ZARZĄDZENIE NR 72
BURMISTRZA MIROSŁAWCA

z dnia 10 września 2018 r.

w sprawie wprowadzenia "Instrukcji zarządzania systemami infromatycznymi w Urzędzie Miejskim w Mirosławcu"

Na podstawie art. 24 ust. 1 i 2 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) zarządza się, co następuje:

§ 1. Wprowadza się „Instrukcję zarządzania systemami informatycznymi w Urzędzie Miejskim w Mirosławcu" stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§ 2. Zobowiązuje się wszystkie osoby przetwarzające dane osobowe w Urzędzie Miejskim w Mirosławcu do przestrzegania zasad i realizacji zadań określonych w załączniku, o którym mowa w § 1.

§ 3. Traci moc Zarządzenie nr 89 Burmistrza Mirosławca z dnia 22 maja 2012 r. w sprawie ustalenia „Polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy i Miasta Mirosławiec oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy i Miasta Mirosławiec".

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik do zarządzenia Nr 72

Burmistrza Mirosławca

z dnia 10 września 2018 r.

Instrukcja zarządzania systemami informatycznymi w Urzędzie Miejskim w Mirosławcu

WSTĘP

Instrukcja stanowi wykaz procedur oraz stosowanych środków technicznych i organizacyjnych mających na celu, zgodnie z art. 32 RODO, zabezpieczyć przetwarzane dane osobowe przed: przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych oraz nieuprawnionym dostępem do danych osobowych.

§ 1. Zabezpieczenia fizyczne budynku Urzędu Miejskiego w Mirosławcu:

1. Budynek Urzędu jest zamykany po zakończeniu pracy.

2. Budynek całodobowo jest dozorowany przez system monitoringu Firmy ANTSERWIS - na zewnątrz budynku oraz wewnątrz zainstalowane są kamery (na zewnątrz jedna kamera od strony głównej budynku oraz druga od strony dziedzińca i wewnątrz budynku na parterze w korytarzu głównym).

3. W budynku Urzędu zainstalowany jest system alarmowy (2 czujniki na parterze – w korytarzu głównym oraz sterowniki w pokoju nr 9).

4. Od strony dziedzińca budynek jest częściowo okratowany.

5. W budynku Urzędu zgodnie z obowiązującymi przepisami rozmieszczony jest sprzęt przeciwpożarowy.

6. Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osób zatrudnionych i upoważnionych do przetwarzania danych.

7. Pomieszczenia, o których mowa wyżej powinny być zamykane na czas nieobecności pracowników w sposób uniemożliwiający dostęp do nich osób trzecich.

8. W przypadku przebywania interesantów bądź innych osób postronnych w pomieszczeniach, o których mowa wyżej, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

9. Do przebywania w pomieszczeniu, gdzie umieszczone są serwery (pokój nr 105) uprawniony jest Administrator Systemów Informatycznych (ASI), Sekretarz Gminy i Miasta, Inspektor Ochrony Danych oraz Kierownik Referatu Organizacyjno-Prawnego.

10. Przebywanie osób nieuprawnionych w pomieszczeniu, gdzie umieszczone są serwery (np. nieuprawniony pracownik referatu, konserwator, sprzątaczka) dopuszczane jest tylko w obecności osób wymienionych w ust. 9.

11. Kopie zapasowe baz danych przechowywane są w metalowej szafie zamykanej na 2 zamki w pokoju nr 8 oraz w skrytce bankowej.

12. Stosowana jest polityka kluczy.

§ 2. Zabezpieczenia sprzętowe w budynku Urzędu Miejskiego w Mirosławcu.

1. Każdy dokument papierowy, zawierający dane osobowe i przeznaczony do zniszczenia, powinien być zniszczony w sposób uniemożliwiający jego odczytanie przy pomocy niszczarki.

2. Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych drzwiami z zamkami patentowymi, z tym że drzwi wewnętrzne prowadzące do pomieszczenia nr 3a (stanowisko ds. gospodarki odpadami) oraz pomieszczenia, w którym znajduje się Urząd Stanu Cywilnego nr 4 są przeciwpożarowe oraz zabezpieczone przed wyważeniemi, wyposażone w 1 zamek atestowany; okna pomieszczeń nr 3 i 3a zabezpieczone są folią antywłamaniową.

3. Urządzenia wchodzące w skład systemu informatycznego podłączone są do trzech awaryjnych zasilaczy UPS w serwerowni, które zabezpieczają system na wypadek zaniku napięcia albo awarii w sieci zasilającej.

4. Stan instalacji elektrycznej winien zabezpieczać sprzęt informatyczny przed przepięciami, przewężeniami i zwarciami a pośrednio przed wystąpieniem pożaru.

5. Stan techniczny sieci komputerowej winien zabezpieczać system informatyczny przed ingerencją z zewnątrz mogącą spowodować zmianę, kradzież lub utratę bazy danych.

6. Sieć lokalna skonfigurowana jest w topologii gwiazdy.

7. Sieć lokalna podłączona jest do internetu poprzez security router zawierający firewall, IPS, funkcję blokowania adresów internetowych oraz zaawansowany monitor ruchu z funkcją logowania w celu analizy zdarzeń.

8. Sieć lokalna zabezpieczona jest na bieżąco aktualizowanym systemem antywirusowym typu client-serwer, w którym na serwerze zainstalowany jest moduł administrator zarządzający modułami klienckimi na stacjach roboczych.

9. Dostęp do serwera zawierającego dane osobowe zabezpieczony jest hasłem.

10. Kopie zapasowe wykonywane są w cyklach:

1) tygodniowy przyrostowy na serwerze kopii zapasowych oraz na dysku przechowywanym w skrytce bankowej w formie zaszyforwanej,

2) miesięcznym pełnym na macierzy sieciowej w formie zaszyfrowanej.

§ 3. 1. Środki ochrony w ramach oprogramowania systemu:

1) dostęp do baz danych osobowych zastrzeżony jest wyłącznie dla uprawnionych pracowników,

2) konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych przechowywanych w systemie informatycznym wyłącznie za pośrednictwem aplikacji,

3) system informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu odrębnie dla każdego pracownika,

4) zastosowano działający w tle program antywirusowy na komputerach użytkowników.

2. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych:

1) zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji,

2) dla każdego użytkownika systemu wyznaczony jest odrębny identyfikator,

3) użytkownicy mają dostęp do aplikacji umożliwiający dostęp tylko do tych danych osobowych, do których mają uprawnienia.

§ 4. Środki ochrony w ramach narzędzi baz danych i aplikacji.

1. Komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem.

2. Zastosowano wygaszenie ekranu oraz blokadę hasłem podczas dłuższej nieaktywności użytkownika w przypadku dłuższej nieaktywności użytkownika.

§ 5. Procedura nadawania uprawnień do przetwarzania danych osobowych.

Celem procedury jest minimalizacja ryzyka przetwarzania danych przez osoby nieupoważnione.

1. Dostęp do danych osobowych posiadają osoby, którym udzielono upoważnienia do przetwarzania danych osobowych.

2. Upoważnienia do przetwarzania danych osobowych udziela Administrator Danych Osobowych.

3. Osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do pracy zostaną przeszkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz poinformowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym.

4. Administrator Danych Osobowych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych oraz osób upoważnionych do przebywania w pomieszczeniach Urzędu.

5. Wszyscy użytkownicy podlegają okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na sprzęt nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.

6. Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych.

7. Wprowadzono obowiązek rejestracji wszystkich przypadków awarii systemu, działań konserwacyjnych w systemie oraz naprawy systemu.

8. Określono sposób postępowania z nośnikami informacji.

9. W przypadku, gdy zachodzi konieczność naprawy sprzętu poza siedzibą urzędu, należy wymontować z niego nośniki informacji zawierające dane osobowe.

§ 6. Metody i środki uwierzytelnienia (polityka haseł).

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

1. Pierwsze (pierwotne) hasło użytkownika nadawane jest przez administratora i przekazywane mu w poufny sposób.

2. Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła.

3. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.

4. W przypadku, gdy użytkownik zapomni hasła, administrator nadaje je ponownie, w trybie pierwszego (pierwotnego) ustawienia.

5. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.

6. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.

7. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.

8. Standard hasła do wszystkich programów i systemów to: hasło minimum 8 – znakowe, zawierające trzy wyróżniki (małe duże litery oraz znaki specjalne lub/i cyfry).

9. Hasło do stacji roboczej zmieniane jest co 90 dni. Zmiana hasła jest wymuszana przez system.

10. W przypadku programów systemowych zmiana hasła następuje wg norm tych systemów.

11. Hasła administracyjne zdeponowane są w metalowej szafie w pokoju Nr 101, natomiast klucze szyfrujące w metalowej szafie w pokoju nr 8.

12. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

13. W przypadkach awaryjnych (np. nieobecność administratora) hasło może być przekazane decyzją Informatyka osobie zastępującej administratora.

14. Po ustaniu sytuacji awaryjnej, Administrator jest zobowiązany do zmiany hasła.

§ 7. Procedura tworzenia kopii zapasowych.

1. Zbiory danych, oprogramowanie oraz konfiguracja systemów operacyjnych serwerów Administratora powinny być zabezpieczone w postaci cyklicznie wykonywanych kopii bezpieczeństwa lub archiwalnych.

2. Kopie bezpieczeństwa należy wykonywać minimum:

a) przed dokonaniem zmian w konfiguracji systemów operacyjnych lub oprogramowania,

b) przed dokonaniem zmian w programach (np. zmiana wersji),

c) przed i/lub po każdej istotnej zmianie danych w bazie danych.

3. Pliki użytkowników systemu informatycznego powinny być przechowywane na indywidualnie udostępnionych dyskach serwerów.

4. Dyski serwerów, o których mowa w pkt 3 zabezpiecza się przed utratą danych w postaci kopii bezpieczeństwa i/lub archiwalnych.

5. Kopie bezpieczeństwa należy wykonywać w co najmniej dwóch egzemplarzach, każdą, przy czym przynajmniej jedną zachować na zaszyfrowanym nośniku wymiennym,

6. Miejsce przechowywania kopii zabezpieczone jest przed nieuprawnionym dostępem oraz skutkami zdarzeń takich jak: pożar, zalanie, oddziaływanie silnego pola elektromagnetycznego, zanieczyszczenia środowiska.

§ 8. Utylizacja elektronicznych nośników i wydruków oraz czyszczenie danych.

1. Podlegające likwidacji uszkodzone lub przestarzałe nośniki a w szczególności macierze dyskowe / twarde dyski z danymi osobowymi ze stacji roboczych i laptopów / pendrive / pamięci flash / dyski SSD / płyty DVD / telefony komórkowe / smartfony są niszczone w sposób fizyczny. Stosowana metoda niszczenia, to fizyczne niszczenie (pocięcie, nawiercenie, młotkowanie) wymontowanych nośników / użycie degaussera / zmielenie w specjalistycznej firmie potwierdzone protokołem zniszczenia lub certyfikatem bezpieczeństwa firmy utylizacyjnej lub nagraniem z procesu transportu i utylizacji.

2. Nośniki informacji zamontowane w sprzęcie IT a w szczególności twarde dyski muszą być wyczyszczone specjalistycznym oprogramowaniem zanim zostaną przekazane poza obszar organizacji (np. sprzedaż lub darowizna komputerów stacjonarnych / laptopów / smartfonów).

3. Dokumentacja papierowa niszczona jest w niszczarkach paskowych oraz tam, gdzie to wymagane w niszczarkach o podwyższonym standardzie.

4. Dokumentacja papierowa niszczona jest za pośrednictwem firmy niszczącej dokumenty. Firma zobowiązana jest do wykazania się bezpieczną procedurą utylizacji (np. posiadać certyfikat ISO27001, nagrania z procesu transportu i utylizacji.

§ 9. Procedura zabezpieczenia systemu informatycznego.

1. Bezpieczeństwo przetwarzania danych poza organizacją:

1) użytkownicy komputerów przenośnych wynoszonych poza obszar organizacji, na których są przetwarzane dane osobowe są zobowiązani do przestrzegania zasad bezpieczeństwa i podpisania regulaminu użytkowania komputerów przenośnych.
2) stosuje się procedurę zabezpieczenia sprzętu mobilnego.
3) stosuje się szyfrowanie dysków komputerów przenośnych zawierających dane osobowe, jeśli wynoszone są poza obszar organizacji.
4) dyski przenośne / pendrive wynoszone poza organizację muszą być zaszyfrowane.
5) sprzęt mobilny (smartfony/tablety) zabezpieczono mechanizmem uwierzytelniania.
6) sprzęt mobilny wyposażony jest w oprogramowanie umożliwiające jego nadzór, blokowanie dostępu, czyszczenie zawartości.
7) w przypadku użycia komputerów przenośnych lub sprzętu mobilnego do zdalnego dostępu do zasobów wewnętrznej sieci przez Internet, stosuje się szyfrowanie tego połączenia z użyciem VPN.
8) w przypadku użycia komputerów przenośnych lub sprzętu mobilnego do zdalnego dostępu do zasobów wewnętrznej sieci przez Internet uwierzytelnienia dokonuje się z użyciem loginu i podania hasła.

2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej (stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów):

1) dokonuje się aktualizacji oprogramowania (firmware / sterowniki) urządzeń sieciowych oraz innych (np. w urządzeniach jak: routery, switche, access pointy, firewalle, macierze, dyski NAS, drukarki, skanery),
2) dokonywana jest konfiguracja urządzeń sieciowych oraz innych (routery, switche, access pointy, firewalle, macierze, drukarki, skanery) w celu zabezpieczenia przed nieuprawnionym dostępem do nich (np. zmiana domyślnych haseł na urządzeniach, zmiana domyślnych nazw kont administratora w urządzeniach, konfiguracja portów na routerze),
3) dokonuje się aktualizacji oprogramowania systemów i aplikacji (systemy operacyjne na stacjach roboczych / systemy operacyjne serwerów / przeglądarki www / Dedykowany CMS / Adobe / Flash / Java / inne).

Aktualizacja dokonywana jest zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki),

4) monitoring usług sieciowych, np.: (np. DHCP, DNS, SSH, http, telnet, FTP, SMTP, SNMP) oraz utrzymuje się niezbędne usługi oraz dezaktywuje pozostałe.

5) zastosowano system antywirusowy na serwerze i na stacjach roboczych.

6) zastosowano filtr antyspamowy.

7) stosowany jest Firewall na serwerze, na stacjach roboczych, na wirtualnym serwerze.

8) zastosowano mechanizmy kontroli dostępu do sieci w postaci: IPS/IDS - do wykrywania i blokowania ataków do sieci komputerowej.

9) sieć bezprzewodową zabezpieczono technologią WPA.

10) separacja sieci wewnętrznej od sieci przeznaczonej dla gości (dla wifi i dla Ethernet) np. w sali narad.

3. Zabezpieczenia infrastruktury IT:

1) serwer wyposażono w macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej,

2) zastosowano wirtualizację serwera,

3) zastosowano redundantny serwer,

4) dokonano dezaktywacji nieużywanych gniazd sieciowych (np. przez wypięcie przewodów lub wyłączenie portów na switchu),

5) na stacjach roboczych zastosowano „zahasłowane wygaszacze ekranu”, aktywowane po 5 minutach nieaktywności użytkownika,

6) ustawienie monitorów uniemożliwiające wgląd w dane przez osoby postronne.

4. Zabezpieczenia aplikacji:

1) zapewniono rozliczalność operacji dla pracy w kluczowych aplikacjach / bazach / serwerach plików.

2) w ramach rozliczalności logowane są operacje tworzenia, zmiany (historii zmian), usuwania rekordu, wglądu w dane, eksportu danych do plików.

3) kluczowe aplikacje/bazy z danymi osobowymi zabezpieczono przed eksportem danych do plików (np. tekstowych, .csv, .xls).

4) zabezpieczono interfejsy programistyczne poprzez zmianę domyślnych loginów i haseł / wyłączenie dostępu zdalnego, gdy nie jest wymagany.

5) szyfrowanie baz danych.

§ 10. Procedura wykonywania przeglądów i konserwacji.

1. Stosowany jest system wykrywania słabości i zagrożeń (Skanery podatności).

2. Stosowane jest oprogramowanie do inwentaryzacji infrastruktury IT / zainstalowanego oprogramowania na stacjach roboczych (serwerach) oraz do kontroli procesu aktualizacji (patche / łatki).

3. Administrator Systemów Informatycznych jest odpowiedzialny za monitoring/przegląd logów aktywności aplikacji /baz.

4. Administrator Systemów Informatycznych jest odpowiedzialny za monitoring/przegląd logów aktywności oraz uprawnień użytkowników i administratorów.

5. Administrator Systemów Informatycznych odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków, optymalizację baz danych.

6. Administrator Systemów Informatycznych odpowiada za sprawdzanie poprawności działania systemu IT, w tym: stacji roboczych, serwerów, drukarek, baz danych, aplikacji, poczty email.

7. Administrator Systemów Informatycznych odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.

8. W przypadku napraw dokonywanych na zewnątrz z komputerów należy uprzednio wymontować dyski, z urządzeń mobilnych karty pamięci, usunąć dane z nośnika z użyciem specjalistycznego oprogramowania.

9. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest zawarcie specjalnego zapisu w umowie serwisowej, gwarantującego bezpieczną naprawę (należy na to zwrócić uwagę przy zakupach sprzętu).

10. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku / karcie pamięci. Sprzęt przekazywany jest do serwisu bez podania hasła.

11. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta (umowy gwarancyjne on-site).

12. Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych) muszą być wykonywane pod nadzorem osób upoważnionych.

13. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.