Polityka bezpieczeństwa danych osobowych

Wstęp

Celem polityki bezpieczeństwa danych osobowych jest zapewnienie bezpieczeństwa przetwarzania danych osobowych, przez które powinno rozumieć się:

- Poufność danych - dane nie są udostępniane nieupoważnionym osobom,
- Integralność danych – dane osobowe nie zostały zmienione w sposób nieautoryzowany,
- Dostępność danych – właściwość polegająca na tym, że dane są dostępne i użyteczne na żądanie upoważnionych osób,
- Rozliczalność danych – właściwość zapewniająca, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie.

Szkoła Podstawowa nr 3 im. Mikołaja Kopernika zobowiązuje się do ochrony przetwarzanych przez siebie danych osobowych, stosując odpowiednie zabezpieczenia fizyczne i logiczne, procedury organizacyjne, oprogramowanie systemowe, jak również poprzez system szkoleń dla użytkowników systemu. Zastosowane procedury, systemy informatyczne są na bieżąco monitorowane i udoskonalane.

Polityka bezpieczeństwa danych osobowych jest głównym dokumentem składającym się na dokumentację ochrony danych osobowych prowadzoną w organizacji, do której zalicza się:

- Politykę bezpieczeństwa danych osobowych,
- Politykę zarządzania ryzykiem,
- Formularz nadzoru nad oryginałem dokumentu.

Dokumentacja Ochrony Danych Osobowych określa minimalne zabezpieczenia stosowane w organizacji.

Polityka bezpieczeństwa danych osobowych (zwana dalej „**Polityką**”) oraz inne dokumenty składające się na dokumentację ochrony danych osobowych w Szkoła Podstawowa nr 3 im. Mikołaja Kopernika zostały opracowane zgodnie z postanowieniami:

- ✓ Rozporządzenia 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 (zwane w dalszej części „RODO”)
- ✓ Ustawy o ochronie danych osobowych z dnia 10 Maja 2018 r. (tj. Dz.U. 2019.1781 z późn. zm.)

Definicje:

- **ADO – Administrator danych osobowych** – organ, jednostka organizacyjna, podmiot bądź też osoba decydująca o celach i środkach przetwarzania danych osobowych – Szkoła Podstawowa nr 3 im. Mikołaja Kopernika (dalej: Administrator lub SP 3)
- **Podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
- **Naruszenie ochrony danych osobowych** - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych;
- **Kierownictwo** – organ zarządzający i reprezentujący Administratora danych osobowych – Dyrekcja jednostki
- **Inspektor ochrony danych** – osoba, powołana przez **Kierownictwo** zgodnie z art. 37 RODO**,** nadzorująca przestrzeganie przepisów z zakresu ochrony danych osobowych, wykonująca zadania określone w niniejszym dokumencie oraz zadania określone w art. 39 RODO;
- **Dokumentacja ochrony danych osobowych** – dokumenty wdrożone w organizacji, których celem jest zapewnienie bezpieczeństwa przetwarzanych danych osobowych, na które składają się Polityka bezpieczeństwa danych osobowych, Polityka zarządzania ryzykiem, Formularz nadzoru nad oryginałem dokumentu;
- **Regulaminy** – dokumenty, z którymi powinny zapoznać się osoby upoważnione do przetwarzania danych osobowych;
- **Audyt –** sprawdzenie zgodności oraz skuteczności systemu ochrony danych osobowych;
- **Dane osobowe** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”);
- **Zbiór danych osobowych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów (niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie), przetwarzany w określonym celu;
- **Przetwarzanie danych osobowych** – jakiekolwiek operacje dokonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;
- **Usuwanie danych osobowych** – niszczenie danych osobowych, w sposób uniemożliwiający identyfikację osób ich dotyczących;
- **Użytkownik/osoba upoważniona** – osoba przetwarzająca dane osobowe z użyciem systemu informatycznego.

I Kierownictwo i jego obowiązki

1 Obowiązkiem kierownictwa jest zapewnienie legalności oraz bezpieczeństwa przetwarzanych danych osobowych poprzez zastosowanie odpowiednich środków technicznych jak i organizacyjnych. W szczególności do obowiązków kierownictwa należy:

1) wyznaczenie Inspektora ochrony danych;
2) zapewnienie niezbędnych środków do zagwarantowania bezpieczeństwa danych osobowych;
3) Zawieranie stosownych umów powierzenia przetwarzania danych osobowych;
4) nadzór nad zadaniami wykonywanymi przez osoby odpowiedzialne za system ochrony danych osobowych, w szczególności przez IOD;
5) nadzór nad systemem ochrony danych osobowych, w szczególności analiza raportów przedstawianych przez IOD, a także podejmowanie koniecznych działań;
6) zapewnienie szkoleń dla osób upoważnionych do przetwarzania danych osobowych;
7) wydawanie upoważnień do przetwarzania danych osobowych.

II Inspektor ochrony danych i jego obowiązki

1 Do obowiązków IOD należy w szczególności:
   1) informowanie administratora, podmiotów przetwarzających oraz użytkowników/osób upoważnionych, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO, a także innych przepisów Unii lub krajowych;
   2) pełnienie funkcji doradczych w stosunku do osób upoważnionych do przetwarzania danych osobowych;
   3) monitorowanie przestrzegania RODO, innych przepisów Unii lub krajowych o ochronie danych, a także polityk administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   4) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
   5) współpraca z organem nadzorczym;
   6) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
   7) nadzór nad podpisywaniem umów powierzenia danych osobowych;
   8) systematyczna aktualizacja polityki i instrukcji;
   9) podejmowanie doraźnych działań w celu minimalizacji skutków zdarzenia w przypadku naruszenia ochrony danych osobowych;
   10) analiza naruszeń oraz przedstawianie Kierownictwu zaleceń mających na celu uniknięcie podobnych zdarzeń w przyszłości;
   11) przedstawienie Kierownictwu sprawozdań dotyczących zgodności przetwarzania danych osobowych z obowiązującymi przepisami prawa.

III Dane osobowe, ich lokalizacja oraz struktura

1 Cele i podstawy przetwarzania danych osobowych oraz zakres danych osobowych przetwarzanych w organizacji.
   1) Cele i podstawy przetwarzania danych osobowych oraz zakres danych osobowych przetwarzanych w organizacji przedstawiony został w Załączniku nr 1 – Rejestrze czynności przetwarzania danych osobowych (opisującym cele i zakres przetwarzania danych osobowych przez SP 3 jako administratora danych osobowych) oraz w Załączniku nr 2 – Rejestrze kategorii czynności przetwarzania danych osobowych (opisującym cele i zakres przetwarzania danych osobowych przez SP 3 jako podmiotu przetwarzającego).

2 Lokalizacja danych osobowych: wykaz budynków, pomieszczeń lub ich części, tworzących obszar, w których są przetwarzane.
   1) Wszystkie miejsca, w których przetwarzane są dane osobowe wskazuje **załącznik nr 3.**

3 Wykaz firm, którym powierzono przetwarzanie danych osobowych oraz wykaz firm, w imieniu których przetwarzane są dane osobowe:
   1) lista firm zaangażowanych w proces przetwarzania danych osobowych wraz z podstawą powierzenia została określona w **załącznikach nr 1 oraz 8.**

4 Wykaz programów wykorzystywanych w organizacji przetwarzających poszczególne zbiory danych osobowych / Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól i ich wzajemne powiązania:
   1) zestawienie programów, w których przetwarza się dane osobowe, ze wskazaniem zbiorów obsługiwanych przez program, prezentuje **Załącznik nr 4.** W załączniku opisano również struktury programów (wskazano jakie kategorie danych osobowych przetwarzane są w poszczególnych programach).

IV Środki fizyczne, techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności oraz dostępności w procesie przetwarzania danych

1 Stosowane w organizacji fizyczne, techniczne i organizacyjne środki ochrony danych osobowych powinny być wdrażane na podstawie przeprowadzanej analizy ryzyka. Analiza ta powinna być wykonywana zgodnie z postanowieniami zawartymi w *Polityce zarządzania ryzykiem*. Arkusze analizy ryzyka powinny być utrwalone i przechowywane razem z dokumentacją ochrony danych osobowych. Po przeprowadzanej analizie ryzyka, arkusz należy uwzględnić w formularzu nadzoru nad oryginałem dokumentu.

1) *Fizyczne środki ochrony danych osobowych*
   a) Fizyczne zabezpieczenia stosowane w celu ochrony danych osobowych przedstawiono w załączniku nr 3.
2) *Techniczne środki ochrony danych osobowych*
   a) Dostęp do komputera zawierającego dane osobowe możliwy jest jedynie po uwierzytelnieniu za pomocą loginu i hasła;
   b) W przypadku dostępu do danych osobowych poprzez Internet (np. poprzez e-mail) wymagana jest autoryzacja z użyciem loginu i hasła;
   c) W przypadku dostępu do danych osobowych przez Internet, połączenie musi być szyfrowane (np. poprzez SSL, SFTP, VPN);
   d) Na wszystkich komputerach zainstalowany jest licencjonowany program antywirusowy;
   e) Na każdym z komputerów używa się systemu Firewall;
   f) Użytkownicy posiadają indywidualne konta w programach służących do przetwarzania danych osobowych, w których nadano im uprawnienia adekwatne do zajmowanego stanowiska;
   g) Użytkownik logujący się do programu zobowiązany jest do uwierzytelnienia poprzez podanie loginu oraz hasła;
   h) Na wszystkich komputerach zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego, w przypadku dłuższej nieaktywności pracy użytkownika;
3) Zabezpieczenia organizacyjne
   a) Opracowano i wdrożono Politykę bezpieczeństwa danych osobowych, Politykę zarządzania ryzykiem oraz Formularz nadzoru nad oryginałem dokumentu;
   b) Do przetwarzania danych osobowych dopuszczone są tylko i wyłącznie osoby posiadające upoważnienia nadane przez **ADO**;
   c) Osoby upoważnione do przetwarzania danych osobowych zostały zobligowane do zachowania ich w poufności;
   d) Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;
   e) Prowadzony jest Rejestr czynności przetwarzania danych osobowych, zgodnie z Załącznikiem nr 6;
   f) Prowadzony jest Rejestr kategorii czynności przetwarzania danych osobowych, zgodnie z Załącznikiem nr 7;
   g) Osoby upoważnione do przetwarzania danych osobowych zostały zaznajomione z regulaminami adekwatnymi do zajmowanego stanowiska oraz przepisami dotyczącymi ochrony danych osobowych;
   h) Pracownicy zobligowani są do stosowania polityki czystego biurka, to znaczy po zakończeniu pracy lub w przypadku czasowego opuszczenia stanowiska pracy wszelkie dokumenty zawierające dane osobowe muszą zostać zabezpieczone przed dostępem osób nieupoważnionych;
   i) Pracownicy zobligowani są do stosowania polityki czystego ekranu, to znaczy uniemożliwienia osobom nieupoważnionym (np. stażystom) wglądu do informacji wyświetlanych na ekranach monitorów;
   j) Przetwarzanie danych osobowych odbywa się w warunkach uniemożliwiających dostęp do danych osobowych przez nieuprawnione osoby;
   k) Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane;

l) Usuwanie danych osobowych odbywa się w taki sposób, by po ich usunięciu niemożliwe było zidentyfikowanie osób, których dotyczą.

V Postępowanie w przypadku wystąpienia naruszenia ochrony danych osobowych

1 Naruszeniem ochrony danych osobowych nazywamy zdarzenie prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych. Do naruszeń bezpieczeństwa zalicza się w szczególności:
   1) ujawnienie danych osobowych osobom nieupoważnionym;
   2) zagubienie dokumentacji zawierającej dane osobowe;
   3) kradzież dokumentacji zawierającej dane osobowe;
   4) zniszczenie dokumentacji lub nośników zawierających dane osobowe w wyniku zdarzenia losowego (powódź, pożar, brak zasilania);
   5) zgubienie urządzeń elektronicznych zawierających dane osobowe;
   6) próby wyłudzenia haseł dostępu lub danych osobowych.
2 W przypadku stwierdzenia naruszenia ochrony danych osobowych, należy o tym fakcie natychmiast poinformować **Kierownictwo, które następnie przekazuje informacje IOD**.
3 **IOD** powinien ocenić stopień zagrożenia oraz podjąć działania mające na celu zniwelowanie skutków naruszenia a w przypadku utraty danych, ich odzyskanie.
4 W przypadku wystąpienia naruszenia, **IOD** powinien dokonać analizy ryzyka związanego z zaistniałym naruszeniem, tj. ocenić prawdopodobieństwo i wpływ zagrożeń wynikających z tego zdarzenia, dla naruszenia praw i wolności osób fizycznych:
   1) Analiza ryzyka powinna być dokonana w szczególności w oparciu o „Wytyczne w sprawie powiadomień o naruszeniu ochrony danych osobowych na mocy rozporządzenia 2016/679" przyjęte 3 października 2017 r. przez GRUPĘ ROBOCZA DS. OCHRONY DANYCH NA MOCY ART. 29,
   2) IOD powinien dokonywać analizy ryzyka, biorąc pod uwagę w szczególności zagrożenia dla praw lub wolności osób fizycznych, których dane te dotyczą.
5 **IOD** po dokonaniu analizy, o której mowa w pkt. 4 powinien niezwłocznie poinformować **Kierownictwo** o jej wynikach. Następnie Kierownictwo podejmuje decyzje o konieczności podjęcia wszelkich niezbędnych działań, w szczególności zgłoszeniu naruszenia do organu nadzorczego, zawiadomieniu osób, których dane dotyczą.
6 Działania, o których mowa w pkt. 3 - 5 powinny zostać wykonane w ciągu 72h od stwierdzenia naruszenia ochrony danych osobowych. W przypadku, w którym SP 3 występuje jako podmiot przetwarzający należy dokonać zawiadomienia administratora danych osobowych w terminie określonym w umowie powierzenia przetwarzania danych osobowych.
7 W przypadku wystąpienia naruszenia, **IOD** powinien odnotować ten fakt w rejestrze naruszeń ochrony danych osobowych, który stanowi załącznik nr 6 do niniejszej Polityki.
8 Po podjęciu kroków o których mowa w pkt 3-6, **IOD** powinien dokonać analizy przyczyn zdarzenia i określić działania mające na celu uniknięcie podobnych naruszeń w przyszłości.

VI Prawa osób, których dane dotyczą

1 Osoby, których dane dotyczą posiadają prawo żądania:
   1) dostępu do danych osobowych;
   2) sprostowania danych osobowych;
   3) usunięcia danych osobowych;
   4) ograniczenia przetwarzania;
   5) sprzeciwu wobec przetwarzania danych osobowych;
   6) prawo do cofnięcia zgody, o ile zgoda jest podstawą przetwarzania danych osobowych.
2 Osoby, których dane dotyczą mogą zwrócić się z wnioskiem o wykonanie praw, o których mowa w pkt. 1 poprzez wysłanie oświadczenia pod adres kontaktowy administratora danych lub adres kontaktowy inspektora ochrony danych. Dane kontaktowe zawarte są w klauzulach informacyjnych.

3 Osoba wyznaczona przez administratora danych osobowych lub IOD koordynuje proces realizacji praw, o których mowa w pkt. 1.
4 Wykonanie praw, o którym mowa w pkt. 1 jest możliwe wyłącznie po wcześniejszej weryfikacji tożsamości osoby wnioskującej.

VII Szkolenie dla osób przetwarzających dane osobowe

1 Każda osoba przed rozpoczęciem przetwarzania danych osobowych powinna zapoznać się z postanowieniami regulaminów adekwatnych do zajmowanego stanowiska oraz z zapisami aktów prawnych regulujących zasady przetwarzania danych osobowych.
2 Każda osoba dopuszczona do przetwarzania danych osobowych powinna niezwłocznie wziąć udział w szkoleniu.
3 IOD prowadzi ewidencję osób przeszkolonych.
4 Każda osoba posiadająca dostęp do przetwarzania danych osobowych powinna wziąć udział w szkoleniu z zakresu ochrony danych osobowych co najmniej raz na 2 lata.
5 Szkolenia, o których mowa w pkt. 2 – 4 mogą odbywać się w formie stacjonarnej jak i elektronicznej.

VIII Audyty

1 Inspektor ochrony danych zobowiązany jest do przeprowadzania systematycznych audytów systemu ochrony danych osobowych (zwanych dalej ”audytami”).
2 Audyt, o którym mowa w pkt. 1 powinien obejmować w szczególności:
   1) sprawdzenie zgodności przetwarzania danych z aktualnymi przepisami prawa;
   2) sprawdzenie zgodności przetwarzania danych z dokumentacją z zakresu ochrony danych osobowych;
   3) sprawdzenie kompletności i aktualności prowadzonej dokumentacji ochrony danych osobowych.
3 Kompleksowy audyt ochrony danych osobowych powinien być wykonywany co najmniej 1 raz do roku.
4 **IOD** przedstawia Kierownictwu sprawozdanie z przeprowadzonych audytów.

IX Konsekwencje naruszenia polityki bezpieczeństwa oraz instrukcji

1 Działania niezgodne z Polityką bezpieczeństwa danych osobowych w SP 3 mogą być potraktowane jako ciężkie naruszenie przez Osobę upoważnioną podstawowych obowiązków pracowniczych zgodnie z art. 52 ust.1 pkt. 1 ustawy Kodeks Pracy lub też naruszenie postanowień umowy cywilnoprawnej wiążącej strony lub innych umów.

X Procedura nadawania oraz odbioru uprawnień do przetwarzania danych osobowych

1 Uprawnienia do przetwarzania danych osobowych może otrzymać osoba, która:
   1) zapoznała się z obowiązującymi regulaminami;
   2) zapoznała się z zapisami aktów prawnych regulujących zasady przetwarzania danych osobowych;
   3) otrzymała upoważnienie do przetwarzania danych osobowych;
   4) zobowiązała się do zachowania poufności zgodnie z oświadczeniem stanowiącym załącznik nr 5 do **Polityki.**
2 Upoważnienia do przetwarzania danych osobowych nadaje ADO zgodnie z **Załącznikiem nr 5**.
3 Uprawnienia w systemie Windows nadawane są przez Kierownictwo lub osobę wyznaczoną przez Kierownictwo.
4 **Identyfikator użytkownika,** który utraci uprawnienia do przetwarzania danych osobowych nie może być przydzielony innej osobie.
5 Osoba upoważniona zobligowana jest do podpisania oświadczenia o poufności z **Załącznika nr 5**.
6 **ADO** prowadzi ewidencję osób dopuszczonych do przetwarzania danych osobowych, zawierającą:
   1) Imię i nazwisko upoważnionej osoby;

2) Zakres upoważnienia;
3) Datę nadania oraz ustania upoważnienia.

7 Polityka haseł
1) Jeżeli autoryzacja dostępu do oprogramowania, w którym przetwarzane są dane osobowe następuje poprzez podanie hasła:
   a) powinno się ono składać z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne;
   b) system wymusza zmianę hasła co 90 dni lub użytkownik zobowiązany jest do zmiany hasła co 90 dni.
2) Użytkownik zobligowany jest do zachowania hasła w poufności oraz do jego natychmiastowej zmiany w przypadku jego ujawnienia;
3) W przypadku ujawnienia hasła lub podejrzenia ujawnienia hasła, użytkownik zobligowany jest do poinformowania o tym fakcie inspektora ochrony danych.
4) Zapamiętywanie haseł w przeglądarkach internetowych jest zabronione, jeżeli oprogramowanie zwiera dane osobowe.

8 Procedura rozpoczęcia, zawieszenia i zakończenia pracy
1) Użytkownik loguje się do systemu/programu informatycznego przetwarzającego dane osobowe poprzez podanie loginu i hasła;
2) Użytkownik zobligowany jest do uniemożliwienia osobom nieupoważnionym (np. stażystom, pracownikom obcych organizacji) wglądu do informacji wyświetlanych na ekranie monitora – tzw. **Polityka czystego ekranu**;
3) Użytkownik przed czasowym opuszczeniem stanowiska pracy zobowiązany jest do zablokowania dostępu do systemu (np. poprzez użycie skrótu klawiszowego Windows + L);
4) Po zakończeniu pracy użytkownik zobligowany jest do wylogowania się z systemu informatycznego.

9 Procedura korzystania z urządzeń kopiujących
1) Użytkownik powinien zabrać wszystkie dokumenty z podajników, skanerów i szuflad niezwłocznie po wykonaniu kopii lub wydrukowaniu dokumentu – tzw. polityka czystej drukarki;
2) Użytkownik powinien upewnić się, że wszystkie dokumenty oraz ich kopie zostały zabrane;

10 Procedury tworzenia kopii zapasowych
1) Procedury tworzenia kopii zapasowych zostały opisane w **Załączniku nr 4.**

11 Sposób korzystania z elektronicznych nośników informacji oraz urządzeń przenośnych zawierających dane osobowe
1) **Elektroniczne nośniki informacji**
   a) Przez elektroniczne nośniki informacji powinno rozumieć się materiał lub urządzenie służące do **zapisywania, przechowywania i odczytywania danych** w postaci cyfrowej lub analogowej czyli np. dyskietki, płyty CD, dyski twarde, pamięci typu flash.
   b) W przypadku wynoszenia elektronicznych nośników informacji poza obszar przetwarzania danych osobowych, zawarte na nich dane osobowe powinny być zaszyfrowane. W przypadku szyfrowania danych osobowych należy ustawić hasło o sile co najmniej 8 znaków, małe i wielkie litery, cyfry, lub znaki specjalne.
2) **Urządzenia przenośne**
   a) Przez urządzenia mobilne należy rozumieć urządzenia przenośne z zainstalowanym systemem operacyjnym, w szczególności: laptop, smartphone, tablet.
   b) Sprzęt komputerowy, telekomunikacyjny i oprogramowanie przekazane pracownikowi do użytkowania mogą być wykorzystywane tylko do realizacji obowiązków służbowych.
   c) Obowiązkiem użytkownika wynoszącego urządzenia przenośne poza obszar przetwarzania danych jest zapewnienie bezpieczeństwa zawartych na nich danych, w szczególności zabezpieczenia przed kradzieżą lub przypadkowym wykorzystaniem przez nieuprawnione osoby.
   d) Zabrania się pozostawiania urządzeń przenośnych bez nadzoru w środkach transportu.
   e) Zabrania się pozostawiania urządzeń przenośnych bez nadzoru w pomieszczeniach, z wyłączeniem pomieszczeń niedostępnych dla osób trzecich, w których odbywają się szkolenia

lub spotkań biznesowych, o ile użytkownik jest wylogowany z systemu zabezpieczonego hasłem.

f) Podczas wykonywania pracy poza obszarem przetwarzania danych osobowych (w szczególności w miejscach publicznie dostępnych oraz środkach transportu) użytkownik powinien zwrócić szczególną uwagę na zabezpieczenie wyświetlanych na ekranie informacji przed wglądem przez nieupoważnione osoby (tzw. polityka czystego ekranu).

g) Dyski urządzeń przenośnych zostały zaszyfrowane.

XI Sposób korzystania z poczty elektronicznej

1 Poczta elektroniczna służy wyłącznie do celów służbowych.

2 Użytkownik powinien zwracać szczególną uwagę na adresatów maili, tak by w przypadku przesyłania danych osobowych za pośrednictwem poczty elektronicznej, korespondencja nie trafiła do błędnych adresatów.

3 Użytkownik powinien zwracać szczególną uwagę na pliki stanowiące załączniki do korespondencji, tak by nie doszło do omyłkowego załączenia niewłaściwego pliku, w szczególności Użytkownik powinien dwukrotnie zweryfikować poprawność załączonego pliku.

4 Podczas rozsyłania wiadomości e-mail do grupy odbiorców zewnętrznych (w szczególności klientów indywidulanych), użytkownik zobligowany jest do ukrycia adresatów wiadomości (zastosowania opcji UDW (BCC)). Niniejsza procedura nie ma zastosowania do:

1) adresatów należących do SP 3;

2) adresatów, którzy z uwagi na treść wiadomości powinni być widoczni w celu wspólnej wymiany korespondencji.

5 W przypadku przesyłania szczególnych kategorii danych osobowych zarówno wewnątrz jak i poza organizację, Użytkownik powinien zastosować środki ochrony kryptograficznej (na przykład zaszyfrować przesyłany plik).

6 W przypadku przesyłania wiadomości e-mail zawierających zestaw danych osobowych w połączeniu z: numer PESEL lub numer dowodu osobistego lub numer paszportu lub dane dotyczące wynagrodzeń lub tytuły wykonawcze, Użytkownik powinien zastosować środki ochrony kryptograficznej (na przykład zaszyfrować przesyłany plik).

7 W przypadku szyfrowania pliku lub danych, o którym mowa w pkt. 5 - 6, należy ustawić hasło o sile co najmniej 8 znaków, małe i wielkie litery, cyfry, lub znaki specjalne.

8 Hasło, o którym mowa w pkt. 7 powinno być przekazane odrębnym kanałem komunikacji (np. poprzez SMS, telefonicznie).

9 Podczas korzystania z poczty elektronicznej zabrania się otwierania jakichkolwiek załączników od nieznanych adresatów.

XII Środki zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania

1 Na każdym z komputerów używa się licencjonowanego programu antywirusowego.

2 Na każdym z komputerów używa się systemu Firewall.

3 Zabrania się wyłączania przez użytkownika programu antywirusowego oraz systemu Firewall.

4 Podczas korzystania z poczty elektronicznej zabrania się otwierania jakichkolwiek załączników od nieznanych adresatów.

5 W przypadku sygnalizacji przez system informatyczny komunikatu o jego zainfekowaniu wirusowym bądź też stwierdzenia jakiejkolwiek nieprawidłowości związanej z bezpieczeństwem przetwarzanych danych, użytkownik powinien niezwłocznie poinformować o tym fakcie **Kierownictwo**.

Wydanie	***Data***	***Zatwierdził***
Wydanie 1	Kliknij tutaj, aby wprowadzić datę.	