Zarządzenie Nr 4/2021
Dyrektora
samorządowego zakładu budżetowego
Zakładu Gospodarki Komunalnej i Mieszkaniowej w Okonku
z dnia 22 kwietnia 2021r.

w sprawie ustalenia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zakładzie Gospodarki Komunalnej i Mieszkaniowej w Okonku ze szczególnym uwzględnieniem bezpieczeństwa informacji

Na podstawie art. 5 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 zarządza się co następuje:

§ 1. Wprowadza się instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zakładzie Gospodarki Komunalnej i Mieszkaniowej w Okonku ze szczególnym uwzględnieniem bezpieczeństwa informacji, stanowiący załącznik nr 1 do niniejszego zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
ZGKiM w Okonku
mgr Paweł Cackowski

Załącznik nr 1
do Zarządzenia Nr 4/2021
Dyrektora
Zakładu Gospodarki Komunalnej i Mieszkaniowej w Okonku
z dnia 22 kwietnia 2021r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zakładzie Gospodarki Komunalnej i Mieszkaniowej w Okonku ze szczególnym uwzględnieniem bezpieczeństwa informacji

Postanowienia ogólne

§ 1

1. Niniejsza Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej Instrukcją, przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych Zakładu Gospodarki Komunalnej i Mieszkaniowej w Okonku przetwarzane są w sposób zgodny z przepisami prawa mającymi zastosowanie do takiej czynności, zgodnie z zasadą art. 5 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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.
2. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (dalej jako „Instrukcja"), zawiera w szczególności:
   1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
   2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
   3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
   4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
   5) sposób, miejsce i okres przechowywania:
      a) elektronicznych nośników informacji zawierających dane osobowe,
      b) kopii zapasowych,
   6) sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania;
   7) sposób odnotowania udostępnienia danych osobowych innym podmiotom;
   8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych.

3. Instrukcję opracowano na podstawie:
   1) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych,
   2) Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024),
   3) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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.
4. Wdrożenie Instrukcji nastąpi poprzez zapoznanie użytkowników z jej tekstem, przeprowadzenie przez osobę upoważnioną przez Administratora Danych Osobowych szkolenia wśród użytkowników oraz udostępnienie tekstu Instrukcji w pomieszczeniach w których będą przetwarzane dane osobowe.

§ 2

Instrukcja powyższa powinna być interpretowana i odczytywana w zgodzie z postanowieniami Polityki Bezpieczeństwa Danych Osobowych w Zakładzie Gospodarki Komunalnej i Mieszkaniowej w Okonku (dalej: „Polityka"). Wszystkie terminy i pojęcia nie zdefiniowane odrębnie w Instrukcji należy odczytywać w znaczeniu jakie nadano im w Polityce.

§ 3

System informatyczny służący do przetwarzania danych osobowych stanowią komputery osobiste, z systemem operacyjnym Microsoft Windows 10, połączone z siecią Internet

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

§ 4

1. Osobą odpowiedzialną za nadawanie uprawnień poszczególnym użytkownikom systemu informatycznego, modyfikację tych uprawnień, ich cofnięcie oraz wykonywanie wszelkich czynności związanych z w/w funkcjami jest Administrator.
2. Administrator ma prawo powierzenia czynności technicznych osobie zatrudnionej do obsługi systemu informatycznego lub wykonującej tego rodzaju usługi na rzecz Administratora (Osoba Odpowiedzialna).
3. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie wydane przez Administratora.

§ 5

1. Nadanie uprawnienia obejmuje:
a) przypisanie użytkownikowi identyfikatora (login) do przypisanego urządzenia,
b) utworzenie konta użytkownika,
c) przypisanie użytkownikowi identyfikatora (login) do stosowanego oprogramowania, w którym przetwarzane są dane osobowe, w tym dane wrażliwe.
2. Osoba która uzyskała upoważnienie do przetwarzania danych osobowych otrzyma indywidualny identyfikator użytkownika, a następnie dla tego identyfikatora zostanie utworzone konto użytkownika. Czynności powyższe zostaną wykonane po sprawdzeniu prawdziwości okazanego w tym celu pisemnego upoważnienia do przetwarzania danych osobowych.
3. Dla każdego Użytkownika Systemu informatycznego ustalony jest odrębny identyfikator i hasło.
4. Identyfikator Użytkownika nie może być zmieniany, a po wyrejestrowaniu Użytkownika z systemu informatycznego nie może być przydzielony innej osobie.
5. Zakazuje się przekazywania haseł poprzez osoby trzecie lub przy użyciu metod, które nie gwarantują zachowania jego poufności oraz niezaprzeczalnego ustalenia nadawcy i odbiorcy hasła, np. przez niechronione wiadomości przekazywane elektronicznie.
6. Administrator dokonuje rejestracji i prowadzi wykaz loginów przydzielonych poszczególnym Użytkownikom, który wiąże loginy z imiennie wskazanymi pracownikami.
7. Użytkownikom nadawane są uprawnienia do prac tylko w modułach i funkcjach programu wymaganych dla realizacji powierzonych im zadań.
8. Administrator oraz każdy, kto poweźmie wiadomość o cofnięciu użytkownikowi upoważnienia do przetwarzania danych osobowych obowiązany jest poinformować o tym fakcie Osobę Odpowiedzialną, która usunie konto użytkownika.
9. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, zostaje niezwłocznie wyrejestrowany z systemu informatycznego, w którym są przetwarzane, zaś hasło dostępu zostaje unieważnione oraz zostają podjęte inne działania niezbędne w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 6

1. Dostęp do systemu informatycznego przez poszczególnych użytkowników będzie możliwy wyłącznie po zalogowaniu się do utworzonego konta użytkownika, co nastąpi po wprowadzeniu

przypisanego im hasła.

2. Hasło do konta użytkownika będzie składało się z min. 8 znaków i będzie tworzone przez osobę upoważnioną przez Administratora Danych.
3. Hasło Użytkownika:
   a) musi się składać co najmniej z 8 znaków, w tym zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
   b) nie może zawierać znaków następujących po sobie na klawiaturze bądź tych samych liter lub cyfr,
   c) nie może zawierać imion, nazwisk, przezwisk, inicjałów, dat, numerów rejestracyjnych samochodów, numerów telefonów i innych kombinacji znaków mogących doprowadzić do łatwego rozszyfrowania go przez osoby nieupoważnione,
   d) nie może być zapisywane w systemie w postaci jawnej,
   e) nie może być wyświetlane na ekranie komputera w sposób jawny,
   f) nie może być ujawnione innej osobie, nawet po upływie ich ważności,
   g) musi być zabezpieczone przez Użytkownika przed nieuprawnionym dostępem osób trzecich;
4. Hasło do konta użytkownika będzie przekazywane temu użytkownikowi na piśmie.
5. Po otrzymaniu hasła, użytkownik zobowiązany będzie do zalogowania się do systemu i dokonania niezwłocznej zmiany otrzymanego hasła na własne, składające się z co najmniej 8 znaków.
6. Użytkownik będzie zobowiązany do zmiany hasła nie rzadziej niż raz na 30 dni. Zmiana dokonywana będzie ręcznie.
7. Zabronione jest posługiwanie się identyfikatorem lub hasłem innego Użytkownika.
8. Osoba Odpowiedzialna pełni funkcję administratora systemu, posiadającego uprawnienie do tworzenia i usuwania kont użytkowników. Operacje te będzie mogła wykonać przy wykorzystaniu własnego konta, które będzie miało charakter uprzywilejowany. Hasło do tego konta będzie znane wyłącznie Osobie Odpowiedzialnej, nie będzie ono przechowywane w systemie informatycznym.
9. Dla każdej osoby, której dane osobowe są przetwarzane w Systemie informatycznym, system zapewnia odnotowanie:
   a) daty pierwszego wprowadzenia danych do systemu,
   b) identyfikatora Użytkownika wprowadzającego dane osobowe do systemu,
   c) źródła danych (w przypadku zbierania danych nie od osoby, której dane dotyczą),
   d) informacji o odbiorcach, którym dane osobowe zostały udostępnione,
   e) sprzeciwu.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

§ 7

1. Wszelkie urządzenie zawierające dane osobowe muszą być zabezpieczone przed nieuprawnionym dostępem poprzez wykorzystanie szyfrowania dysku twardego lub inny sposób szyfrowania i ochrony dostępu do danych.
2. Minimalne środki ochrony to:
   a) zainstalowanie na stacjach roboczych zapory sieciowej firewall i oprogramowania antywirusowego,
   b) wdrożenie systemu aktualizacji systemu operacyjnego oraz jego składników,
   c) wymaganie podania hasła przed uzyskaniem dostępu do systemu operacyjnego,
   d) niepozostawianie niezablokowanych stacji roboczej bez nadzoru,
   e) praca z wykorzystaniem konta nieposiadającego uprawnień administracyjnych.
3. Użytkownik jest zobowiązany do stałego monitorowania komunikatów pochodzących z oprogramowania antywirusowego zainstalowanego na stacji roboczej oraz na urządzeniach mobilnych i reagowania na nie.

§ 8

1. Pracownik przed uruchomieniem sprzętu komputerowego zobowiązany jest do sprawdzenia, czy nie zostały do niego podłączone żadne niezidentyfikowane urządzenia.
2. Przy logowaniu się do systemu informatycznego użytkownik obowiązany jest do zachowania środków ostrożności, wykluczających uzyskanie informacji o identyfikatorze oraz haśle użytkownika przez osoby trzecie.
3. W razie konieczności czasowego zaprzestania pracy przy stanowisku użytkownika, zobowiązany jest on do zakończenia pracy wszelkich programów komputerowych za pomocą których przetwarzane są dane osobowe, zamknięcia wszelkich plików zawierających dane osobowe oraz wylogowania się z konta użytkownika celem uniemożliwienia dostępu do danych osobie nieuprawnionej.
4. Każdy Użytkownik zobowiązany jest do stosowania wygaszacza ekranu zabezpieczonego hasłem oraz wylogowania się z systemu lub jego blokowania przy każdorazowym opuszczeniu miejsca pracy. Zablokowanie komputera odbywa się poprzez naciśnięcie kombinacji klawiszy. Niezależnie od tego wygaszacz ekranu powinien aktywować się nie później niż w 10 minucie bezczynności Użytkownika. Odblokowanie odbywa się poprzez ponowne zalogowanie się tego samego Użytkownika.
5. Zakończenie pracy w systemie polega na wybraniu odpowiedniego polecenia systemowego. Zaleca się wyłączenie wszystkich programów i zapisanie otwartych plików. Użytkownik powinien pozostać przy komputerze do chwili zamknięta systemu.
6. Użytkownik kończący pracę powinien sprawdzić czy wszelkie nośniki elektroniczne lub wydruki i dokumenty zawierające dane osobowe zostały odpowiednio zabezpieczone przez dostępem osób nieupoważnionych.
7. Osoba opuszczająca pomieszczenie, w którym przetwarzane są dane osobowe, zobowiązana jest do zamknięcia okien oraz drzwi na klucz.
8. W sytuacji podejrzenia naruszenia bezpieczeństwa systemu, użytkownik zobowiązany jest powiadomić o tym fakcie Osobę Odpowiedzialną oraz zaprzestać dalszego przetwarzania danych do momentu wyjaśnienia sprawy. W tym celu powinien podjąć czynności opisane w ustępie poprzedzającym.
9. Za naruszenie bezpieczeństwa systemu uważa się w szczególności brak możliwości zalogowania na konto użytkownika, stwierdzenie ingerencji w przetwarzane dane osobowe, użytkowane narzędzie programowe lub sprzętowe.

Procedury
tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

§ 8

1. W celu zabezpieczenia danych osobowych przed ich utratą lub zniszczeniem będą tworzone kopie zapasowe:
   a) danych osobowych,
   b) programów i narzędzi programowych służących do przetwarzania danych osobowych (dalej Kopie Programowe).
2. Kopie danych osobowych będą tworzone metodą przyrostową/całościową, poprzez wykonywanie z użyciem narzędzi systemowych MS Windows oraz systemu Ferro Backup i macierzy QNAP.
3. Kopie zapasowe danych osobowych będą wykonywane nie rzadziej niż raz na miesiąc. Wykonanie kopii zapasowych będzie wykonywać się automatycznie w powtarzalnych cyklach.

Sposób, miejsce i okres przechowywania nośników danych zawierających dane osobowe oraz kopii zapasowych

§ 9

1. Nośniki danych z kopiami archiwalnymi powinny być zabezpieczone przed dostępem do nich osób nieupoważnionych, przez zniszczeniem oraz kradzieżą.
2. Nośniki z danymi zarchiwizowanymi nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są bieżąco używane.
3. Nośniki informacji, kopie zapasowe, które nie są przeznaczone do udostępnienia, przechowuje się w sposób uniemożliwiający dostęp do niech osobom nieupoważnionym.
4. Niszczenie nośników wykonuje Osoba Odpowiedzialna. Po wykonaniu wymienionych czynności Osoba Odpowiedzialna zobowiązana jest do przygotowania odpowiedniego protokołu z ww. czynności i przekazania jej Administratorowi.

Sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania.

§ 10

1. Możliwymi źródłami przedostania się szkodliwego oprogramowania do systemu informatycznego są:
   a) sieć publiczna – Internet,
   b) oprogramowanie instalowane przez użytkowników,
   c) przenośne nośniki danych podłączane przez użytkowników do komputerów tworzących system informatyczny.
2. W celu ochrony systemu informatycznego przed szkodliwym oprogramowaniem pochodzącym z sieci publicznej – Internet, na komputerach na których przetwarzane będą dane osobowe zainstalowane zostanie oprogramowanie antywirusowe ESET NOD32 Antywirus.
3. Oprogramowanie antywirusowe jest instalowane na wszystkich stanowiskach komputerowych oraz urządzeniach mobilnych i elektronicznych nośnikach informacji.
4. W celu ochrony systemu informatycznego przed szkodliwym oprogramowaniem pochodzącym z oprogramowania instalowanego przez użytkowników, użytkownicy nie będą uprawnieni do samodzielnego instalowania oprogramowania. Wszelkie programy komputerowe niezbędne do przetwarzania danych osobowych i funkcjonowania systemu informatycznego zostaną dostarczone przez Administratora i zainstalowane przez wyznaczone do tego osoby.
5. W celu ochrony systemu informatycznego przed szkodliwym oprogramowaniem pochodzącym z przenośnych nośników danych podłączanych przez użytkowników do komputerów tworzących system informatyczny, użytkownik zobowiązany jest dokonać skanowania nośnika programem antywirusowym.
6. W przypadku wykrycia niebezpieczeństwa przez użytkownika, zobowiązany jest on do, o ile to możliwe, zaprzestania korzystania z używanego sprzętu i poinformowanie Osoby Odpowiedzialnej w celu podjęcia odpowiednich działań.
7. Pracownicy mogą korzystać z poczty elektronicznej w celach służbowych oraz w celach prywatnych w zakresie ograniczonym swoimi obowiązkami.
8. Administrator może poznawać treść wiadomości elektronicznych wykorzystywanych przez pracowników znajdujących się we wszystkich systemach Administratora.
9. Zabronione jest otwieranie wiadomości e-mail pochodzących od nieznanego nadawcy bądź z podejrzanym tytułem (tzw. phishing e-mail). W szczególności zabronione jest otwieranie linków bądź pobieranie plików zapisanych w komunikacji zewnętrznej od nieznanego nadawcy.

Cadu

Odnotowanie udostępniania danych osobowych innym podmiotom

§ 11

1. W celu udostępnienia danych osobowych innym podmiotom, tworzona będzie kopia plików programu, w którym przetwarzane są dane osobowe, opatrzona datą i zawierająca opis podmiotu, któremu dane osobowe będą udostępnione.
2. Plik będzie chroniony przed dostępem, dokonaniem w nim zmian lub usunięciem poprzez jego zaszyfrowanie za pomocą oprogramowania 7Zip.
3. Hasło umożliwiające dokonywanie operacji na w/w plikach będzie przekazywane odbiorcom danych drogą elektroniczną, na uzgodniony adres e-mail.
4. Informacje o odbiorcach danych zapisywane będą w systemie informatycznym, z którego nastąpiło udostępnienie.
5. Informacja o odbiorcach danych będzie zawierała datę i zakres udostępnienia oraz szczegółowe określenie danych odbiorcy.
6. System informatyczny zapewni możliwość sporządzenia i wydrukowania raportu zawierające, w powszechnie zrozumiałej formie, powyżej wskazane informacje.

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

§ 12

1. W razie wystąpienia takiej potrzeby, lecz nie rzadziej niż raz na rok, Osoba Odpowiedzialna za przegląd przestrzegania instrukcji zarządzania systemem informatycznym, dokonuje przeglądu i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych.
2. W przypadku wykrycia podczas przeglądu i konserwacji nieprawidłowości w działaniu sprzętu lub programów służących do przetwarzania danych osobowych, Administrator zobowiązany jest do zapewnienia ich niezwłocznego usunięcia. Przegląd i konserwacja mogą zostać zlecone pracownikowi lub podmiotowi zewnętrznemu wyspecjalizowanemu w tego rodzaju działaniach.
3. Osoba odpowiedzialna za usunięcie wykrytych nieprawidłowości jest zobowiązana do niezwłocznego sporządzenia protokołu z podjętych działań oraz poinformowania Administratora o ww. czynnościach.
4. W wypadku przekazania sprzętu lub nośników informacji służących do przetwarzania danych osobowych podmiotowi trzeciemu, pozbawia się je zapisanych danych osobowych w sposób, który uniemożliwi ich odtworzenie.
5. W przypadku zlecenia podmiotowi zewnętrznemu przeglądów kontrolnych, serwisu sprzętu i oprogramowania, powinno to zostać zlecone wyspecjalizowanej firmie serwisowej, z którą zostały zawarte umowy zawierające postanowienia zobowiązujące je do przestrzegania zasad poufności informacji uzyskanych w ramach wykonywanych zadań.
6. Przy dokonywaniu serwisu należy przestrzegać następujących zasad:
   a) czynności serwisowe powinny być wykonywane w obecności osoby upoważnionej do przetwarzania danych,
   b) przed rozpoczęciem tych czynności dane i programy znajdujące się w systemie powinny zostać zabezpieczone przed ich zniszczeniem, skopiowaniem lub niewłaściwą zmianą,
   c) prace serwisowe należy ewidencjonować w książce zawierającej rodzaj wykonywanych czynności serwisowych, daty rozpoczęcia i zakończenia usługi, odnotowanie osób dokonujących czynności serwisowych, tj. imienia i nazwiska, a także osób uczestniczących w pracach serwisowych,
   d) w przypadku prac serwisowych dokonywanych przez podmiot zewnętrzny, wymagających dostępu do danych osobowych, z podmiotem takim powinny zostać zawarte stosowne umowy powierzenia danych osobowych.

Postanowienia końcowe

§ 13

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do zapoznania się z treścią niniejszej Instrukcji. Każda z osób upoważnionych do przetwarzania Danych obowiązana będzie złożyć pisemne oświadczenie o zapoznaniu się z treścią Instrukcji, najpóźniej w momencie otrzymania upoważnienia. Każdy upoważniony będzie mógł zgłaszać wątpliwości lub pytania co do treści lub interpretacji postanowień Instrukcji, które rozpoznawane będą przez Administratora.
2. Wykonanie powyższych zobowiązań pracownik zobowiązany jest potwierdzić własnoręcznym podpisem.

DYREKTOR
ZGKiM w Okonku
mgr Paweł Cackowski