Załącznik Nr 2
do Zarządzenia
Burmistrza Lubienia Kujawskiego
Nr 4/2016 z dnia 21 stycznia 2016r.

Instrukcja zarządzania systemem informatycznym w Urzędzie Miejskim w Lubieniu Kujawskim

Lubień Kujawski, 2016

SPIS TREŚCI

1. CHARAKTERYSTYKA SYSTEMU

1. W Urzędzie Miejskim w Lubieniu Kujawskim istnieje sieć informatyczna do której podłączone są serwery, komputery stacjonarne i przenośne oraz drukarki sieciowe.
2. Sygnał internetowy dostarczany jest przez usługodawcę internetowego i odpowiednio zabezpieczony.
3. System zabezpieczony jest oprogramowaniem antywirusowym zainstalowanym na każdym stanowisku.

2. OGÓLNE ZASADY PRACY W SYSTEMIE INFORMATYCZNYM

1. Administrator Bezpieczeństwa Informacji odpowiada za korygowanie niniejszej instrukcji w przypadku uzasadnionych zmian organizacyjno – funkcjonalnych w Urzędzie Miejskim w Lubieniu Kujawskim,
2. Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez dopuszczone przez Administratora Bezpieczeństwa Informacji do eksploatacji licencjonowane oprogramowanie.
3. Administrator Bezpieczeństwa Informacji prowadzi ewidencję oprogramowania.
4. Do eksploatacji dopuszcza się systemy informatyczne wyposażone w:
    a. mechanizmy kontroli dostępu umożliwiające autoryzację użytkownika, z pominięciem narzędzi do edycji tekstu,
    b. mechanizmy umożliwiające wykonanie kopii bezpieczeństwa oraz archiwizacje danych, niezbędne do przywrócenia prawidłowego działania systemu po awarii,
5. Użytkownikom zabrania się:
    a. korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami i dniami pracy bez pisemnej zgody ADO w Urzędzie Miejskim w Lubieniu Kujawskim,
    b. udostępniania stanowisk roboczych osobom nieuprawnionym,
    c. wykorzystania sieci komputerowej Urzędu Miejskiego w Lubieniu Kujawskim w celach innych niż wyznaczone przez ADO,
    d. samowolnego instalowania i używania nielicencjonowanych programów komputerowych,
    e. korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich,
    f. samowolnego aktualizaowania programów komputerowych,
    g. umożliwienia dostępu do zasobów wewnętrznej sieci informatycznej Urzędu Miejskiego w Lubieniu Kujawskim oraz sieci internetowej osobom nieuprawnionym.

3. PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

Nadawanie uprawnień

1. Administrator Systemu Informatycznego w Urzędzie Miejskim w Lubieniu Kujawskim przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego wniosku pozytywnie opiniowanego przez Administratora Bezpieczeństwa Informacji oraz zatwierdzanego przez Administratora Danych Osobowych – Burmistrza Lubienia Kujawskiego, określającego zakres uprawnień pracownika do przetwarzania danych osobowych – wg procedury wew. opisanej w dokumencie „Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Lubieniu Kujawskim.
2. Uprawnienia do przetwarzania danych osobowych są nadawane tylko i wyłącznie w zakresie wykonywanych przez pracownika zadań. Nadanie uprawnień polega na utworzeniu unikatowego identyfikatora użytkownika w systemie informatycznym.
3. Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie.
4. Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta użytkownika w przypadku np. podczas zawieszenia w pełnieniu obowiązków służbowych.
5. Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy pracownika.
6. Jeżeli zachodzi konieczność modyfikacji nadanych uprawnień do przetwarzania danych w systemie informatycznym, dokonuje niniejszego Administrator Systemów Informatycznych zgodnie z całą procedurą nadawania uprawień do przetwarzania danych osobowych określoną w Polityce bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Lubieniu Kujawskim.
7. Osoby, które zostały upoważnione do przetwarzania danych są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku pracy.
8. Ewidencja osób upoważnionych do przetwarzania danych osobowych prowadzona jest przez Administratora Bezpieczeństwa Informacji.
9. Wydane upoważnienia do przetwarzania danych osobowych w Urzędzie Miejskim w Lubieniu Kujawskim załączane są do akt osobowych pracowników Urzędu.
10. Nadzór i kontrolę nad procesem rejestracji uprawnień do przetwarzania danych osobowych w systemie informatycznym sprawuje Administrator Systemów Informatycznych w Urzędzie Miejskim w Lubieniu Kujawskim.
11. Hasło Administratora Systemu Informatycznego do zarządzania uprawnieniami w wykorzystywanych w systemach, programach, aplikacjach wykorzystywanych w Urzędzie przechowywane jest w sposób zabezpieczony przez Administratora Danych Osobowych – Burmistrza Lubienia Kujawskiego.

Osoby odpowiedzialne za nadawanie, modyfikacje, odbieranie uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemach informatycznych

1. Kontrola przestrzegania instrukcji przez pracowników Urzędu – Administrator Bezpieczeństwa Informacji w Urzędzie Miejskim w Lubieniu Kujawskim.
2. Aktualizacja instrukcji - Administrator Bezpieczeństwa Informacji w Urzędzie Miejskim w Lubieniu Kujawskim.
3. Nadawanie, rejestrowanie, modyfikacja, wyrejestrowanie uprawnień do przetwarzania danych w systemach informatycznych - Administrator Bezpieczeństwa Informacji w Urzędzie Miejskim w Lubieniu Kujawskim.

4. STOSOWANE METODY I ŚRODKI UWIERZYTELNIANIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

1. Pierwsze hasło użytkownika jest zawsze przekazywane ustnie i ustalane przez Administratora Systemów Informatycznych w Urzędzie - nadającego uprawnienie dostępu w systemie informatycznym Urzędu.
2. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora oraz pierwszego hasła oraz określeniu zakresu dostępnych danych.
3. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika Administrator Bezpieczeństwa Informacji nadaje inny identyfikator odstępując od ogólnej zasady.

Wygania dotyczące hasła:

- autoryzacja w systemie operacyjnym odbywa się za pomocą hasła, które nie powinno zawierać mniej niż 8 znaków (używane małe i duże litery, cyfry oraz znaki specjalne),
- autoryzacja w programach przetwarzających dane osobowe odbywa się za pomocą loginu i hasła, które nie powinno zawierać mniej niż 8 znaków (używane małe i duże litery, cyfry oraz znaki specjalne),
- hasło nie może być takie samo jak identyfikator,
- identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie,
- hasło mu być zmieniane przynajmniej raz w miesiącu przez użytkownika,
- użytkownikowi nie wolno zapisywać hasła na papierze,
- użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności,

- hasło przy wpisaniu nie może być wyświetlane na ekranie,
- za gospodarkę loginami odpowiedzialny jest Administrator Systemu Informatycznego w porozumieniu z Administratorem Bezpieczeństwa Informacji,
- zabronione jest stosowanie rozwiązań programowych pozwalających na zapamiętywanie identyfikatorów i haseł.

5. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY UŻYTKOWNIKÓW SYSTEMU

Procedura rozpoczęcia pracy

1. Przed rozpoczęciem pracy, w trakcie pracy oraz po jej zakończeniu należy zwrócić uwagę, czy nie występują przesłanki, mogące świadczyć o naruszeniu zasad ochrony danych osobowych.
2. Rozpoczęcie pracy pracownika w Urzędzie w systemie informatycznym obejmuje uruchomienie komputera, wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.
3. Użytkownik systemu jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system przed osobami niemającymi uprawnień.

Procedura zawieszenia pracy

1. Opuszczając stanowisko pracy (stacje roboczą komputera) użytkownik zobowiązany jest dokonać zamknięcie używanych programów służących do przetwarzania danych osobowych oraz zapisać wszystkie otwarte dokumenty.
2. W przypadku czasowego opuszczenia stanowiska pracy, po 2 minutach winien uruchomić się automatycznie wygaszacz ekranu zabezpieczający hasłem. Monitory komputerów usytuowane są w sposób uniemożliwiający odczytanie informacji z ekranu komputera osobom postronnym.

Procedura zakończenia pracy

1. Procedurę zakończenia pracy, należy rozpocząć od zamknięcia wszystkich używanych programów służących do przetwarzania danych osobowych oraz zapisać wszystkie otwarte dokumenty.
2. Użytkownik systemu nie powinien opuszczać stanowiska pracy do chwili całkowitego wyłączenia komputera.
3. Administrator Bezpieczeństwa Informacji monitoruje logowanie oraz wylogowanie się użytkowników oraz nadzoruje zakres przetwarzanych przez nich zbiorów danych.

6. PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW

1. Dane osobowe zabezpiecza się poprzez wykonywanie kopii zapasowych.
2. Ochronie poprzez wykonywanie kopii podlegają także programy i narzędzia programowe służące przetwarzaniu danych. Kopie programów i narzędzi wykonywane są zaraz po instalacji oraz po każdej aktualizacji na zewnętrznych, elektronicznych nośnikach informacji.
3. Kopie zapasowe baz danych stosowanych systemach informatycznych używanych w urzędzie sporządza systematycznie Administrator Systemów Informatycznych.
4. W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych, użytkownicy systemu Informatycznego zobowiązani są do wykonywania samodzielnego kopii bezpieczeństwa zbiorów.
5. Kopie awaryjne mogą być wykonywane tylko na nośnikach informatycznych zaakceptowanych przez Administratora Bezpieczeństwa Informacji.
6. Kopie awaryjne mogą być sporządzane automatycznie lub manualnie z wykorzystaniem specjalistycznych urządzeń do wykonywania kopii lub standardowych narzędzi oferowanych przez stacje robocze.
7. Kopie awaryjne wykonuje się nie później niż ostatniego dnia każdego miesiąca.
8. Kopie awaryjne przechowuje Administrator Danych Osobowych w zabezpieczonym miejscu, a przypadku przetwarzania danych na stacjach roboczych poszczególni użytkownicy. Kopie usuwa się niezwłocznie po ustaniu ich użyteczności.
9. Administrator Bezpieczeństwa Informacji zobowiązany jest do okresowego wykonywania testów odtworzeniowych kopii awaryjnych.
10. Wszelki wydruki zawierające dane osobowe powinny być przechowywane w miejscu uniemożliwiającym ich odczyt przez osoby nieupoważnione, zaś po upływie czasu ich przydatności – niszczone w niszczarkach dokumentów.
11. Pracownicy użytkujący przenośne komputery, w których przetwarzane są dane osobowe, zobowiązani są zachować szczególną ostrożność podczas transportu i przechowywania tego komputera. W celu zabezpieczenia ingerencji osób niepowołanych, dostęp do komputera należy zabezpieczyć hasłem i nie zezwalać na użytkowanie komputera osobom nieupoważnionym.

7. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI

1. Nośniki danych oraz programów służących do przetwarzania danych osobowych, a także danych konfiguracyjnych systemu Informatycznego, przechowuje się w odpowiednio zabezpieczonym pomieszczeniu.
2. Za zgodą Administratora Danych Osobowych dane osobowe można przetwarzać na dyskach twardych komputerów stacjonarnych lub zarejestrowanych nośnikach informacji dostarczonych przez Administratora Bezpieczeństwa Informacji.

3. Przenośne nośniki danych powinny być obowiązkowo zabezpieczone ochroną kryptograficzną.
4. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   a) **likwidacji** – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
   b) **przekazanie podmiotowi nieuprawnionemu do przetwarzania danych** pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie.
   c) **naprawy** – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie.
5. Nośniki kopii awaryjnych, które zostały wycofane z użycia podlegają zniszczeniu po usunięciu danych osobowych w odpowiednim urządzeniu niszczącym przez Administratora Bezpieczeństwa Informacji.

8. SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

Komputery służące do przetwarzania danych osobowych w Urzędzie Miejskim w Lubieniu Kujawskim posiadają dostęp do sieci publicznej, wówczas system informatyczny narażony jest na oprogramowanie, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu – zatem wprowadza się wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.

Można wyróżnić następujące rodzaje występujących zagrożeń:

- nieuprawniony dostęp bezpośrednio do baz danych;
- uszkodzeniu kodu aplikacji umożliwiającej dostęp do bazy danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu;
- przechwycenie danych z aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych przez wyspecjalizowany program szpiegowski i nielegalne przesyłanie tych danych poza miejsce przetwarzania danych;
- uszkodzenie lub zfałszowanie danych osobowych przez wirus komputerowy zakłócający pracę aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych.

W celu przeciwdziałania zagrożeniom system informatyczny powinien posiadać następujące zabezpieczenia:

- logowanie użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu;
- użytkownicy systemu pracują wyłącznie na zbiorach danych osobowych do których posiadają upoważnienie wydane przez Administratora Danych Osobowych.
- dostęp do serwerowni ma wyłącznie Administrator Systemów Informatycznych i osoby upoważnione przez Administratora Danych Osobowych.
- Administrator Systemów Informatycznych jest zobowiązany monitorować pracę w sieci WAN i LAN za pomocą dostępnego oprogramowania narzędziowego i logów.
- zabronione jest pobieranie oraz instalowanie bez nadzoru Administratora Systemu Informatycznego jakichkolwiek programów na wszystkich komputerach służących do przetwarzania danych osobowych;
- uczestnictwo w internetowych grupach dyskusyjnych dozwolone jest jedynie za zgodą Administratora Systemów Informatycznych;
- stosowanie odpowiedniej ochrony antywirusowej na stacjach roboczych wykorzystywanych dla przetwarzania danych osobowych.

Potencjalnymi źródłami przedostania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:

- załączniki do poczty elektronicznej,
- przeglądane strony internetowe,
- pliki i aplikacje pochodzące z nośników wymiennych uruchamiane i odczytywane na stacji roboczej.

Sposoby zabezpieczenia systemu informatycznego

1. W celu zapewnienia ochrony antywirusowej Administrator Systemów Informatycznych jest odpowiedzialny za zarządzanie systemem wykrywającym i usuwającym wirusy. Do ochrony antywirusowej należy stosować program antywirusowy zainstalowany na wszystkich komputerach połączony z siecią lokalną na których odbierana jest poczta elektroniczna i sprawdzane są wszystkie zewnętrzne nośniki informacji przed ich uruchomieniem w sieci.
2. Każdą przesyłkę otrzymaną za pomocą transmisji danych należy sprawdzić programem antywirusowym. W celu zapewnienia maksymalnej ochrony program antywirusowy oraz jego baza powinna być aktualizowana kilkukrotnie w ciągu dnia.
3. Użytkownicy systemu Informatycznego Urzędu mają obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.
4. Każdy pracownik przetwarzający dane osobowe przy użyciu komputera w wypadku jakichkolwiek podejrzeń dotyczących obniżenia bezpieczeństwa danych osobowych, powinien poinformować o tym fakcie Administratora Systemów Informatycznych oraz Administratora Bezpieczeństwa Informacji w Urzędzie Miejskim w Lubieniu Kujawskim.

9. PRZESYŁANIE DANYCH POZA OBSZAR PRZETWARZANIA

1. Urządzenia i nośniki zawierające dane osobowe przekazywane poza obszar przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność tych danych, w szczególności poprzez zastosowanie ochrony kryptograficznej.
2. W wypadku przesyłania danych osobowych poza sieć przystosowaną do transferu danych osobowych należy zastosować szczególne środki bezpieczeństwa, które obejmują:
   a) zatwierdzenie przez Administratora Bezpieczeństwa Informacji zakresu danych osobowych przeznaczonych do wysłania,
   b) zastosowanie mechanizmów szyfrowania danych osobowych,
   c) zastosowanie mechanizmów podpisu elektronicznego zabezpieczającego transmisje danych osobowych oraz rejestrację transmisji wysyłania danych osobowych.
3. Umożliwienie wysyłania danych osobowych tylko z wykorzystaniem określonej aplikacji i tylko przez określonych użytkowników.

10. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW INFORMATYCZNYCH

1. Przeglądy i konserwacje systemu Informatycznego oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez Administratora Danych Osobowych.
2. Wszelkie prace związane z naprawami i konserwacją systemu Informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych, w szczególności poprzez bezpośredni nadzór prowadzony przez Administratora Bezpieczeństwa Informacji.
3. W przypadku uszkodzenia zestawu komputerowego, nośniki danych, na których są przechowywane dane osobowe powinny zostać zabezpieczone przez Administratora Bezpieczeństwa Informacji.
4. W przypadku konieczności przeprowadzenia prac serwisowych poza Urzędem dane osobowe znajdujące się w naprawianym urządzeniu muszą zostać w sposób trwały usunięte.
5. Jeżeli nie ma możliwości usunięcia danych z nośnika na czas naprawy komputera, należy zapewnić stały nadzór nad tym nośnikiem przez osobę upoważnioną do przetwarzania danych osobowych na nim zgromadzonych.
6. Administrator Bezpieczeństwa Informacji wykonuje okresowe przeglądy nośników danych osobowych eliminując te, które nie zapewniają odpowiedniego poziomu bezpieczeństwa oraz niezawodności.
7. Zabronione jest dokonanie napraw sprzętu komputerowego samodzielnie przez pracowników. O wszelkich nieprawidłowościach lub awariach użytkownik systemu powinien niezwłocznie powiadomić Administratora Systemów Informatycznych.

11. PROCEDURY KORZYSTANIA Z INTRNETU I POCZTY E-MAIL W URZĘDZIE MIEJSKIM W LUBIENIU KUJAWSKIM

1. Użytkownicy systemu Informatycznego w Urzędzie zobowiązani są do powiadamiania Administratora Systemu Informatycznego o każdej nieprawidłowości użytkowania Internetu, w szczególności poczty elektronicznej.
2. Administrator Systemu Informatycznego odpowiedzialny jest za tworzenie zasad optymalizujących i monitorujących generowany ruch wychodzący i wchodzący do sieci wewnętrznej urzędu, zgłaszania prób łamania prawa, polityki bezpieczeństwa lub innych przyjętych w firmie zasad dotyczących używania Internetu.
3. Administrator Danych Osobowych decyduję, w porozumieniu z Administratorem Bezpieczeństwa Informacji, czy pracownik powinien mieć ograniczony czy nieograniczony dostęp do Internetu, lub też czy nie powinien mieć wcale dostępu do Internetu.
4. Administrator Danych Osobowych za pośrednictwem Administratora Systemów Informatycznych zastrzega sobie prawo do całkowitego monitorowania korzystania z Internetu, w szczególności korzystania ze służbowej elektronicznej skrzynki pocztowej.
5. Wszelkie informacje przechowywane na komputerach i w sieci są własnością Urzędu i nie uważa się ich za własność prywatną.
6. Niewłaściwe korzystanie z łącza internetowego może doprowadzić do wszczęcia postępowania dyscyplinarnego lub nawet zwolnienia z pracy. Ponadto, korzystanie z Internetu dla celów niezgodnych z prawem może pociągnąć użytkowników do odpowiedzialności karnej.
7. Zabrania się przeglądania, zgrywania lub ujawniania informacji dostępnych przez Internet, które uznaje się w jakikolwiek sposób za obraźliwe lub niebezpieczne dla wewnętrznych systemów informatycznych.
8. Zabrania się czerpania korzyści osobistych lub prowadzenia działalności gospodarczej wykorzystując dostęp do internetu z Urzędu Miejskiego w Lubieniu Kujawski.
9. Zabrania się przekazywania poza urząd poufnych informacji oraz łamania prawa.
10. Zabrania się zgrywania aplikacji i danych z Internetu bez poprzedniego uzyskania zgody Administratora Systemu Informatycznego.
11. Zabrania się korzystania z osobistych kont pocztowych.
12. Zabrania się nieuzasadnionego – nie związanego z wykonywanymi służbowymi obowiązkami - nadmiernego korzystania z internetu powodując tym samym niepotrzebne obciążenie łącza.
13. Administrator Danych Osobowych zastrzega sobie prawo do wglądu w pocztę elektroniczną pracowników, jeżeli są ku temu podstawy tzn. dla celów bezpieczeństwa, kiedy jest to wymagane przez prawo lub jako element śledztwa. Każdorazowy wgląd w pocztę elektroniczną pracownika musi zostać wcześniej zapowiedziany w sposób jasny i zrozumiały dla użytkownika danego konta pocztowego w Urzędzie Miejskim w Lubieniu Kujawskim.

14. Jeżeli poufne lub zastrzeżone informacje mają być wysłane pocztą elektroniczną powinny one być zakodowane (np. Skompresowane programem z założonym hasłem na plik).
15. Przychodzące wiadomości kontrolowane są automatycznie z wykorzystaniem specjalistycznego oprogramowania pod względem obecności wirusów i innej niepożądanej zawartości, która mogłaby uszkodzić systemy firmy lub w inny sposób negatywnie na nie wpłynąć lub zmniejszyć wydajność.
16. Niewłaściwe użycie poczty elektronicznej w firmie może doprowadzić do wszczęcia postępowania dyscyplinarnego, a czynności zakazane prawem są przestępstwem i mogą doprowadzić do postępowania karnego.
17. Przesyłanie informacji za pośrednictwem poczty elektronicznej winno odbywać się zgodnie z uprawnieniami adresatów do korzystania z określonego typu danych. W przypadku wątpliwości nadawca powinien sprawdzić, czy dana osoba ma uprawnienia do korzystania z dokumentów danego typu lub o określonej klauzuli poprzez skonsultowanie się z Administratorem Bezpieczeństwa Informacji.
18. Użytkownicy powinni zwrócić szczególną uwagę na poprawność adresu odbiorcy dokumentu.
19. Jeżeli istotne jest potwierdzenie otrzymania przez adresata przesyłki, użytkownik winien skorzystać, o ile jest to technicznie możliwe, z opcji systemu poczty elektronicznej informującej o dostarczeniu i otwarciu dokumentu. Dodatkowo zaleca się, aby użytkownik zawarł w treści dokumentu prośbę o potwierdzenie otrzymania i zapoznania się z informacją. Adresat zobowiązany jest w takiej sytuacji przesłać nadawcy potwierdzenie.
20. Użytkownikom zabronione jest otwieranie wiadomości e-mail od nieznanych sobie osób, których tytuł nie sugeruje związku z wypełnianymi przez nich obowiązkami służbowymi. W przypadku otrzymania takiej wiadomości, użytkownik powinien ją zniszczyć lub skontaktować się z Administratorem Bezpieczeństwa Informacji.
21. Użytkownikom zabronione jest uruchamiać wykonywalne załączniki dołączone do wiadomości przesłanych pocztą elektroniczną. W takim przypadku użytkownik powinien poinformować o zdarzeniu Administratora Bezpieczeństwa Informacji, który winien sprawdzić, czy załącznik stanowi zagrożenie dla przetwarzanych w systemie informatycznym informacji.
22. Użytkownicy nie powinni rozsyłać za pośrednictwem poczty elektronicznej informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia" itp.
23. Użytkownicy nie powinni rozsyłać, wiadomości zawierających załączniki o dużym rozmiarze dla większej liczby adresatów - określenie krytycznych rozmiarów przesyłek i krytycznej liczby adresatów jest uzależnione od wydajności systemu poczty elektronicznej
24. Użytkownicy powinni okresowo kasować niepotrzebne wiadomości pocztowe.
25. Korzystanie z poczty według uznania jest przywilejem, który może zostać w każdej chwili wycofany.
26. Imię i nazwisko użytkownika, adres i inne podobne informacje przesyłane wraz z wiadomościami rzutują na wizerunek Urzędu Miejskiego w Lubieniu Kujawskim. Użytkownicy nie mogą zmieniać, przeinaczać, ukrywać lub zamieniać się swoimi danymi identyfikacyjnymi w czasie wysyłania wiadomości.

12. POSTANOWIENIA KOŃCOWE

1. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zadaniami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie interdyscyplinarne.
2. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych.
3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być traktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa Informacji.
4. Orzeczona kara dyscyplinarna wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2014r. poz. 1182 ze zm.) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
5. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2014r., poz. 1182 ze zm.) rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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. 2004 Nr 100, poz. 1024).

BURMISTRZ
Marek Wiliński