Załącznik nr 2 do Zarządzenia Nr 94/2019 Wójta Gminy Stara Dąbrowa
z dnia 06 sierpnia 2019 roku

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W URZĘDZIE GMINY W STAREJ DĄBROWIE

I. WSTĘP

Administrator danych jest obowiązany zastosować takie środki techniczne i organizacyjne, które zapewnią właściwą ochronę informacji, w tym danych osobowych. W szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Wybór odpowiednich środków gwarantuje przetwarzanym danym optymalny stopień zabezpieczenia.

Niniejszy dokument jest wykazem procedur, środków organizacyjnych i technicznych, które mają na celu zabezpieczyć informacje oraz dane osobowe przed zniszczeniem, utraceniem, modyfikacją i zmianą. Ochronie ma być poddane również nieuprawnione ujawnienie danych osobowych, a także nieuprawniony dostęp do danych osobowych.

Zabezpieczenie danych odbywać się będzie na dwóch poziomach: organizacyjnym i technicznym.

II. ZABEZPIECZENIA TECHNICZNO- ORGANIZACYJNE

W jednostce wprowadzono Politykę Bezpieczeństwa Informacji (dalej PBI) oraz Regulamin Ochrony Danych Osobowych. Kierownik jednostki pisemnie upoważnił pracowników do przetwarzania danych osobowych w zbiorach elektronicznych i papierowych, w zakresie niezbędnym do wykonywania obowiązków pracowniczych. Każdy pracownik Jednostki własnoręcznym podpisem oświadczył, że zapoznał się z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz wewnętrzną dokumentacją ochrony danych osobowych. Procedury postepowania w przypadku wystąpienia incydentów dotyczących ochrony danych osobowych i bezpieczeństwa informacji opisano w PBI. Na poziomie organizacyjnym przyjęto do stosowania dla pracowników regulamin ochrony danych osobowych.

Obszar przetwarzania danych został zabezpieczony przed dostępem osób nieuprawnionych, a także utratą, uszkodzeniem lub zniszczeniem. Szczegółowy wykaz zabezpieczeń technicznych i organizacyjnych zastosowanych w jednostce został wyszczególniony w załączniku nr 5 do przyjętej polityki bezpieczeństwa informacji. W budynku funkcjonuje system przeciwpożarowy.

Wszystkie pomieszczenia jednostki (pomieszczenia administracyjne, archiwum, serwerownia) zostały zabezpieczone drzwiami zamykanymi na klucz. Dostęp do tych pomieszczeń posiadają wyłącznie osoby upoważnione. Budynek dodatkowo jest chroniony przez monitoring wizyjny, systemem alarmowym oraz zewnętrzną firmę ochroniarską. W większości przypadków dokumentacja przechowywana jest w szafkach zamykanych na klucz, dokumenty wrażliwe przechowywane są w szafach metalowych.

Dostęp do urządzeń, programów i aplikacji posiadają osoby uprawnione poprzez nadane przez Kierownika Jednostki upoważnienie, dzięki czemu ograniczono możliwość ujawniania, modyfikacji, usunięcia i zniszczenia danych przez osoby nieupoważnione.

Wyznaczono osobę odpowiedzialną za ochronę antywirusową systemu informatycznego oraz osobę odpowiedzialną za wdrażanie nowych wersji oprogramowania systemowego i użytkowego, poprawek i uzupełnień podnoszących ich bezpieczeństwo (Administrator Systemów Informatycznych).

Aktualizacja systemów operacyjnych i oprogramowania oraz urządzeń sieciowych wykonywana jest automatycznie w ramach obsługi producenckiej.

System informatyczny zabezpieczono oprogramowaniem antywirusowym, filtrem antyspamowym oraz systemem Firewall Cisco ASA 5508.

Stanowiska komputerowe rozmieszczono w sposób ograniczający dostęp osób nieupoważnionych. Część stanowisk wyposażono w UPS podtrzymujące zasilanie. Serwer i zabezpieczono urządzeniem podtrzymującym zasilanie (UPS). Inne elementy infrastruktury (klucze, gniazda sieciowe, elektryczne rozdzielnie) chronione są w zamykanych na klucz skrzynkach.

Wszystkich użytkowników zobowiązuje się do wykonywania wydruków z włączoną opcją tzw. „bezpiecznego wydruku". Na ekranach monitorów włączono opcję wygaszacza uruchamiającego się po 30 minutach nieaktywności.

III. NADAWANIE UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

Kierownik jednostki pisemnie nadaje pracownikom upoważnienia do przetwarzania danych w systemach informatycznych. Za nadanie indywidualnego identyfikatora (loginu) i hasła odpowiada wyznaczona osoba, tj. administrator systemu informatycznego (informatyk).

Administrator systemów informatycznych (ASI) jest osobą odpowiedzialną za ochronę systemu informatycznego. Kierownik jednostki wyznacza osobę zastępującą ASI. Administrator systemów jest zobowiązany do pracy bieżącej na koncie roboczym. Uprawnienia „administratora" powinny być używane tylko w sytuacjach awaryjnych, lub w przypadku wprowadzania istotnych zmian w systemie. Hasło „administratora" zdeponowane jest w wyznaczonym bezpiecznym miejscu i wydane osobie zastępującej ASI tylko w sytuacji awaryjnej.

Dostęp do komputerów i systemów informatycznych następuje po podaniu identyfikatora i hasła. Użytkownicy systemów informatycznych pracują z uprawnieniami „użytkownika". Każdy pracownik powinien pracować na własnym koncie. Nie należy umożliwiać innym osobom pracy na swoim koncie. Login po wyrejestrowaniu z systemu informatycznego nie może być nadany lub przydzielony innej osobie.

Wydane pracownikom uprawnienia podlegają regularnym przeglądom i aktualizacji. Wykaz upoważnionych osób stanowi załącznik do polityki ochrony danych osobowych.

IV. TWORZENIE KOPII ZAPASOWYCH

Procedura tworzenia kopii zapasowych określa zasady tworzenia, przechowywania i testowania kopii zapasowych oraz odzyskiwania z nich danych systemów informatycznych, w celu zapewnienia integralności i dostępności informacji oraz środków przetwarzania informacji.

Za wykonywanie kopii zapasowej danych odpowiedzialny jest Administrator systemów informatycznych (informatyk).

Kopie zapasowe sporządza się codziennie, i przechowywane jest w wyodrębnionym pomieszczeniu, do którego dostęp posiada upoważniona osoba. Kopie zapasowe przechowywane są przez 60 dni dla baz danych oraz 30 dni dla plików użytkownika.

Dla systemów informatycznych dostarczanych przez zewnętrznych usługodawców kopia zapasowa wykonywana jest automatycznie i przechowywana na serwerze udostępnionym przez dostawcę.

Niszczenie dysków z kopiami zapasowymi odbywa się komisyjnie.

V. NISZCZENIE ZEWNĘTRZNYCH NOŚNIKÓW DANYCH

Do zewnętrznych nośników danych zaliczają się: dokumentacja papierowa, twarde dyski z komputerów stacjonarnych i przenośnych, macierze dyskowe, płyty CD i DVD, dyski SSD, dyskietki, pendrive'y, telefony służbowe itp.

Wycofane z użytku, uszkodzone lub przestarzałe nośniki danych należy trwale zniszczyć. Ww. czynności należy dokonać komisyjnie i udokumentować stosownym protokołem. W przypadku jeżeli sprzęt oddaje się do zniszczenia wyspecjalizowanej firmie, czynności te należy udokumentować umową powierzenia. Podmiot wykonujący usługę powinien posiadać stosowny certyfikat.

Nośniki informacji (w szczególności twarde dyski) winny być oczyszczone zanim zostaną przekazane poza obszar jednostki w ramach sprzedaży lub darowizny.

Papierowe bazy danych oraz dokumentację należy niszczyć poprzez użycie niszczarek paskowych, a tam gdzie to niezbędne w niszczarkach o podwyższonym standardzie.

VI. WYKONYWANIE PRZEGLĄDÓW I KONSERWACJI

Do obowiązków ASI należy:

- wdrożenie odpowiedniego systemu zabezpieczającego infrastrukturę IT,
- utrzymywanie w aktualizacji infrastruktury IT,
- monitoring i przegląd: logów aktywności baz i aplikacji,
- nadawanie uprawnień użytkowników i administratorów,
- opytmalizacja serwerów, wielkość pamięci i dysków, baz danych,
- sprawdzanie poprawności działania systemu IT (stacji roboczych, drukarek, poczty e-mail),
- identyfikacja i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego, celem ich natychmiastowego usunięcia.

Jeśli naprawy sprzętu zlecane są na zewnątrz należy uprzednio wymontować dyski i nośniki, które zawierają dane. W przypadku wykonywania konserwacji i napraw przez osoby nie posiadających upoważnienia Kierownika jednostki, czynności te muszą być wykonane pod nadzorem osób upoważnionych.

Aktualizacja, konserwacja i naprawa sprzętu wykonywana zdalnie w ramach gwarancji producenckiej powinna być poprzedzona stosowną umową powierzenia. Umowa powierzenia w swoich zapisach obligatoryjnie zawiera: przedmiot; czas trwania, charakter i cel przetwarzania, a także rodzaj danych osobowych, kategorię osób, których dane dotyczą, obowiązki i prawa administratora oraz obowiązki podmiotu przetwarzającego.

VII. Regulamin używania sprzętu mobilnego poza jednostką

Regulamin dotyczy mobilnego sprzętu komputerowego, w tym zewnętrznych nośników danych, zawierających dane osobowe oraz tajemnicę administratora. Pracownicy bez uprzedniej zgody przełożonego mają zakaz wynoszenia poza obszar jednostki sprzętu mobilnego. Użytkownicy sprzętu mobilnego wynoszonego za pozwoleniem poza obszar jednostki, są zobowiązani do przestrzegania zasad bezpieczeństwa:

- przetwarzanie danych osobowych na sprzęcie mobilnym poza obszarem jednostki musi być ograniczone do niezbędnych przypadków,
- sprzęt mobilny wynoszony poza obszar jednostki musi być zaszyfrowany, a służbowe telefony zabezpieczone mechanizmem uwierzytelniania. Sprzęt mobilny powinien być wyposażony w oprogramowanie umożliwiające jego nadzór, blokowanie dostępu oraz czyszczenie zawartości,
- jeśli na urządzeniach przenośnych lub mobilnych uzyskujemy zdalny dostęp do zasobów wewnętrznej sieci przez Internet, należy zastosować szyfrowanie tego połączenia z użyciem VPN (poprzez użycie hasła lub autoryzację adresu IP),
- użytkownik sprzętu mobilnego poza jednostką musi zachować szczególną ostrożność, tj.: transport w odpowiedniej torbie; nie pozostawianie sprzętu w samochodzie lub przechowalni bagażu,
- użytkując sprzęt mobilny w miejscach publicznych i środkach transportu, użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych,
- sprzęt mobilny należy użytkować w sposób minimalizujący ryzyko dostępu do przetwarzanych danych przez osoby nieupoważnione,
- sprzęt mobilny w biurze po zakończeniu pracy zaleca się umieszczać w zamykanych szafkach na klucz,
- użytkownik sprzętu mobilnego jest zobowiązany do regularnego tworzenia kopii zapasowej danych. Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych,
- kradzież lub zagubienie sprzętu mobilnego należy natychmiast zgłosić przełożonemu, ASI lub Inspektorowi Ochrony Danych,
- zabezpieczenia sprzętu mobilnego wprowadza ASI na wniosek użytkownika.