Załącznik do zarządzenia Nr 0050.7.2019

Burmistrza Miasta Zambrów z dnia 22

stycznia 2019 r.

Regulamin ochrony danych

Rozdział 1.
Postanowienia ogólne.

§ 1. 1. Niniejszy Regulamin zawiera zasady i procedury przetwarzania danych w Urzędzie Miasta Zambrów.

2. Każdy pracownik zobligowany jest do zapoznania oraz stosowania się do Regulaminu ochrony danych. **Rozdział**

2.

Zasady bezpiecznego użytkowania sprzętu IT, dysków, programów.

§ 2. 1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety' i smartfony.

2. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.

3. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.

4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wgląd do danych wyświetlanych na monitorach komputerowych - **tzw.** Polityka czystego ekranu.

5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu bądź z programu.

6. Po zakończeniu pracy, użytkownik zobowiązany jest:

1) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy;

2) zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki, na których znajdują się dane osobowe;

3) uporządkować stanowisko pracy, dokumenty papierowe włożyć do szafki zamykanej na klucz.

Rozdział 3.
Zarządzanie uprawnieniami.

§3.1. Każdy użytkownik z dostępem do danych osobowych (np. na swoim komputerze, na dysku sieciowym, w programie lub aplikacji, w poczcie elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się.

2. Użytkownik otrzymuje dostęp i odpowiednie uprawnienia do zasobów i aplikacji na polecenie przełożonego.

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

Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła.

4. Użytkownicy nie mają prawa do samodzielnej zmiany uprawnień, np. przydzielenia sobie uprawnień administratora w Windows.

5. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest zatem umożliwianie innym osobom pracy na koncie innego użytkownika.

Rozdział 4.
Polityka haseł

§ 4. 1. Hasła powinny składać się z minimum 8 znaków.

2. Hasła powinny zawierać przynajmniej po jednym znaku: dużą literę, mała literę, cyfrę, znak specjalny.

3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych

słów, typowych zestawów: 123456, qwerty.

4. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.

5. W przypadku ujawnienia hasła - należy natychmiast go zmienić.

6. Hasła należy zmieniać co 30 dni.

7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobow iązany jest do samodzielnej zmiany hasła.

Rozdział 5.
Zabezpieczenie dokumentacji papierowej z danymi osobowymi.

§ 5. 1. Osoby przetwarzające dane osobowe są zobowiązane do stosowania tzw. „Polityki czystego biurka". Polega ona na zabezpieczaniu (zamykaniu) dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.

2. Pracownicy zobowiązani są do przechowywania na biurku tylko tych dokumentów, które są im niezbędne w danym momencie do wykonania bieżących zadań.

3. Osoby przetwarzające dane osobowe zobowiązane są do niszczenia dokumentów i wydruków w niszczarkach.

4. Zabrania się pozostawiania dokumentów zdanymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w' korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach ogólnodostępnych.

5. Po zakończonej pracy pracownik zobowiązany jest odłożyć wszystkie dokumenty do zamykanej na klucz szafy.

6. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych miejskich.

Rozdział 6.
Zasady korzystania z internetu.

§ 6. 1. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych.

2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewuadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą Administratora Systemu Informatycznego i tylko w uzasadnionych przypadkach.

3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.

4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).

5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.

6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą ''https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.

7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów.

Rozdział 7.
Zasady korzystania z poczty elektronicznej.

§7. 1. Użytkownik do celów służbowych zobowiązany jest wyłączenie do korzystania z adresu e-mail należącego do Urzędu.

2. Zabrania się wykorzystywanie innych adresów e-mail (np. wp.pl, onet.pl, gmail.com) do przesyłania poczty służbowej, jak również przekierowywania poczty służbowej na serwery z poza infrastruktury Urzędu.

3. W przypadku przesyłania danych osobowych poza Urząd należy wykorzystywać mechanizmy kryptograficzne (hasłowanie lub szyfrowanie wysyłanych dokumentów lub plików).

4. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasto należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.

5. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.

6. Nie należy otwierać załączników (plików) w mailach nawet od rzekomo znanych nam nadawców bez weryfikacji tegoż nadawcy. Tego typu maile większości przypadków zawierają załączniki ze szkodliwymi programami, które po „kliknięciu" infekują komputer użytkownika oraz często pozostałe komputery w sieci. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowaniem przez krypto wirusy.

7. Bez weryfikacji wiarygodności nadawcy, nie należy „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych.

8. Należy zgłaszać przypadki podejrzanych e-maili.

9. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości - UD W". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości"!

10. Użytkownicy powinni okresowo kasować niepotrzebne maile.

11. Mail służbowy jest przeznaczony wyłącznie do wykonywania obow iązków służbowych.

12. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych nieupoważnionych osób.

13. Pracownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.

Rozdział 8.
Ochrona antywirusowa.

§8. 1. Każdy przypadek problemu zdziałaniem programu antywirusowego powinien być zgłaszany do Administratora.

2. Użytkownicy zobow iązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym.

3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, zainstaluj program antywirusowy" bądź każdych innych niezrozumiałych bądź wzbudzających podejrzenie, użytkownik obow iązany jest poinformować niezwłocznie o tym fakcie Administratora Systemu Informatycznego.

Rozdział 9.
Zasady postępowania z kluczami do pomieszczeń służbowych.

§ 9. 1. Podstawowym środkiem zabezpieczenia budynków Urzędu oraz pomieszczeń użytkowych jest klucz do zamka.

2. Uprawnienia do pobrania klucza nadawane są pracownikowi Urzędu lub innej osobie, działającej na podstawde upoważnienia, przez umieszczenie ich danych na wykazie osób upoważnionych do pobierania klucza.

3. 1) Do każdego pomieszczenia Urzędu wymagane jest posiadanie trzech kompletów kluczy:

a) klucze użytkowe;

b) klucze zapasowe;

c) klucze rezerwowe.

2) Przechowywanie kluczy do pomieszczeń dokonywane jest zgodnie z następującymi zasadami:

a) klucze użytkowe - przechowywane są w zamykanej na klucz szafce na stanowisku ochrony;

b) klucze zapasowe - przechowywane są na stanowisku ochrony w zamkniętym pojemniku;

c) klucze rezerwowe - przechowywane i zabezpieczone są w zamkniętej metalowej szafie.

4. Wydawanie kluczy zapasowych, o których mowa w ust. 3 pkt. 2 lit. b, uprawnionym do ich pobrania pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz w przypadkach awaryjnych za zgodą Sekretarza Miasta Zambrów - za pokwitowaniem w odpowiednim rejestrze wraz z uzasadnieniem konieczności wydania kluczy.

5. Klucze zapasowe, po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu za poświadczeniem zwrotu.

6. Pracownicy przed rozpoczęciem pracy pobierają klucze do pomieszczeń służbowych z portierni (stanowisko ochrony).

7. Po otwarciu pomieszczeń biurowych, jeszcze przed przystąpieniem do pracy, pracownicy sprawdzają stan zastosowanych zabezpieczeń sprzętu biurowego i komputerowego, a także składowanej w tych pomieszczeniach dokumentacji i innego wyposażenia.

8. W przypadku stwierdzenia zmian lub naruszenia stanu zabezpieczeń, pracownik, który to stwierdził, natychmiast powiadamia swojego bezpośredniego przełożonego.

9. Od momentu pobrania kluczy do momentu ich zdania, na pracownikach spoczywa pełna odpowiedzialność za zabezpieczenie pomieszczeń biurowych w których pracują.

10. Pomieszczenie służbowe, w którym chwilowo nie przebywa żaden pracownik powinno być zamknięte na klucz.

11. Klucza nie wolno przekazywać/udostępniać innej osobie.

7. Klucze od biurek stanow iskowych, szaf biurowych są w ciągłym posiadaniu pracowników, którzy ponoszą pełną odpowiedzialność za ich zabezpieczenie.

8. Po zakończeniu pracy, wszyscy pracownicy Urzędu są zobowiązani do uporządkowania swoich stanowisk pracy, wykonania czynności zabezpieczających adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych, w szczególności: zabezpieczenia komputerów i wszelkich nośników danych, wyłączenia wszystkich urządzeń elektronicznych (nie wymagających stałego zasilania), zamknięcia szafek, okien i drzwi oraz pozostawienie kluczy do pomieszczeń służbowych w dyżurce.

9. Zabrania się wynoszenia kluczy do pomieszczeń służbowych poza siedzibę Urzędu oraz ich dorabiania.

10. Pracownik Urzędu chcąc kontynuować pracę poza normalnymi godzinami pracy, może uzyskać zgodę Burmistrza, Zastępcy Burmistrza lub Sekretarza - w ściśle uzasadnionych przypadkach.

11. Sprzątaczka dysponuje kompletem kluczy do wszystkich pomieszczeń służbowych, ponosi pełną odpowiedzialność za ich zabezpieczenie przed utratą. Klucze przechowywane są na portierni w osobnej, zabezpieczonej szafce. Sprzątaczka ponosi pełną odpowiedzialność za zamknięcie drzwi do pomieszczeń po zakończonej pracy.

12. Zgubienie klucza, przekazanie innej osobie lub utrata w jakikolwiek inny sposób może skutkować dla pracownika konsekwencjami służbowymi lub dyscyplinarnymi.

13. 1) Pomieszczeniami podlegającymi szczególnej ochronie są:

a) pomieszczenia Urzędu Stanu Cywilnego:

b) pomieszczenie serwerów ni:

c) pomieszczenia Wydziału Spraw Obywatelskich:

d) pomieszczenia archiwum zakładowego.

2) Sprzątanie pomieszczeń wyżej wymienionych odbywa się wyłącznie w godzinach pracy Urzędu w obecności pracownika upoważnionego.

14. Budynek Urzędu podlega ochronie polegającej na całodobowym monitorowaniu przez system alarmowy zainstalowany w budynku oraz na zewnątrz.

15. Budynek Urzędu monitorowany jest przez system alarmowy włączany w czasie zamknięcia Urzędu, w godzinach od 21.00 do 6.00.

16. Budynek obsługuje koncesjonowana firma ochroniarska zapewniająca stały nadzór fizyczny w godzinach od 6.00 do 21.00.

17. Otwarcia budynku Urzędu po porze nocnej oraz zamknięcia po zakończonym dniu pracy oraz załączenia systemu alarmowego dokonuje pracownik firmy ochroniarskiej.

18. Szczegółowy zakres obowiązków i ustaleń w zakresie ochrony i dozoru reguluje umowa zawarta pomiędzy Starostwem Powiatowym w Zambrowie a firmą świadczącą usługi ochroniarskie.

Rozdział 10.
Obowiązek zachowania poufności i ochrony danych.

§ 10. 1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:

1) przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach;

2) zachowania w tajemnicy danych osobowych do których posiada dostęp w związku z wykonywaniem zadań powierzonych przez Administratora danych osobowych;

3) niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora;

4) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych;

5) ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

2. Osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych.

3. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom, których tożsamości nie można zweryfikować.

4. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.

§ 11. 1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.

2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane za naruszenie przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 26 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.