ZARZĄDZENIE NR 109/2022
BURMISTRZA MIASTA ŻARÓW

z dnia 4 lipca 2022 r.

w sprawie instrukcji użytkowania systemu informatycznego w Urządzie Miejskim w Żarowie

Na podstawie art. 24 ust. 1 i 2 Rozporządzenia Ogólnego 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 (Dz. U. UE. L. z 2016 r. Nr 119, str. 1; zm.: Dz. U. UE. L. z 2018 r. Nr 127, str. 2 oraz z 2021 r. Nr 74, str. 35) zarządzam, co następuje:

§ 1. Wprowadzam Instrukcję Zarządzania systemem informatycznym w Urzędzie Miejskim w Żarowie, stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Zobowiązuję wszystkich pracowników do zapoznania się z treścią i przestrzegania zapisów niniejszego zarządzenia.

§ 3. Wykonanie zarządzenia powierzam informatykowi urzędu.

Załącznik do Zarządzenia nr 109/2022
z dnia 4 lipca 2022 roku
w sprawie: instrukcji użytkowania systemu informatycznego
w Urządzie Miejskim w Żarowie

INSTRUKCJA UŻYTKOWANIA SYSTEMU INFORMATYCZNEGO W URZĘDZIE MIEJSKIM W ŻAROWIE

1. Wprowadzenie

Tworzy się niniejszy dokument o nazwie Instrukcja Zarządzania Systemem Informatycznym (zwany dalej „Instrukcją") w Urzędzie Miejskim w Żarowie, której celem jest ustanowienie zasad zarządzania systemem informatycznym, w którym przetwarzane są dane osobowe, jak również warunków organizacyjnych i technicznych, jakie spełniać powinny, wchodzące w jego skład urządzenia, biorąc pod uwagę skalę zagrożeń i kategorie danych objęte ochroną.

Przestrzeganie zasad instrukcji ma na celu zapewnienie bezpieczeństwa przetwarzanych danych osobowych w Urzędzie Miejskim w Żarowie, rozumianego jako zapewnienie: poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.

Opis wymagań organizacyjno – technicznych służących ochronie danych osobowych w systemach informatycznych wprowadzone zostały zarządzeniem Burmistrza Miasta Żarów nr 119/2018.

2. Podstawa prawna

§ 1

Rozporządzenie 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; DZ.U.UE.L.2016.119.1.; dalej: Rozporządzenie RODO).

2.1. Definicje

§ 2

Użyte w niniejszej dokumentacji przetwarzania danych osobowych definicje i pojęcia są wspólne dla wszystkich dokumentów powiązanych z niniejszą dokumentacją. Ilekroć w niniejszej polityce/instrukcji użytkowania systemu informatycznego jest mowa o:

1. **Administratorze danych (ADO)** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W niniejszej dokumentacji przetwarzania danych osobowych przez Administratora danych rozumie się Burmistrza Miasta Żarów dalej zwanego „Administratorem";
2. **Systemie informatycznym** - należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
3. **Danych osobowych** – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
4. **Integralności** - należy przez to rozumieć zapewnienie, że dane nie zostały zmienione, zniszczone lub uszkodzone w sposób nieuprawniony;
5. **Poufności** - należy przez to rozumieć zapewnienie, że informacja nie jest udostępniana lub ujawniana podmiotom nieuprawnionym;
6. **Dostępności** - należy przez to rozumieć zapewnienie, że dane są możliwe do wykorzystania zawsze, gdy podmiot uprawniony tego potrzebuje;
7. **Rozliczalności** - należy przez to rozumieć zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
8. **Użytkowniku systemu** – rozumie się przez to osobę upoważnioną do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym;

9. **Administratorze systemów informatycznych (ASI)** – rozumie się przez to osobę wyznaczoną przez Administratora, która odpowiada za zapewnienie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych, w których przetwarzane są dane osobowe.

2.2. Zakres stosowania

§ 3

Niniejsza instrukcja znajduje zastosowanie do systemów informatycznych, stosowanych w Urzędzie Miejskim w Żarowie, w których przetwarzane są dane osobowe, a w szczególności określa:

a) zasady dotyczące bezpieczeństwa systemów informatycznych;

b) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w Systemie Informatycznym;

c) metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;

d) procedury rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników Systemu;

e) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;

f) sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych;

g) zarządzanie bezpieczeństwem sieci;

h) sposób zabezpieczenia Systemu Informatycznego przed działalnością wirusów komputerowych, nieuprawnionym dostępem;

i) sposoby realizacji w Systemie wymogów dotyczących przetwarzania danych;

j) procedury wykonywania przeglądów i konserwacji Systemu oraz nośników informacji służących do przetwarzania danych.

Przyjęta instrukcja przez Administratora do stosowania, stanowi obowiązujący wszystkich pracowników i współpracowników dokument.

3. Bezpieczeństwo systemów informatycznych

§ 4

3.1. Wymagania bezpieczeństwa

1. Bezpieczeństwo powinno być integralną częścią systemów informatycznych służących do przetwarzania danych osobowych.
2. Aplikacje oraz usługi, które nie są wykorzystywane powinny być wyłączone.
3. Krytyczne poprawki bezpieczeństwa powinny być przetestowane i zainstalowane przez Administratora systemu lub automatycznie przez system.
4. Dostęp do poszczególnych usług systemów informatycznych powinien być zabezpieczony za pomocą kontroli dostępu.
5. Wymagania bezpieczeństwa, na które mogą się również składać wymagania prawne związane z ochroną danych osobowych, należy identyfikować i uzgodnić przed opracowaniem i/lub ich wdrożeniem. W szczególności wymagania muszą być zidentyfikowane dla:
   a) systemów operacyjnych;
   b) aplikacji;
   c) poszczególnych usług;
   d) narzędzi programowych;

e) baz danych;

f) infrastruktury teleinformatycznej;

6. Aplikacje przeglądarkowe przed wdrożeniem powinny zostać poddane przeglądowi bezpieczeństwa mającemu na celu zidentyfikowanie podatności na zagrożenia pochodzące z sieci Internet.

3.2. Zarządzanie systemami informatycznymi

§ 5

1. Administratorzy systemu informatycznego powinni zarządzać systemami operacyjnymi, bazodanowymi, urządzeniami sieciowymi korzystając ze specjalnych kont administracyjnych, służących jedynie wykonywaniu obowiązków Administratora systemów informatycznych.
2. Administratorzy powinni odnotowywać w prowadzonych rejestrach systemów wszystkie ważne zdarzenia związane z zarządzanym systemem, w szczególności:
3. zmiany, np. instalacja nowego oprogramowania;
4. fakty wejścia do serwerowni osób trzecich;
5. okresowe testy i konserwacje;
6. incydenty bezpieczeństwa (awarie sprzętu, błędy oprogramowania, naruszenia bezpieczeństwa, zdarzenia losowe, ataki szkodliwego oprogramowania) i sposób ich obsługi;
7. fakty audytowania i kontroli.

3.3. Szkolenia

§ 6

Użytkownicy systemu powinni odbywać okresowe szkolenia, odpowiednio do potrzeb wynikających ze zmian w systemie informatycznym (np. wymiana sprzętu na nowszej generacji, zmiana oprogramowania), a także w związku ze zmianą przepisów prawa o ochronie danych osobowych lub zmianą wewnętrznych regulacji lub na wniosek bezpośredniego przełożonego.

4. Procedury dotyczące uprawnień do systemów przetwarzających dane osobowe

§ 7

Zasady przyznawania użytkownikowi systemu informatycznego uprawnień, jak również zasady związane z nadawaniem, modyfikacją lub usuwaniem uprawnień dostępu użytkownika do zasobów systemu informatycznego. Dodatkowo zasady administrowania systemem informatycznym w przypadkach awaryjnych oraz wskazanie osoby/osób odpowiedzialnych za realizację procedur dotyczących uprawnień.

§ 8

1. Uprawnienia do systemu informatycznego nadawane są w oparciu o następujące zasady:

   a) **Minimalnych przywilejów** – każdy użytkownik posiada prawa dostępu do zasobów ograniczone wyłącznie do tych, które są niezbędne do wykonywania powierzonych mu obowiązków;

   b) **Wiedzy koniecznej** – pracownicy posiadają wiedzę o zasobach ograniczoną wyłącznie do zagadnień, które są niezbędne do realizacji powierzonych im zadań;

   c) Domniemanej odmowy – wszystkie działania, które nie są jawnie dozwolone są zabronione.

2. Uprawnienia dostępowe do systemów informatycznych Administratora mogą posiadać, w zależności od wykonywanych czynności służbowych lub umownych:

a) pracownicy Administratora w zakresie niezbędnym do właściwego wykonywania obowiązków służbowych;

b) osoby, przy pomocy których Administrator wykonuje swoje czynności, w szczególności:

   a) osoby zatrudnione na podstawie umowy cywilnoprawnej;

   b) pracownicy lub osoby działające w imieniu podmiotu zewnętrznego świadczącego usługi na rzecz administratora danych;

   c) stażyści, na podstawie umowy z Urzędem Pracy;

3. Każdy zarejestrowany użytkownik korzysta z przydzielonego mu konta użytkownika, opatrzonego identyfikatorem (login) i hasłem dostępu.

4. Aby zapewnić zasadę rozliczalności wynikającą z rozporządzenia ogólnego każdy użytkownik systemu informatycznego jest jednoznacznie identyfikowany poprzez nadany mu indywidualny identyfikator (login) użytkownika.

5. Zabronione jest korzystanie z tego samego identyfikatora (loginu) przez więcej niż jednego użytkownika.

6. Uprawnienia są nadawane wyłącznie w zakresie wynikającym z zajmowanego stanowiska i potrzeby wykonywania obowiązków służbowych na danym stanowisku pracy.

7. Użytkownikowi systemu informatycznego zostaje nadany dostęp po:

   a) zapoznaniu z przepisami dotyczącymi ochrony danych osobowych,

   b) zapoznaniu się z niniejszą Dokumentacją przetwarzania danych osobowych,

   c) otrzymaniu upoważnienia do przetwarzania danych osobowych.

8. Administrator Danych Osobowych lub osoba upoważniona przez Administratora ma obowiązek prowadzenia rejestru osób upoważnionych do korzystania z systemów informatycznych zgodnie z załącznikiem nr 1 do Instrukcji Zarządzania Systemem Informatycznym - Rejestr Uprawnień do systemów Informatycznych.

9. Rejestr, o którym mowa powyżej prowadzony jest w postaci elektronicznej lub papierowej.

10. Administrator Danych Osobowych lub osoba upoważniona przez Administratora raz na 30 dni dokonuje przeglądu stanu aktywności kont użytkowników.

4.1. Procedura nadawania i modyfikacji uprawnień

§ 9

1. Pracownik lub bezpośredni przełożony pracownika zobowiązany jest do złożenia wniosku o nadanie lub modyfikację uprawnień do systemu informatycznego określającego poszczególne zasoby, do których użytkownik ma otrzymać uprawnienia. *Wzór stanowi załącznik nr 2 do Instrukcji Zarządzania Systemem Informatycznym* (*Załącznik nr 2 - Wniosek o nadanie modyfikację odebranie uprawnień*).

   Wniosek może być złożony w wersji papierowej lub elektronicznej.

2. Wniosek przekazywany jest do Administratora celem akceptacji.

3. Jeśli wniosek zostanie zaakceptowany, Administrator lub osoba upoważniona przez Administratora (np. ASI) nadaje użytkownikowi odpowiednie uprawnienia.

4. W przypadku nadania uprawnień wymagających logowania, Administrator lub osoba upoważniona przez Administratora przekazuje użytkownikowi informację zawierającą wymienione z nazwy systemy informatyczne, do których użytkownik otrzymał dostęp oraz login i hasło na potrzeby pierwszego logowania.

4.2. Procedura odebrania uprawnień

§ 10

1. Bezpośredni przełożony pracownika jest zobowiązany do złożenia wniosku o odebranie uprawnień do systemu informatycznego określającego, do jakiego zasobu uprawnienia mają zostać odebrane. *Wzór stanowi załącznik nr 2 do Instrukcji Zarządzania Systemem Informatycznym (Załącznik nr 2 – Wniosek o nadanie modyfikację odebranie uprawnień)*. Wniosek może być złożony w wersji papierowej lub elektronicznej.
2. Terminami obowiązującymi przy składaniu wniosku są w szczególności:
   a) w przypadku ustania stosunku pracy – wniosek odbierający wszystkie uprawnienia – natychmiast, najpóźniej ostatniego dnia pracy zatrudnionego;
   b) długotrwałe zwolnienie lekarskie – wniosek odbierający wszystkie uprawnienia – natychmiast po upływie 30 (trzydziestu) dni kalendarzowych zwolnienia lekarskiego;
   c) zmiana stanowiska pracy – wniosek odbierający część uprawnień – natychmiast, najpóźniej ostatniego dnia pracy przed zmianą stanowiska na stanowisko wymagające zmniejszenia uprawnień;
   d) ograniczenie zakresu danych, do których pracownik miał dostęp.
3. Po wypełnieniu powyższych wymagań wniosek powinien zostać przekazany do Administratora Danych Osobowych lub Administratora Systemu Informatycznego.
4. Administrator Danych Osobowych lub ASI bezzwłocznie realizuje otrzymany wniosek oraz aktualizuje rejestr osób uprawnionych.

4.3. Konto uprzywilejowane

§ 11

1. Nadawane przywileje, czyli większe uprawnienia niż wynika to z realizowanych zadań użytkownika podlegają ścisłej ewidencji prowadzonej przez Administratora Danych Osobowych, Administratora Systemu Informatycznego lub osobę upoważnioną przez Administratora.
2. Konta użytkownika uprzywilejowanego należy oznaczyć, zapewnić ich łatwą identyfikację oraz zapewnić, że odwołują się do jednego użytkowania.
3. Konto uprzywilejowane nie może służyć do realizacji przez użytkownika standardowych zadań.
4. Czynności wykonywane za pomocą kont uprzywilejowanych należy rejestrować oraz zapewnić możliwości ich identyfikacji i rozliczalności.
5. Przywileje podlegają cofnięciu niezwłocznie po ustaniu potrzeby uzasadniającej ich nadanie.
6. Konta uprzywilejowane podlegają regularnym przeglądom i kontroli.

4.4. Zasady postępowania z hasłami administracyjnymi

§ 12

1. W stosunku do haseł administracyjnych stosuje się zaostrzone standardy bezpieczeństwa. Szczególna ochrona dotyczy haseł:
   a) administracyjnych do systemów, aplikacji, baz danych;
   b) do zarządzania urządzeniami sieci teleinformatycznej (switch, router, firewall);
   c) wykorzystywanych do szyfrowania danych.

2. Do przechowywania haseł zapisanych w formie papierowej stosuje się wyłącznie koperty, które uniemożliwiają otwarcie bez uszkodzenia ich struktury, tzw. koperty bezpieczne.
3. Koperty z hasłami administracyjnymi przechowuje się w miejscu zapewniającym dostęp tylko osobom upoważnionym.
4. Koperty z hasłami administracyjnymi podlegają ścisłej ewidencji prowadzonej przez Administratora Danych Osobowych, Administratora Systemu Informatycznego lub osobę upoważnioną przez Administratora.
5. Ewidencja haseł administracyjnych prowadzona jest w formie rejestru w formie papierowej lub elektronicznej, który zawiera;
   a) numer ewidencyjny;
   b) oznaczenie przynależności hasła administracyjnego zawartego w kopercie (nazwa systemu, zasobu, komputera);
   c) imię i nazwisko, pełnioną funkcję osoby składającej kopertę (właściciela hasła);
   d) datę złożenia koperty;
   e) imię i nazwisko osoby przyjmującej kopertę na przechowanie;
   f) datę wygaśnięcia ważności hasła zawartego w kopercie;
   g) adnotację o wydaniu koperty z hasłem (użyciu awaryjnym).
6. Dane umieszczone na bezpiecznej kopercie zawierają:
   a) numer koperty adekwatny do numeru ewidencyjnego podanego w rejestrze haseł;
   b) oznaczenie przynależności hasła administracyjnego zawartego w kopercie (nazwa systemu, zasobu, komputera);
   c) imię i nazwisko, pełnioną funkcję osoby składającej kopertę (właściciela hasła);
   d) datę złożenia koperty z hasłem;
   e) imię i nazwisko osoby przyjmującej kopertę na przechowanie;
   f) datę wygaśnięcia ważności hasła zawartego w kopercie;
   g) adnotację o wydaniu koperty z hasłem.
7. Za aktualność przechowywanych haseł odpowiedzialny jest Administrator Danych Osobowych, Administrator systemu Informatycznego lub osoba upoważniona przez Administratora.
8. Awaryjne otwarcie bezpiecznej koperty oraz pobranie kopii hasła znajdującego się w kopercie wymaga uprzedniej akceptacji Administratora lub osoby przez niego upoważnionej i jest udokumentowane w ewidencji kopert.
9. Po użyciu, hasło ulega zniszczeniu, a w to miejsce jest generowane nowe hasło, którego kopia jest przechowywana na identycznych zasadach jak w przypadku zniszczonego hasła.

5. Metody oraz środki uwierzytelniana

§ 13

Zasady przydzielania haseł oraz wymogi dotyczące stopnia ich złożoności jak również wskazanie osób odpowiedzialnych za przydział haseł.

5.1. Zasady ogólne

§ 14

1. Dostęp do danych osobowych przetwarzanych w systemie informatycznym odbywa się na podstawie uwierzytelnienia, poprzez podanie indywidualnej nazwy (identyfikatora/loginu) i hasła Użytkownika;
2. Identyfikator (login) Użytkownika jednoznaczne określa osobę, która się nim posługuje.
3. Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.
4. Użytkownik ponosi pełną odpowiedzialność za tworzone hasła (poza pierwszym hasłem do systemu nadawanego przez administratora) i jego przechowywanie.
5. Osoba będąca Administratorem systemu informatycznego powinna posiadać dodatkowo konto służące tylko i wyłącznie do administracji danym systemem informatycznym zwane kontem administracyjnym, o ile dany system udostępnia taką funkcjonalność.
6. W przypadku stwierdzenia ujawnienia klucza osobie nieupoważnionej lub podejrzenia jego ujawnienia, należy bezzwłocznie powiadomić Administratora Danych Osobowych, Administratora Systemu Informatycznego oraz Inspektora Ochrony Danych.

5.2. Zasady tworzenia i używania haseł

§ 15

Każdy użytkownik posiadający dostęp do systemów informatycznych Administratora przetwarzających dane osobowe jest zobowiązany do:

a) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie informatycznym;

b) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia oraz poinformowania o tym Administratora Systemu Informatycznego;

c) niezwłocznej zmiany hasła tymczasowego służącego do pierwszego logowania, przekazanego przez Administratora Systemu Informatycznego;

d) stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację małych i dużych liter oraz cyfr lub znaków specjalnych;

e) stosowania haseł nie posiadających w swojej strukturze części loginu,

f) zmiany wykorzystywanych haseł nie rzadziej niż raz na 30 dni lub w momencie żądania przez wykorzystywany w pracy system informatyczny.

§ 16

1. Hasła zachowują swoją poufność również po ustaniu ich użyteczności.
2. Zabronione jest:

a) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób;

b) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.;

c) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach;

d) udostępnianie haseł innym użytkownikom;

e) przeprowadzanie prób łamania haseł;

f) stosowanie rozwiązań programowych pozwalających na zapamiętywanie identyfikatorów i haseł.

§ 17

1. Obowiązkiem Administratora Systemu Informatycznego jest skonfigurowanie systemu w taki sposób, aby próby dostępu do tego systemu były limitowane zarówno w ujęciu ilościowym, jak i czasowym jeżeli tylko system umożliwia wymienioną konfigurację.
2. W przypadku, gdy system umożliwia limitowanie wprowadzenia błędnego hasła, konto użytkownika powinno zostać zablokowane po 3ciej nieudanej próbie logowania.
3. Wskazane jest ograniczenie możliwości wielokrotnego logowania, gdzie użytkownik loguje się na kilku komputerach równocześnie wykorzystując ten sam identyfikator.
4. W przypadku zablokowania dostępu do systemu informatycznego fakt ten należy zgłosić do administratora systemu w celu odblokowania konta.

5.3. Zasady zabezpieczania haseł

§ 18

1. Haseł nie powinno się przechowywać w systemach, aplikacjach, bazach danych, skryptach i plikach konfiguracyjnych w postaci jawnej, nie zapewniającej im poufności.
2. Haseł nie powinno się przesyłać za pomocną narzędzi i usług teleinformatycznych w postaci jawnej, nie zapewniającej im poufności.
3. Należy stosować bezpieczną procedurę przekazywania haseł użytkownikom np. nieprzesyłanie haseł przez sieć (np. w niechronionych wiadomościach poczty elektronicznej).
4. Zabronione jest przechwytywanie lub odgadywaniem haseł innych użytkowników.
5. Hasła należy utrzymywać w tajemnicy również po upływie ich ważności.
6. Zabronione jest wpisywanie haseł „na stałe” (np. w skryptach logowania) oraz wykorzystywania opcji auto zapamiętywania haseł (np. w przeglądarkach internetowych).

5.4. Klucze kryptograficzne

§ 19

1. W przypadku transmisji danych osobowych wrażliwych lub informacji poufnych Administratora zaleca się wykorzystywanie kluczy kryptograficznych służących do zabezpieczenia danych.
2. Za generowanie, przechowywanie i bezpieczną dystrybucję kluczy kryptograficznych odpowiada Administrator Danych Osobowych lub osoba upoważniona przez Administratora.
3. Obowiązkiem użytkownika jest zabezpieczenie kluczy (prywatnych) przed dostępem osób nieupoważnionych.
4. W przypadku stwierdzenia ujawnienia klucza osobie nieupoważnionej lub podejrzenia jego ujawnienia, należy bezzwłocznie powiadomić Administratora Danych Osobowych, Administratora Systemu Informatycznego oraz Inspektora Ochrony Danych.
5. Dane osobowe wrażliwe lub informacje poufne Administratora, w przypadku których nie stosuje się kluczy kryptograficznych, należy przesyłać wyłącznie pocztą elektroniczną po zabezpieczeniu pliku hasłem. Hasło przekazywane jest odbiorcy innym kanałem dystrybucyjnym.
6. Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania w sposób uniemożliwiający utratę lub dostęp osób niepowołanych.

6. Zarządzanie bezpieczeństwem sieci

6.1. Podstawowe zasady

§ 20

1. Należy zapewnić, by infrastruktura sieciowa była właściwie chroniona, adekwatnie do zagrożeń mogących powodować utratę bezpieczeństwa przetwarzania danych osobowych.
2. Dane osobowe przesyłane poprzez publiczną sieć telekomunikacyjną powinny być zabezpieczone środkami kryptograficznej ochrony.
3. Administrator Systemu Informatycznego systemu powinien chronić system przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, poprzez:
   a) kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną;
   b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.
4. Wewnętrzna adresacja IP, konfiguracja oraz informacja o systemach powiązanych nie powinna być ujawniana osobom nieuprawnionym bez akceptacji ze strony uprawnionej do tego celu osoby.
5. Podłączanie do infrastruktury sieciowej nieautoryzowanych lub niesprawdzonych przez ASI urządzeń takich jak modemy, urządzenia sieciowe, w tym urządzenia sieci bezprzewodowych jest zabronione.

6.2. Polityka dotycząca korzystania z usług sieciowych

§ 21

1. Użytkownikom należy zapewnić dostęp tylko do tych usług infrastruktury teleinformatycznej (np. dostęp do Internetu, zdalny dostęp, poczta elektroniczna) do których zostali autoryzowani.
2. Należy zapewnić, by osoby nie będące pracownikami nie posiadały nieautoryzowanego i niekontrolowanego dostępu do infrastruktury teleinformatycznej.
3. Należy zapewnić, by niezabezpieczone usługi infrastruktury teleinformatycznej, pozwalające przesyłać hasła w postaci niezabezpieczonej np. telnet lub ftp, nie były wykorzystywane i były zablokowane.

6.3. Bezpieczeństwo sieci bezprzewodowych

§ 22

1. Sieci bezprzewodowe podłączone do infrastruktury teleinformatycznej powinny być autoryzowane, udokumentowane, monitorowane oraz odpowiednio zabezpieczone.
2. Wszystkie urządzenia sieci bezprzewodowych, do których podłączane są systemy informatyczne powinny być zatwierdzone lub sprawdzone przez Administratora Bezpieczeństwa Informacji lub Administratora Systemu Informatycznego.

7. Procedury rozpoczęcia, zawieszenia i zakończenia pracy

§ 23

Czynności, jakie należy wykonać w celu uruchomienia systemu informatycznego oraz zasady postępowania użytkowników podczas przeprowadzania procesu uwierzytelniania się (logowania się do systemu). Procedury obejmują:

a) sposób postępowania w sytuacji tymczasowego zaprzestania pracy na skutek opuszczenia stanowiska pracy;

b) sposób postępowania w sytuacji, kiedy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba;

c) sposób postępowania w sytuacji podejrzenia naruszenia bezpieczeństwa systemu, np. w razie braku możliwości zalogowania się użytkownika na jego konto czy też w sytuacji stwierdzenia fizycznej ingerencji w przetwarzane dane bądź użytkowane narzędzia programowe lub sprzętowe.

§ 24

1. Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest sprawdzić urządzenie komputerowe i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
2. Rozpoczęcie pracy w systemie informatycznym następuje po wprowadzeniu unikalnego identyfikatora i hasła.
3. Zawieszenie pracy w systemie informatycznym tzn. brak wykonywania jakichkolwiek czynności przez okres 10 minut w systemie informatycznym powoduje automatycznie uruchomienie systemowego wygaszacza ekranu blokowanego hasłem. Uruchomienie wygaszacza ekranu wiąże się z koniecznością ponownego zalogowania, celem wznowienia pracy stacji roboczej. Zastosowanie powyższego mechanizmu nie zwalnia użytkownika z obowiązku każdorazowego blokowania ekranu wygaszaczem chronionym hasłem po odejściu od stanowiska (Windows + L lub Ctrl+Alt+Delete).
4. Przed zakończeniem pracy należy zweryfikować czy dane zostały zapisane, aby uniknąć ich utraty.
5. Po zakończeniu pracy, użytkownik obowiązany jest wylogować się z systemu informatycznego przetwarzającego dane osobowe i z systemu operacyjnego, zabezpieczyć nośniki informacji (elektroniczne i papierowe) oraz wyłączyć komputer.
6. W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.
7. Użytkownik systemu informatycznego przetwarzającego dane osobowe ma obowiązek niezwłocznie powiadomić administratora systemu w przypadku, gdy:
   a) wygląd systemu, sposób jego działania, zakres danych lub sposób ich przedstawienia przez system informatyczny odbiega od standardowego stanu uznawanego za typowy dla danego systemu informatycznego;
   b) niektóre opcje, dostępne użytkownikowi w normalnej sytuacji, przestały być dostępne lub też opcje niedostępne użytkownikowi w normalnej sytuacji, stały się dostępne.

7.1. Zasady korzystania ze służbowej poczty elektronicznej

§ 25

1. Informacja o służbowym adresie skrzynki pocztowej jest jawna i dostępna powszechnie oraz w tym może być dostępna na łamach witryny internetowej Administratora Danych Osobowych.
2. Konto e-mail służy wyłącznie do realizacji celów służbowych lub umownych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych Administratora Danych Osobowych może podlegać rejestrowaniu i monitorowaniu. Informacje przesyłane za pośrednictwem sieci (w tym do i z Internetu) nie stanowią własności prywatnej użytkownika.
3. Użytkownicy dokonujący wysyłki korespondencji masowej poza organizację, obowiązani są do ukrywania odbiorów w kopii (pole UDW).
4. Zabronione jest:
   a) wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu);

b) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi administratora danych;

c) odbieranie przesyłek z nieznanych źródeł;

d) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;

e) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe, plików multimedialnych oraz plików graficznych;

f) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika;

g) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem; w przypadku otrzymania takiej wiadomości należy przesłać ją administratorowi systemu informatycznego;

h) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;

i) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb administratora danych lub do poszukiwania dodatkowego zatrudnienia.

7.2. Korzystanie z sieci internet

§ 26

1. Sieć, w której pracują urządzenia komputerowe oraz działają systemy informatyczne Administratora musi być odseparowana od sieci publicznej zaporą ogniową (firewall) lub urządzeniem typu UTM.
2. Systemy informatyczne przetwarzające dane osobowe powinny korzystać z szyfrowanych protokołów wymiany danych np. Https.
3. Dostęp użytkowników do sieci publicznej powinien być ograniczony do niezbędnego minimum na danym stanowisku pracy.
4. Dalsze ograniczenia dostępu do sieci Internet mogą być rekomendowane przez Inspektora Ochrony Danych.
5. System informatyczny (system operacyjny) musi być zabezpieczony oprogramowaniem antywirusowym.

7.3. Zasady postępowania z nośnikami elektronicznymi i sprzętem komputerowym podczas pracy poza obszarem przetwarzania danych

§ 27

Każdy użytkownik wymiennych nośników elektronicznych ponosi całkowitą odpowiedzialność za powierzony do użytkowania sprzęt oraz jest zobowiązany do stosowania się do poniższych zasad:

1. Zabrania się pozostawiania bez opieki w miejscach publicznych nośników wymiennych przetwarzających informacje Administratora.
2. Obowiązkiem Administratora Danych Osobowych lub Administratora Systemu Informatycznego jest stosowanie szyfrowania dysków twardych oraz nośników wymiennych w celu zabezpieczenia przed wyciekiem danych osobowych.
3. Komputery przenośne należy przewozić jako bagaż podręczny i w miarę możliwości je maskować.

4. Użytkownik wykonując czynności zawodowe lub umowne w domu powinien zadbać o należyte zabezpieczenie powierzonego sprzętu oraz dostępu do informacji przed nieautoryzowanym dostępem osób trzecich.
5. Zabrania się spożywania posiłków i picia podczas pracy z powierzonym sprzętem.
6. Zabrania się udostępniania osobom trzecim nośników elektronicznych informacji oraz powierzonego sprzętu będącego własnością Administratora.
7. W przypadku utraty nośnika elektronicznego lub sprzętu komputerowego należy ten fakt bezzwłocznie zgłosić do Administratora Danych Osobowych, Administratora systemu Informatycznego lub Inspektora Ochrony Danych.
8. Problemy wynikające z nieprawidłowego funkcjonowania sprzętu komputerowego należy zgłaszać Administratorowi Systemu Informatycznego.

8. Procedury tworzenia kopii zapasowych

§ 28

Metody i częstotliwość tworzenia kopii zapasowych danych oraz kopii zapasowych systemu informatycznego używanego do ich przetwarzania. Procedury obejmują również:

a) określenie, dla jakich danych wykonywane będą kopie zapasowe, typ nośników, na których będą one wykonywane oraz narzędzia programowe i urządzenia, które mają być do tego celu wykorzystywane;
b) harmonogram wykonywania kopii zapasowych dla poszczególnych zbiorów danych wraz ze wskazaniem odpowiedniej metody sporządzania kopii.

8.1. Zasady ogólne

§ 29

1. Kopie zapasowe systemów, baz danych i dokumentów użytkowanych przez Administratora służą do zapewnienia możliwości odtworzenia w przypadku utraty aktualnie użytkowanych danych i/lub konfiguracji systemów i aplikacji. Kopia zapasowa może dotyczyć zarówno pliku, jak również baz danych oraz obrazu całego systemu.
2. Osobą odpowiedzialną za tworzenie kopii jest Administrator Systemów Informatycznych.
3. Tworzenie kopii odbywa się zgodnie z procedurą tworzenia i odtwarzania kopii zapasowych i podlega rejestracji zgodnie z załącznikiem nr 3 do Instrukcji Zarządzania Systemem Informatycznym (*Załącznik nr 3 – Rejestr tworzenia kopii*). Rejestr prowadzony jest w postaci papierowej lub elektronicznej.
4. Miejsce przechowywania kopii jest zabezpieczone przed nieuprawnionym dostępem oraz skutkami zdarzeń takich, jak pożar, zalanie, oddziaływanie silnego pola elektromagnetycznego, promieniowanie, zanieczyszczenie środowiska na takim poziomie, jak jest zabezpieczony system, z którego kopia zapasowa została wykonana.

8.2. Zasady tworzenia kopii bezpieczeństwa

§ 30

1. Zbiory danych oraz oprogramowanie znajdujące się na komputerach Administratora jak również bazy danych oraz systemy znajdujące się na serwerach Administratora i podwykonawców powinny być zabezpieczone w postaci cyklicznie wykonywanych kopii bezpieczeństwa.
2. Kopie bezpieczeństwa należy wykonywać:

a) przed dokonaniem zmian w konfiguracji systemów operacyjnych lub oprogramowania (w przypadku systemów wirtualnych wykonywanie punktu przywracania systemu);

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

c) kopie plików na urządzeniach końcowych zgodnie z określonym przez Administratora harmonogramem czasowym.

3. Kopie bezpieczeństwa należy:

a) wykonać w co najmniej jednym egzemplarzu;

b) przechowywać w innym miejscu niż te, w którym zbiory eksploatowane są na bieżąco (co najmniej w innej strefie pożarowej).

c) Daną kopię bezpieczeństwa należy przechowywać do momentu wykonania następnej kopii bezpieczeństwa.

8.3. Okres przechowywania kopii bezpieczeństwa

§ 31

Okres przechowywania kopi bezpieczeństwa zawierających dane osobowe powinien być ustalony przez Administratora i przekazany do Administratora Systemu Informatycznego odpowiedzialnego za wykonywanie kopii zapasowych.

8.4. Zabezpieczanie kopii bezpieczeństwa

§ 32

1. Kopie bezpieczeństwa należy odpowiednio zabezpieczyć przed nieuprawnionym dostępem, nadużyciem lub uszkodzeniem.
2. Należy zapewnić aby dostęp do kopii bezpieczeństwa był zgodny z nadanymi i autoryzowanymi uprawnieniami.
3. Należy zapewnić aby procedury niszczenia kopii bezpieczeństwa były zgodne z obowiązującymi regulacjami i przepisami prawa.

8.5. Użytkowanie sprzętu komputerowego, oprogramowania, nośników danych

§ 33

1. Do sprzętu komputerowego zalicza się między innymi:

a) komputery stacjonarne,

b) komputery przenośne (notebooki),

c) urządzenie mobilne np. tablety, smartphony

d) drukarki,

e) sprzęt sieciowy np. switch, router,

f) sprzęt serwerowy, monitory,

g) osprzęt dostarczony razem z wyżej wymienionym sprzętem lub zakupiony oddzielnie, a w szczególności: zasilacze, torby, klawiatury, myszki komputerowe.

2. Administrator Danych Osobowych, Administrator Systemu Informatycznego lub osoba upoważniona przez Administratora odpowiada za poprawne działanie sprzętu komputerowego. Czynność tą Administrator Danych Osobowych, Administrator Systemu Informatycznego może wykonywać poprzez pracowników lub współpracowników Administratora lub poprzez podmioty zewnętrzne.
3. Administrator Danych Osobowych lubAdministrator Systemu Informatycznego odpowiedzialny jest za przygotowanie sprzętu komputerowego do prawidłowej i zgodnej z przeznaczeniem pracy.

4. Administrator Danych Osobowych lub ASI jest zobowiązany do prowadzenia ewidencji posiadanego sprzętu komputerowego oraz oprogramowania wraz z dostarczoną dokumentacją.
5. Administrator Danych Osobowych lub ASI ma obowiązek przechowywać karty gwarancyjne oraz klucze i licencje do oprogramowania.
6. Administrator udziela pomocy użytkownikowi w obsłudze sprzętu i oprogramowania.
7. Administrator lub Administrator Systemu Informatycznego ma prawo instalować wyłącznie licencjonowane oprogramowanie lub oprogramowanie, które nie wymaga opłaty licencyjnej, zgodnie z warunkami licencji.
8. Użytkownik jest zobowiązany do dbałości o sprzęt oraz oprogramowanie, a także odpowiedzialny jest za zabezpieczenie go przed używaniem przez osoby nieuprawnione oraz do ochrony przed kradzieżą lub zagubieniem.
9. Użytkownik nie może samodzielnie zmieniać konfiguracji przekazanego sprzętu komputerowego oraz instalować lub usuwać oprogramowania, w tym nie może używać na przekazanym sprzęcie prywatnego oprogramowania. Zalecane jest aby użytkownik nie posiadał uprawnień administracyjnych na komputerze.
10. Użytkownik nie może udostępniać powierzonego mu sprzętu służbowego, w szczególności urządzeń mobilnych, osobom trzecim.

8.6. Procedura zdalnego dostępu do systemów informatycznych

§ 34

Możliwości zdalnego dostępu do systemów informatycznych administratora, którego celem może być świadczenie usługi wsparcia technicznego lub utrzymania systemu informatycznego.

Do nawiązywania zdalnych połączeń administracyjnych lub użytkowników umożliwiających zdalną pracę muszą być stosowane:

a) rozwiązania komunikacyjne bazujące na bezpiecznych standardach komunikacji zapewniające szyfrowanie transmisji;
b) użytkownik systemu musi zezwolić na autoryzacje zdalnego połączenia poprzez podanie id sesji oraz hasła dostępowego;
c) użytkownik inicjujący zdalne połączenie zobowiązany jest nadzorować proces zdalnego połączenia;
d) po zakończeniu pracy zdalnej sesja musi zostać zamknięta;
e) pracownicy korzystający z tzw. zdalnej pracy, mogą korzystać tylko i wyłącznie z rozwiązań zaakceptowanych i nadzorowanych przez Administratora Systemu Informatycznego.

8.7. Zabezpieczenie systemu informatycznego przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej

§ 35

Wszystkie urządzenia informatyczne (komputery, serwery, urządzenia sieciowe), na których zainstalowane jest oprogramowanie służące do przetwarzania danych osobowych, powinny być zasilane z wydzielonej sieci oraz zabezpieczone przed krótkotrwałymi zanikami napięcia, przepięciami itp., przy pomocy zasilaczy awaryjnych (UPS). Minimalny czas podtrzymania zasilania za pomocą zasilaczy awaryjnych nie może być krótszy niż 15 minut. W przypadku urządzeń serwerowych zalecany czas podtrzymania to min. 2 godziny.

9. Sposób zabezpieczania systemu informatycznego przed działalnością szkodliwego oprogramowania

§ 36

Sposób zabezpieczenia systemów informatycznych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu mającego wpływ na integralność, poufność i dostępność danych. Procedury obejmują również:

a) zdefiniowane źródła przedostania sie szkodliwego oprogramowania do systemu oraz działania, jakie należy

podejmować, aby minimalizować możliwość jego zainstalowania się;

b) zastosowane narzędzia programowe, których zadaniem jest przeciwdziałanie skutkom szkodliwego oprogramowania;

c) metody i częstotliwość aktualizacji definicji wirusów oraz osoby odpowiedzialne za zarządzanie oprogramowaniem antywirusowym;

d) sposób postępowania użytkowników na okoliczność zidentyfikowania zagrożeń.

9.1. Ochrona przed szkodliwym oprogramowaniem

§ 37

1. Systemy informatyczne należy chronić przed szkodliwym oprogramowaniem (np. wirusy, trojany, bomby logiczne, robaki) poprzez stosowanie odpowiednich środków technicznych i organizacyjnych

2. Zidentyfikowanymi obszarami systemów informatycznych Administratora narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są dyski twarde lub karty pamięci urządzeń, elektroniczne nośniki informacji, dostęp do sieci publicznej, poczta e-mail.

3. Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, sieć lokalna lub elektroniczne nośniki informacji.

4. Stacje robocze, komputery przenośne, serwery muszą być objęte ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego oraz zapory (firewall), zapewniających integralność zasobów przechowywanych i przetwarzanych w systemie informatycznym Administratora.

5. Oprogramowanie antywirusowe uruchamiane jest przy starcie systemu, a użytkownik nie posiada uprawnień do jego wyłączenia. Możliwość zatrzymania usługi systemu antywirusowego posiada jedynie Administrator lub ASI.

6. Konfiguracja programu antywirusowego zapewnia ciągłe monitorowanie otrzymywanych i wysyłanych, a także uruchamianych plików pod kątem występowania oprogramowania złośliwego.

7. System antywirusowy musi posiadać możliwość automatycznego skanowania każdego zewnętrznego elektronicznego nośnika informacji, który jest podłączany do urządzenia komputerowego.

8. W przypadku stwierdzenia pojawienia się wirusa i braku możliwości usunięcia go przez program antywirusowy, użytkownik powinien skontaktować się z administratorem systemu.

9. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez msystemm antywirusowy,m ASI podejmuje działania zmierzające do musunięcia zagrożenia.

W szczególności działania te mogą obejmować: usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego;

a) odtworzenie plików z kopii zapasowych, po uprzednim sprawdzeniu, czy dane zapisane na kopiach zapasowych nie są zainfekowane;

b) samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z odpowiednim serwisem.

10. Procedura usuwania awarii sprzętu lub oprogramowania

§ 38

1. W przypadku wystąpienia awarii Systemu Informatycznego pracownik lub współpracownik, który ją stwierdził zobowiązany jest do zgłoszenia faktu wystąpienia awarii administratorowi danych, Administratorowi Systemu Informatycznego lub osobie odpowiedzialnej za obsługę informatyczną.

2. Administrator danych lub osoba odpowiedzialna za obsługę informatyczną zobowiązany jest do niezwłocznego podjęcia czynności zmierzających do usunięcia awarii np. poprzez wezwanie serwisu.

3. Po usunięciu awarii administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do:

a) uruchomienia Systemu Informatycznego;

b) kontroli poprawności jego funkcjonowania;

c) kontroli integralności danych.

4. W przypadku stwierdzenia uszkodzenia danych zgromadzonych w Systemie, administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do otworzenia danych z ostatniej posiadanej kopii bezpieczeństwa (backup).

5. W przypadku gdy usunięcie awarii wymaga przekazania sprzętu komputerowego na zewnątrz, przed przekazaniem tego sprzętu administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do usunięcia z dysków twardych wszystkich danych, po ich uprzednim skopiowaniu na inny nośnik. Jeśli z przyczyn technicznych jest to niemożliwe, osoba przekazująca sprzęt ze strony Kancelarii zobowiązana jest uzyskać od serwisanta protokół przyjęcia danych i zobowiązanie do zachowania ich poufności.

11. Sposób realizacji wymogów odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione

§ 39

Dla każdej osoby, której dane osobowe przetwarzane są w systemie informatycznym, system ten powinien zapewnić odnotowanie informacji o udostępnieniach danych odbiorcom, w rozumieniu art. 4 pkt 9 rozporządzenia ogólnego, zawierające informacje komu, kiedy i w jakim zakresie dane osobowe zostały udostępnione.

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

§ 40

1. Cel, zakres, częstotliwość oraz procedury wykonywania przeglądów i konserwacji sprzętu informatycznego oraz podmioty i osoby do tego uprawnione. Procedury obejmują również:

   a) sposób nadzoru nad osobami spoza organizacji wykonującymi czynności konserwacyjne systemu; tryb przekazywania sprzętu komputerowego do naprawy lub zniszczenia.Konserwacja i naprawa sprzętu komputerowego, systemów informatycznych oraz nośników informacji Administratora ma na celu zapewnienie nieprzerwanej i bezpiecznej pracy tych systemów, zapobieganie utraty, uszkodzenia lub naruszenia bezpieczeństwa.

2. Sprzęt podlega konserwacji według ustalonego planu, wynikającego z zaleceń producentów.

3. Naprawy oraz konserwacje urządzeń komputerowych oraz zmiany w systemie informatycznym Administratora przeprowadzane są – o ile to możliwe – przez upoważnionych pracowników Administratora lub upoważnione firmy zewnętrzne.

4. Naprawy, konserwacje i zmiany w systemie informatycznym Administratora przeprowadzane przez serwisanta zewnętrznego prowadzone są pod nadzorem Administratora Danych Osobowych, Administratora Systemu Informatycznego lub osoby upoważnionej przez Administratora w siedzibie Administratora (jeśli to możliwe) lub poza siedzibą Administratora, po uprzednim usunięciu elementów zawierających dane osobowe, o ile nie wiąże się to z nadmiernymi utrudnieniami.

5. Wszelkie prace, o których mowa powyżej, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie pomiędzy Administratorem a tymże podmiotem, z uwzględnieniem klauzuli powierzenia przetwarzania danych lub klauzuli dotyczącej zachowania w poufności przez wykonawcę wszelkich informacji, do których ma dostęp w czasie wykonywania usługi.

6. W przypadku zdalnej obsługi serwisowej systemów informatycznych Administratora, porty komunikacyjne powinny być włączane jedynie na wyraźne żądanie dostawcy takich usług, za zgodą Administratora systemu informatycznego i muszą być ponownie odłączone tuż po zakończeniu prac serwisowych.

7. Jeśli nośnik danych (dysk, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie zgodnie z procedurami Administratora.

13. Postanowienia końcowe

§ 41

1. Dokumentacja/instrukcja użytkowania systemu informatycznego stanowi wewnętrzną regulację Administratora i obowiązuje wszystkich pracowników i współpracowników Administratora.
2. Dokumentacja/instrukcja użytkowania systemu informatycznego obowiązuje od dnia jej wprowadzenia w życie w sposób przyjęty u Administratora. Wszelkie zmiany Dokumentacji/instrukcji użytkowania systemu informatycznego obowiązują od dnia ich wprowadzenia w życie w sposób przyjęty u Administratora.
3. Każdy kto przetwarza dane posiadane przez Administratora zobowiązany jest do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Dokumentacji/instrukcji użytkowania systemu informatycznego.
4. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.
5. W sprawach nieuregulowanych w niniejszej instrukcji mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy rozporządzenia RODO.

REJESTR UPRAWNIEŃ DO SYSTEMÓW INFORMATYCZNYCH						
lp.	Imię i nazwisko osoby uprawnionej	Data nadania uprawnienia	Data ustania uprawnienia	Nazwa/ systemu/usługi/ udziału	Identyfikator/login	Osoba odpowiedzialna

WNIOSEK O NADANIE/MODYFIKACJĘ/ODEBRANIE UPRAWNIEŃ DLA UŻYTKOWNIKA W SYSTEMIE INFORMATYCZNYM

Nowy użytkownik	Modyfikacja uprawnień	Odebranie uprawnień w systemie

DOTYCZY SYSTEMU:

……

nazwa systemu/rodzaj konta

Imię i nazwisko użytkownika:		
Jednostka Organizacyjna/Dział:		
Posiada upoważnienie do przetwarzania danych osobowych:	TAK	NIE
Opis zakresu uprawnień użytkownika w systemie informatycznym i uzasadnienie:		
Data obowiązywania uprawnienia:		
Data zgłoszenia:	**Podpis Administratora Danych Osobowych**	

REJESTR TWORZENIA KOPII								
Lp.	Nazwa systemu	Nazwa serwera	Rodzaj kopii (baza danych, poczta, pliki)	Typ kopii (pełna, różnicowa, przyrostowa)	Wolumen (GB)	Miejsce przetrzymywania	Data Tworzenia kopii	Osoba odpowiedzialna