnego ePUAP (na polecenie ADO) uprawnień pracownikowi realizującemu potwierdzanie, przedłużenie i unieważnianie profili zaufanych ePUAP uregulowana jest odrębnymi przepisami.

**Metody i środki uwierzytelnienia oraz zasady związane z ich zarządzaniem i użytkowaniem**

§ 14. 1. Pracownikom nadawane są unikalne identyfikatory.

2. Nazwy kont pracowników muszą zapewniać jednoznaczną identyfikację i składają się z pierwszej litery imienia pracownika oraz jego nazwiska.

3. W identyfikatorze pomija się polskie znaki diakrytyczne.

4. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika, ASI za zgodą ADO, nadaje inny identyfikator, odstępując od zasady określonej powyżej.

§ 15. 1. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

2. Hasło nie może być identyczne z identyfikatorem użytkownika, ani jego imieniem lub nazwiskiem.

3. W systemie SIAD wyróżniamy dwa hasła – hasło do stacji roboczej oraz hasło do ZSI DOM5.

4. Za prawidłowość konstrukcji haseł odpowiada użytkownik systemu.

5. System informatyczny ZSI DOM 5 wymusza zmianę hasła co 30 dni.

6. IOD może, w uzasadnionych sytuacjach, polecić dokonanie zmiany hasła przez użytkownika systemu.

7. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.

**Procedury rozpoczęcia, zawieszenia i zakończenia pracy, przeznaczone dla użytkowników systemu**

§ 16.1. Rozpoczęcie pracy na stacji roboczej następuje po włączeniu komputera, a następnie wprowadzeniu indywidualnego identyfikatora i hasła użytkownika.

2. Monitory komputerów winny być wyposażone we włączające się nie później niż po 10 minutach od przerwania pracy wygaszacze ekranu.

3. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła.

4. W przypadku opuszczenia stanowiska pracy użytkownik obowiązany jest aktywować wygaszacz ekranu lub w inny sposób zablokować stację roboczą.

5. Zakończenie pracy na stacji roboczej następuje po wprowadzeniu danych tego dnia przetwarzanych w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera.

6. Przed opuszczeniem pokoju należy:

1) zniszczyć w niszczarce, lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe;
2) schować do zamykanych na klucz szaf wszelkie akta zawierające dane osobowe;
3) umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu;
4) zamknąć okna.

7. Opuszczając pokój, należy zamknąć za sobą drzwi na klucz oraz pozostawić go w miejscu do tego wyznaczonym, określonym w Regulaminie pracy.

§ 17.1. O ile to możliwe, przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują zasady określone w IZSI, dotyczące pracy na komputerach stacjonarnych.

2. Użytkownicy, którym zostały powierzone komputery przenośne, powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych, szczególną ostrożność należy zachować podczas ich transportu.

3. Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone, w tym przez domowników i osoby bliskie użytkownikowi.

4. Praca na komputerze przenośnym możliwa jest po wprowadzeniu hasła i indywidualnego identyfikatora użytkownika.

5. Użytkownicy są zobowiązani zmieniać hasła w komputerach przenośnych nie rzadziej niż raz na 30 dni.

6. Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach przenośnych. Wszelkie zmiany mogą być dokonywane tylko pod

nadzorem ASI, stosownie do wymagań IZSI. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zgłosić to ASI.

7. Komputery przenośne wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizację sugeruje automatycznie system.

8. Użytkownik nie posiada praw administracyjnych do komputera przenośnego. Dostęp do BIOS (Basic Input/Output System – podstawowy system wejścia-wyjścia ) jest chroniony hasłem.

§ 18.1. Wynoszenie poza obszar przetwarzania danych urządzeń i dokumentów zawierających dane osobowe jest dopuszczalne jedynie za wiedzą i zgodą ADO lub bezpośredniego przełożonego, gdy konieczność taka została uzgodniona z ADO.

2. Urządzenia zawierające dane osobowe wynoszone poza obszar przetwarzania danych należy chronić przed uszkodzeniami fizycznymi. Należy też bezwzględnie przestrzegać zaleceń producentów dotyczących ochrony sprzętu, w szczególności należy pamiętać, że urządzenia elektroniczne mogą ulec uszkodzeniu w skutek działania silnego pola elektromagnetycznego.

3. Urządzenia przenośne, nośniki danych oraz dokumenty wynoszone poza obszar przetwarzania danych nie powinny być pozostawiane bez nadzoru. W szczególności zabrania się pozostawiania urządzeń i dokumentów zawierających dane osobowe bez odpowiedniego zabezpieczenia w miejscach publicznych, pokojach hotelowych oraz w samochodach.

4. Wykorzystywanie urządzeń przenośnych, nośników danych oraz dokumentów zawierających dane osobowe w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, stwarza warunki minimalizujące ryzyko utraty, zniszczenia lub zapoznania się z danymi przez osoby nieupoważnione.

5. Za miejsca szczególnego ryzyka należy uznać restauracje oraz środki komunikacji publicznej.

6. Niedozwolone jest udostępnianie urządzeń przenośnych i nośników danych należących do Zarządu osobom nieupoważnionym, w tym domownikom i osobom bliskim użytkownika.

7. Użytkownik obowiązany jest zachować w tajemnicy wobec wszystkich osób, w tym wobec domowników i osób bliskich identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym lub chroniącym dostęp do nośników danych.

8. Nośniki magnetyczne z danymi osobowymi powinny być odpowiednio zabezpieczane (np. w zamkniętych na klucz szafach), a po wykorzystaniu dane na nich zawarte powinny zostać trwale usuwane lub nośniki te powinny zostać zniszczone.

9. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia ich programem antywirusowym na wyznaczonym w tym celu stanowisku komputerowym oraz do oznakowania tego nośnika.

**Zasady tworzenia kopii zapasowych**

§ 19.1. W systemie informatycznym wykorzystującym technologię klient-serwer kopie zapasowe wykonuje się po stronie serwera.

2. Dostęp do kopii bezpieczeństwa serwera plików mają wyznaczeni pracownicy Wydziału Informatyki.

3. W przypadku aplikacji ZSI DOM5 kopie bezpieczeństwa tworzone i przechowywane są przez Wydział Informatyki Urzędu Miasta Łodzi.

4. Dostęp do kopii ZSI DOM5 posiadają wyłącznie pracownicy Wydziału Informatyki Urzędu Miasta Łodzi.

§ 20. Kopie zapasowe serwera plików tworzy się raz w tygodniu, a na koniec tygodnia –

kopię wszystkich plików serwera.

§ 21.1. Kopie zapasowe serwera plików przechowuje się na oddzielnym dedykowanym serwerze plików bądź przenośnym dysku USB .

2. Dostęp do kopii zapasowych posiadają wyznaczeni Pracownicy Wydziału Informatyki oraz ADO

3. Zabrania się przechowywania kopii zapasowych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.

§ 22.1. Nośniki zawierające nieaktualne kopie danych, będące poza wykazem cyklicznych kopii, podlegają likwidacji, której dokonują pracownicy Wydziału Informatyki.

2. W przypadku nośników jednorazowych, takich jak płyty CD-R, DVD-R, likwidacja polega na ich fizycznym zniszczeniu w taki sposób, by nie można było odczytać ich zawartości.

3. Nośniki wielorazowego użytku, takie jak dyski twarde, dyskietki, płyty CD-RW, DVD-RW, można wykorzystać ponownie do celów przechowywania kopii bezpieczeństwa po uprzednim usunięciu ich zawartości.

4. Nośniki wielorazowego użytku nienadające się do ponownego użycia należy zniszczyć fizycznie.

§ 23.1. Dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach.

2. Po ustaniu przydatności tych kopii, dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane.

3. Przetwarzając dane osobowe, należy odpowiednio często zapisywać dokonane zmiany, lub robić kopie robocze danych, na których się właśnie pracuje. Dane winny być zapisywane w odpowiednie obszary serwera plików co zapobiegnie ich ewentualnej utracie.

**Sposób zabezpieczenia i konserwacji systemu informatycznego**

§ 24.1. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych przez ASI.

2. Oprogramowanie, o którym mowa w ust. 1, sprawuje ciągły nadzór (praca ciągła w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.

3. Niezależnie od ciągłego nadzoru, o którym mowa w ust. 2, ASI nie rzadziej niż raz na tydzień przeprowadza pełną kontrolę obecności wirusów komputerowych w SIAD.

4. Do obowiązków ASI należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów, dokonywanych przez przedmiotowe oprogramowanie.

5. Użytkownik jest obowiązany zawiadomić ASI o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.

6. Dostęp do Internetu możliwy jest jedynie na stacjach roboczych specjalnie chronionych urządzeniem sprzętowym z wbudowanym programem Firewall i translacją adresów NAT (Network Address Translation).

§ 25. System informatyczny ZSI DOM5 umożliwia automatycznie:

1) przypisanie wprowadzanych danych użytkownikowi (identyfikatorowi użytkownika), który te dane wprowadza do systemu;
2) sygnalizację wygaśnięcia czasu obowiązywania hasła dostępu do stacji roboczej (dotyczy to także komputerów przenośnych);
3) sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane w systemie,

raportu zawierającego:
a) datę pierwszego wprowadzenia danych do systemu,
b) identyfikator użytkownika wprowadzającego te dane,
c) źródła danych – w przypadku zbierania danych nie od osoby, której one dotyczą,
d) informacji o odbiorcach danych, którym dane osobowe zostały udostępnione, o dacie i zakresie tego udostępnienia,
e) wniesienia sprzeciwu wobec przetwarzania danych osobowych, o którym art. w art. 21 RODO;
4) odnotowanie informacji, o których mowa w pkt 3, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

§ 26.1. Przeglądu i konserwacji systemu dokonuje ASI doraźnie.
2. Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) ASI dokonuje nie rzadziej niż raz na tydzień.
3. Poprawy danych osobowych w zbiorze dokonuje użytkownik przy nadzorze ASI.
4. Zapisy logów systemowych powinny być przeglądane przez ASI codziennie oraz każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.
5. Kontrole i testy przeprowadzane przez ASI powinny obejmować wszelkie uprawnienia poszczególnych użytkowników w SIAD.

§ 27.1. Wszelkie naprawy urządzeń komputerowych oraz zmiany w SIAD przeprowadzane są, o ile to możliwe przez pracowników Wydziału Informatyki pod nadzorem ASI.
2. Naprawy i zmiany w SIAD przeprowadzane przez serwisanta dokonywane są pod nadzorem ASI w siedzibie Zarządu (jeśli to możliwe) lub poza siedzibą Zarządu, po uprzednim nieodwracalnym usunięciu danych w nich przetwarzanych. W przypadku nadmiernych utrudnień, przedmiotowe naprawy i zmiany przeprowadzane będą po zawarciu umów powierzenia przetwarzania danych osobowych.
3. Jeśli nośnik danych (dysk, dyskietka, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie i sporządzić protokół z wykonanych czynności.

§ 28.1. Użytkownik zobowiązany jest zawiadomić w pierwszej kolejności ADO i IOD, a następnie ASI o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:
1) naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje, bądź można przetwarzać dane bez wprowadzenia hasła);
2) częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień;
3) braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera;
4) wykryciu wirusa komputerowego;
5) zauważeniu elektronicznych śladów próby włamania do systemu informatycznego;
6) podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe;
7) zmianie położenia sprzętu komputerowego;
8) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.

2. Do czasu przybycia na miejsce ASI należy:
1) o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnić w działaniu również ustalenie jego przyczyn lub sprawców;

2) rozważyć wstrzymanie bieżącej pracy na komputerze, lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia;
3) zaniechać, o ile to możliwe dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę;
4) zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku;
5) przygotować opis incydentu;
6) nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia ASI lub osoby przez niego wskazanej.

3. ASI, po otrzymaniu zawiadomienia, o którym mowa w ust. 1, niezwłocznie:
1) podejmuje czynności zmierzające do weryfikacji informacji zawartych w zawiadomieniu;
2) gdy to właściwe podejmuje czynności zmierzające do minimalizacji ewentualnych negatywnych konsekwencji zaistniałego zdarzenia oraz chroniące system przed ponownym naruszeniem;
3) o ile to możliwe zabezpiecza dowody przydatne do ustalenia przyczyn, typu i skutków naruszenia;
4) w przypadku stwierdzenia naruszenia lub podejrzenia naruszenia ochrony danych osobowych zawiadamia IOD.

4. W ramach czynności wskazanych w ust. 3 pkt 2 i pkt 3, ASI w szczególności:
1) może zarządzić odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części;
2) może zarządzić odtwarzanie danych z kopii zapasowych, po uprzednim upewnieniu się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu.

5. W przypadku, gdy IOD otrzyma zawiadomienie, o którym mowa w ust. 3 pkt 4, do dalszego postępowania stosuje się postanowienia zawarte w PBDO.

6. ASI zobowiązany jest do bieżącego informowania ADO o awariach systemu informatycznego, zauważonych przypadkach naruszenia IZSI przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych. Powyższą informację ASI przekazuje do wiadomości IOD.

**Korzystanie z systemu kontroli dostępu, wydawanie oraz użytkowanie kart dostępu.**

§ 29.1. W siedzibie Zarządu Lokali Miejskich przy al. Tadeusza Kościuszki 47 obowiązuje elektroniczny system kontroli dostępu do stref bezpieczeństwa , o których jest mowa w §24 i § 25 PBDO.

§ 30.1. System kontroli dostępu:
1) weryfikuje uprawnienia wejścia na teren siedziby;
2) nadzoruje ruch osób w określonych obszarach siedziby poprzez zarejestrowanie wejścia i wyjścia z tych stref,
3) zbiera i archiwizuje dane zarówno wejść jak i wyjść pracowników Zarządu Lokali Miejskich.

2. Wstęp na teren stref następuje na podstawie karty dostępu, która identyfikuje w systemie kontroli dostępu daną osobę jako upoważnioną do wejścia na teren określonej strefy.

3. Obszary kontroli dostępu oraz dostępu do nich dla danego pracownika lub grupy pracowników określane są przez IOD przy współpracy z Kierownikiem Wydziału Organizacyjno-Administracyjnego.

4. Wprowadzanie uprawnień, przypisywanie kart oraz obsługa systemu kontroli dostępu zajmuje się ASI lub w przypadku nieobecności Kierownik Wydziału Informatyki.

5. Karty dostępu dla pracowników Zarządu wydawane są na czas ich zatrudnienia na podstawie zawartej umowy o świadczenie pracy.
6. Karty dostępu dla pracowników firm zajmujących się ochroną i sprzątaniem obiektu wydawane są na czas trwania umowy z daną firmą. W przypadku firm zajmujących się doraźnymi pracami na terenie siedziby wydawane są karty dostępu „gość" ograniczone czasowo do godzin pracy w danym dniu roboczym.
7. Karta dostępu jest indywidualnie przypisana do danego pracownika i nie może być odstępowana ani użyczana innym osobom. Za szkody spowodowane nieuprawnionym użyciem karty odpowiada właściciel karty, do momentu zgłoszenia jej utraty.
8. Fakt zniszczenia lub zagubienia Karty należy niezwłocznie zgłosić ASI lub Kierownikowi Wydziału Informatyki. Zgłoszenie takie spowoduje zablokowanie Karty.