Załącznik do zarządzenia nr
1/2023 z dn. 28.02.2023
Dyrektora Szkoły Podstawowej
im. H. Sienkiewicza w Kościelcu

Polityka Bezpieczeństwa Informacji

w Szkole Podstawowej im. H. Sienkiewicza w Kościelcu

LUTY 2023

Spis treści:

I. Cele Polityki

§ 1

Informacja jest newralgicznym zasobem Szkoły Podstawowej im. H. Sienkiewicza w Kościelcu.

§ 2

Celem niniejszej polityki jest:

1. zapewnienie bezpieczeństwa danych osobowych przetwarzanych w Szkole Podstawowej im. H. Sienkiewicza w Kościelcu przed naruszeniem ochrony danych osobowych, prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
2. zapewnienie bezpieczeństwa systemom teleinformatycznym wykorzystywanym w Szkole przed udostępnieniem i wykorzystywaniem w sposób naruszający zasady bezpieczeństwa przetwarzania i dostępu do informacji;
3. prawidłowe zabezpieczenie dokumentacji przed nieuprawnionym do niej dostępem, naruszeniem integralności bądź zniszczeniem aktywów związanych z przetwarzaniem informacji;
4. zagwarantowanie dostępności informacji oraz zdolności do nieprzerwanego świadczenia usług naszym klientom poprzez wdrożenie mechanizmów zarządzania ciągłością działania.

§ 3

Poprzez bezpieczeństwo rozumie się zapewnienie danym:

1. poufności – właściwość polegająca na tym, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
2. integralności - właściwość polegająca na zapewnieniu dokładności i kompletności informacji, dane nie mogą zostać zmienione lub zniszczone w sposób nieautoryzowany;
3. dostępności - właściwość zapewniająca, że informacja jest osiągalna i może być wykorzystana na żądanie upoważnionego podmiotu.

§ 4

„Polityka Bezpieczeństwa Informacji", zwana dalej PBI, została opracowana zgodnie z wymogami:

1. 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 (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. 119.1 z 04.05.2016);

2. Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 poz. 2247 t.j.);
3. polskich norm PN-EN ISO/IEC 27001 i PN-EN ISO/IEC 27002.

§ 5

1. Dyrekcja Szkoły wyraża pełne zaangażowanie dla zapewnienia bezpieczeństwa przetwarzanych informacji w Szkole oraz wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z ochroną tych informacji.
2. Administrator Danych Osobowych – Dyrektor Szkoły Podstawowej im. H. Sienkiewicza w Kościelcu, odpowiedzialny jest m. in. za:
   - zatwierdzanie Polityki Bezpieczeństwa Informacji
   - zapewnianie zasobów niezbędnych do właściwego zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, utratą, uszkodzeniem lub zniszczeniem.
3. Inspektor Ochrony Danych – osoba wyznaczona przez Dyrektora Szkoły do nadzoru nad przestrzeganiem przepisów o ochronie danych osobowych, odpowiedzialny jest m. in. za:
   - przeanalizowanie zagrożeń i ryzyka, na które może być narażone przetwarzanie danych osobowych
   - nadzór nad ustaleniem i zastosowaniem środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemie informacyjnym Szkoły, m.in.:
     - zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym/ nieuprawnionym
     - zapobieganie przetwarzaniu danych osobowych z naruszeniem przepisów o ochronie danych osobowych, ich zmianie, utracie, uszkodzeniu lub zniszczeniu
   - monitorowanie działania zabezpieczeń wdrożonych w celu ochrony danych osobowych
   - coroczną weryfikację zagrożeń i szans dotyczących systemu informacyjnego
   - coroczną weryfikację Polityki Bezpieczeństwa Informacji i ocenę jej funkcjonowania na przeglądzie systemu zarządzania
   - przekazywanie informacji związanych z bezpieczeństwem danych osobowych na bieżąco Dyrekcji Szkoły

- nadzór nad przestrzeganiem przez pracowników zasad wynikających z Polityki Bezpieczeństwa Informacji
- zapewnienie, by upoważnienia do przetwarzania danych pracowników zatrudnionych przy ich przetwarzaniu określały odpowiedzialność związaną z ochroną danych osobowych
- organizację szkoleń mających na celu zaznajomienie pracowników przetwarzających dane osobowe z przepisami dotyczącymi ich ochrony

4. Administrator Systemów Informatycznych – osoba upoważniona do nadzoru nad ochroną elektronicznych zbiorów danych osobowych, odpowiedzialny jest m. in. za:
    - właściwe zabezpieczenie sprzętu, na którym przetwarzane są dane osobowe
    - nadzór nad wykorzystywanym w Szkole Podstawowej im. H. Sienkiewicza w Kościelcu oprogramowaniem i jego legalnością
    - podejmowanie działań przeciw dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe
    - badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych
    - sporządzanie raportów z naruszenia bezpieczeństwa systemu teleinformatycznego i przekazywanie ich inspektorowi ochrony danych (wraz z informacją o podjętych działaniach)
    - nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe
    - definiowanie użytkowników i haseł dostępu
    - aktualizowanie oprogramowania antywirusowego, chyba, że aktualizacje te wykonywane są automatycznie
    - wykonywanie kopii awaryjnych, ich przechowywanie oraz okresowe sprawdzanie pod kątem ich dalszej przydatności
    - okresowa ocena stanu bezpieczeństwa danych osobowych i przekazywanie wyników kontroli inspektorowi ochrony danych
    - szkolenia nowo zatrudnionych pracowników z ochrony danych osobowych w systemie teleinformatycznym
5. Pracownicy przetwarzający dane osobowe odpowiedzialni są m. in. za:
    - stosowanie polityki bezpieczeństwa informacji,
    - ochronę powierzonych im do przetwarzania, archiwizowania lub przechowywania danych przed dostępem osób nieupoważnionych oraz zabezpieczenia przed zniszczeniem, utratą lub modyfikacją

- utrzymywanie w tajemnicy powierzonych identyfikatorów, haseł itp.
- zgłaszanie Inspektorowi Ochrony Danych ewentualnych naruszeń związanych z bezpieczeństwem danych osobowych.

§ 6

1. Wszyscy pracownicy Szkoły Podstawowej im. H. Sienkiewicza w Kościelcu są zobowiązani do zapoznania się z PBI i potwierdzenie u Inspektora Ochrony Danych tego faktu poprzez stosowną informację w ewidencji osób zapoznanych z PBI.
2. Wzór oświadczenia zawiera załącznik nr 1.

II. Definicje

§ 7

Użyte w niniejszej Polityce określenia i zwroty oznaczają:

1) **RODO** – 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);
2) **Administrator Danych Osobowych (ADO)** – Dyrektor Szkoły Podstawowej im. H. Sienkiewicza w Kościelcu;
3) **Inspektor Ochrony Danych (IOD)** – osoba wyznaczona przez ADO w rozumieniu art. 37 RODO;
4) **Administrator Systemów Informatycznych** (**ASI**) - osoba wyznaczona przez ADO, odpowiedzialna za wdrażanie i stosowanie zasad bezpieczeństwa w zakresie technicznych zabezpieczeń systemu teleinformatycznego;
5) **Blokowanie konta** – administracyjne uniemożliwienie korzystania z konta w danym systemie teleinformatycznym;
6) **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą") 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;
7) **Dane uwierzytelniające** – informacje wprowadzone do systemu, potwierdzające tożsamość użytkownika (np. hasła dostępu);
8) **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie teleinformatycznym;

9) **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę w systemie teleinformatycznym;
10) **Incydent** – pojedyncze zdarzenie lub seria niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu;
11) **Kopia archiwalna** – duplikat danych, przechowywanych z uwagi na przepisy prawa lub potrzeby dokumentowania działalności Szkoły; kopia archiwalna nie służy do odtworzenia;
12) **Kopia zapasowa** – duplikat danych, przechowywany na wymiennym nośniku danych służący do odtworzenia systemu, aplikacji, bazy danych, lub dokumentu;
13) **Dyrekcja Szkoły** – Dyrektor Szkoły Podstawowej im. H. Sienkiewicza w Kościelcu;
14) **Nośnik informacji** – medium magnetyczne, optyczne lub papierowe, na którym zapisuje się i przechowuje informacje - forma utrwalenia dokumentu;
15) **Organ nadzorczy** – Urząd Ochrony Danych Osobowych;
16) **Osoba trzecia** – osoba prawna lub fizyczna, organizacyjnie niezwiązana ze Szkołą,
17) **Pracownik** – osoba zatrudniona w Szkole na podstawie umowy o pracę, umów cywilnoprawnych oraz stażysta lub praktykant;
18) **Profil dostępu** – zestaw uprawnień, funkcji i zasobów systemu teleinformatycznego dostępnych poszczególnym użytkownikom systemu;
19) **Profil uprzywilejowany** – profil użytkownika posiadającego większe uprawnienia systemowe niż standardowy użytkownik np. administrator, użytkownik zaawansowany;
20) **Programy zabezpieczające** – programy, których celem jest zabezpieczanie systemu przed szkodliwym oprogramowaniem, nieupoważnionym dostępem oraz wykrywanie, zwalczanie i usuwanie wykrytego szkodliwego oprogramowania;
21) **Przetwarzanie danych** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
22) **Rejestr Oprogramowania (RO)** - rejestr oprogramowania dopuszczonego do funkcjonowania w Szkole. Rejestr jest prowadzony przez ASI;
23) **Rejestr Systemów Teleinformatycznych (RST)** - rejestr systemów teleinformatycznych użytkowanych w ramach infrastruktury teleinformatycznej Szkoły lub na podstawie zawartych umów. Rejestr jest prowadzony przez ASI;

24) **Spam** – niepożądana przesyłka poczty elektronicznej kierowana do niezdefiniowanego adresata;
25) **System teleinformatyczny** – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. 2022 poz. 1648, z późn. zm.);
26) **Szkodliwe oprogramowanie** – wszelkie aplikacje, skrypty i ingerencje mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do użytkownika komputera;
27) **Środki do przetwarzania informacji** – system, usługa lub infrastruktura przetwarzająca informacje;
28) **Uprawnienia administracyjne** – najwyższy poziom dostępu do całości lub części systemu teleinformatycznego w Szkole umożliwiający pełną kontrolę nad wszystkim funkcjami systemu teleinformatycznego;
29) **Szkoła** – Szkoła Podstawowa im. H. Sienkiewicza w Kościelcu;
30) **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
31) **Użytkownik** – osoba posiadająca upoważnienie nadane przez ADO lub osobę wyznaczoną przez niego do korzystania z systemu teleinformatycznego dostępnego w Szkole w celu realizacji powierzonych zadań;
32) **Wymienny nośnik danych** – komputerowy nośnik danych nie zainstalowany w sposób trwały (np. płyta CD\DVD, pamięć typu flash np. USB, karta, przenośny dysk twardy, kamera cyfrowa, smartfon) lub wymontowany z urządzenia służącego do przetwarzania danych;
33) **Zabezpieczenie danych w systemie teleinformatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
34) **Zagrożenie** – potencjalna przyczyna incydentu, który może spowodować stratę w systemie.

III. Przetwarzanie danych osobowych

§ 8

Zgodnie z art. 5 RODO dane osobowe muszą być:

1. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
2. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,

3. adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w którym są przetwarzane (minimalizacja danych),
4. prawidłowe i w razie potrzeby uaktualniane,
5. przechowywane w formie umożliwiającej identyfikacje osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane,
6. przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem (integralność i poufność).

§ 9

Dla zapewnienia skutecznej ochrony przetwarzanych danych osobowych ADO zapewnia:

1. odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne,
2. szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony,
3. okresowe szacowanie ryzyka zagrożeń dla zbiorów danych,
4. kontrolę i nadzór nad przetwarzaniem danych osobowych,
5. monitorowanie zastosowanych środków ochrony.

§ 10

Wszystkie osoby przetwarzające dane osobowe zobowiązane są do:

- posiadania upoważnienia do przetwarzania danych osobowych,
- przetwarzania danych osobowych zgodnie z obowiązującymi przepisami,
- postępowania zgodnie z ustaloną przez ADO Polityką Bezpieczeństwa Informacji.

§ 11

Osoby nieprzestrzegające przepisów w zakresie ochrony danych osobowych podlegają sankcjom przewidzianym w Regulaminie Pracy i w Prawie Cywilnym.

§ 12

Użytkownicy zobowiązani są do:

1. przetwarzania i ochrony danych osobowych zgodnie z przepisami;
2. ścisłego przestrzegania zakresu nadanego upoważnienia;
3. zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;

4. zgłaszania bez zbędnej zwłoki, do IOD, incydentów związanych z naruszeniem bezpieczeństwa ochrony danych osobowych.

§ 13

1. Za przestrzeganie ochrony informacji przetwarzanych w systemach teleinformatycznych odpowiedzialna jest Dyrekcja Szkoły.
2. Każdy użytkownik systemu teleinformatycznego odpowiada za ochronę informacji przetwarzanych w systemie zgodnie z indywidualnym zakresem obowiązków, nadanymi uprawnieniami i zakresem odpowiedzialności wynikającym z zajmowanego stanowiska.
3. Podmiotem doradczym w dziedzinie bezpieczeństwa informacji jest Inspektor Ochrony Danych.
4. Dyrekcja Szkoły odpowiada za przestrzeganie przepisów o ochronie danych osobowych oraz przepisów wewnętrznych na poszczególnych stanowiskach, a w szczególności:
   a) kontroluje sposób zabezpieczenia danych osobowych przez pracowników,
   b) kontroluje sposób realizacji obowiązku udzielania informacji, o jakich mowa w przepisach o ochronie danych osobowych,
   c) zgłasza rejestrację nowych czynności przetwarzania lub zmianę w obecnych czynnościach przetwarzania oraz przygotowuje wniosek w tej sprawie. Wzór wniosku stanowi załącznik nr 2.
   d) wnioskuje o nadanie, zmianę lub odebranie upoważnień do przetwarzania informacji oraz uprawnień użytkownika systemów teleinformatycznych pracownikom,
   e) zgłasza potrzeby w zakresie zabezpieczenia danych osobowych w Szkole.

§ 14

Obszar przetwarzania danych osobowych

1. Przetwarzanie danych w Szkole dopuszczalne jest wyłącznie na wyznaczonym do tego obszarze.
2. Za obszar przetwarzania danych osobowych uznaje się obszar, w którym wykonywana jest choćby jedna z czynności przetwarzania wymienionych art. 4 RODO.
3. Dyrekcja Szkoły zobowiązana jest do niezwłocznego przekazywania do IOD informacji o lokalizacji miejsc przetwarzania danych osobowych.
4. Wykaz pomieszczeń, w których przetwarzane są dane osobowe stanowi załącznik nr 3.
5. W szczególnych przypadkach możliwe jest przetwarzanie danych osobowych poza wyznaczonym obszarem (np. na komputerach przenośnych), jednak wymaga to indywidualnej zgody ADO.
6. Użytkownik urządzenia mobilnego zobowiązany jest do przestrzegania zapisów niniejszej polityki.

§ 15

Rejestr czynności przetwarzania danych

1. ADO prowadzi Rejestr Czynności Przetwarzania, w którym zamieszcza się co najmniej następujące informacje. Wzór rejestru stanowi - załącznik nr 4.
   1) imię i nazwisko lub nazwę oraz dane kontaktowe administratora i inspektora ochrony danych,
   2) cele przetwarzania,
   3) opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych,
   4) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione,
   5) gdy ma to zastosowanie, przekazania danych do państwa trzeciego, w tym nazwa tego państwa,
   6) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
   7) jeżeli jest to możliwe ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.
2. Rejestr, o którym mowa w ust. 1 ma formę pisemną lub formę elektroniczną.

§ 16

Udostępnianie danych osobowych

1. Na wniosek osoby, której dane dotyczą, ADO jest obowiązany do potwierdzenia przetwarzania danych oraz udzielenia następujących informacji:
   a) cele przetwarzania,
   b) kategorie odnośnych danych osobowych,
   c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,
   d) w miarę możliwości planowany okres przechowywania danych osobowych,
   e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
   f) informacje o prawie wniesienia skargi do organu nadzorczego,
   g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle,
   h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu.
3. IOD prowadzi wykaz udostępnień danych osobowych osobom, których dotyczą. Wzór wykazu stanowi załącznik nr 5.
4. Administrator danych udostępnia posiadane dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
5. Wzór wykazu udostępnień danych osobowych innym podmiotom, prowadzonego przez IOD, stanowi załącznik nr 6.
6. Powierzenie przetwarzania danych osobowych innemu podmiotowi może nastąpić wyłącznie w drodze umowy lub innego instrumentu prawnego, zawartej w formie pisemnej przez ADO, określającej przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, a także obowiązki i prawa administratora.
7. IOD prowadzi wykaz podmiotów, którym powierzono przetwarzanie danych osobowych. Wzór w/w wykazu stanowi załącznik nr 7.

§ 17

Zarządzanie ryzykiem oraz ocena skutków

1. Zarządzanie ryzykiem, obejmujące wybór, wdrożenie i utrzymanie zabezpieczeń składających się z technicznych i organizacyjnych środków ochrony danych oraz infrastruktury teleinformatycznej.
2. Przeprowadzenie analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń, a także konieczności przeprowadzenia oceny skutków powierzono zespołowi składającemu się z ASI oraz IOD.
3. Wyniki szacowania ryzyka zatwierdza ADO.

§ 18

Upoważnienia do przetwarzania danych osobowych

1. Wszystkie osoby przetwarzające dane osobowe zobowiązane są do:
   a) posiadania upoważnienia do przetwarzania danych osobowych;
   b) przetwarzania danych osobowych zgodnie z obowiązującymi przepisami;
   c) postępowania zgodnie z ustaloną przez ADO Polityką Bezpieczeństwa Informacji.
2. Dyrekcja Szkoły występuje z wnioskiem o upoważnienie do przetwarzania danych osobowych dla podległego mu pracownika na formularzu, którego wzór stanowi załącznik nr 11.

3. IOD sprawdza przed wydaniem upoważnienia do przetwarzania danych osobowych czy użytkownik spełnia warunki dopuszczenia do przetwarzania danej grupy informacji, a w szczególności:
   a) czy użytkownik zapoznał się i podpisał oświadczenie o zapoznaniu się z Polityką Bezpieczeństwa Informacji – załącznik nr 1;
   b) czy użytkownik podpisał deklarację zachowania poufności - załącznik nr 15.

4. Dyrekcja Szkoły występuje z wnioskiem o upoważnienie do przetwarzania danych osobowych dla podległego mu pracownika na formularzu, którego wzór stanowi załącznik nr 11.

5. Jeżeli użytkownik i jego stanowisko pracy spełniają warunki dopuszczenia, IOD przygotowuje upoważnienie do przetwarzania danych osobowych, którego wzór stanowi załącznik nr 13 i po podpisaniu przez ADO rejestruje je w Ewidencji osób upoważnionych do przetwarzania danych osobowych – którego wzór stanowi załącznik nr 12, a następnie przekazuje wniosek do ASI.

6. Zmiana zakresu uprawnienia następuje na pisemny wniosek Dyrekcji Szkoły i wydaniu nowego upoważnienia. Wzór wniosku stanowi załącznik nr 11.

7. Wykreślenie użytkownika z Ewidencji osób upoważnionych do przetwarzania danych osobowych następuje na pisemny wniosek Dyrekcji Szkoły.

IV. Monitorowanie PBI oraz zgłaszanie naruszenia ochrony danych osobowych

§ 19

Naruszenie zasad PBI może być skutkiem różnych czynników, w szczególności:

- szkodliwego wpływu środowiska na system przetwarzania informacji, zewnętrznych zdarzeń losowych dotyczących systemu przetwarzania informacji,
- zamierzonych lub niezamierzonych czynności użytkowników upoważnionych do przetwarzania informacji,
- nieuprawnionych działań osób nieupoważnionych do przetwarzania informacji.

§ 20

Za naruszenie zasad PBI uważa się, w szczególności:

- ujawnienie indywidualnych haseł dostępu użytkowników do systemu przetwarzającego informacje,
- wykonanie nieuprawnionych kopii informacji – wydruki, kopie na nośnikach zewnętrznych np. pamięci USB itp.,
- niewykonywanie kopii bezpieczeństwa,

- naruszenie lub próby naruszenia integralności systemu przeznaczonego do przetwarzania informacji,
- naruszenie lub próby naruszenia integralności informacji w systemie przetwarzania – wszelkie modyfikacje (dodanie, zmiana, usunięcie), zniszczenie lub próby ich dokonania przez osoby nieupoważnione lub upoważnione działające w złej wierze lub jako błąd osoby uprawnionej (np. zmiana zawartości danych, utrata całości lub części danych),
- naruszenie poufności poprzez celowe lub nieświadome przekazanie informacji osobie nieuprawnionej do ich otrzymania,
- naruszenie ochrony informacji w systemie np. nieautoryzowane logowanie do systemu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu z zewnątrz,
- nieuprawniony dostęp lub próba dostępu do systemu przetwarzania informacji np. nieuprawniona praca na koncie użytkownika czy istnienie nieautoryzowanych kont dostępu do informacji, pojawienie się nowych lub nie zablokowanie czy usunięcie starych kont dostępu,
- umożliwienie dostępu do informacji osobie nieuprawnionej np.: pozostawienie kopii danych (w drukarce/skanerze, ksero, na stole), nie zablokowanie dostępu do systemu (podczas nieobecności osoby uprawnionej), brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi przebywającymi w pomieszczeniach, gdzie przetwarza się informacje,
- nieuprawniony dostęp lub próba dostępu do pomieszczeń, gdzie przetwarza się informacje,
- zmiana lub usunięcie informacji zapisanych na kopiach bezpieczeństwa lub kopiach archiwalnych,
- brak nośnika zawierającego informacje – kradzież lub zaginięcie wydruku, kopii bezpieczeństwa, CD/DVD czy dysku,
- niewłaściwe niszczenie nośników informacji pozwalające na ich odczyt – wyrzucanie na śmietnik niezniszczonych nośników np.: wydruk, CD/DVD, pamięć USB,
- błędne nadanie uprawnień do przetwarzania informacji lub nadanie uprawnień osobie nie spełniającej wymagań.

§ 21

Reagowanie na naruszenia zasad PBI i niewłaściwe funkcjonowanie systemu

1. Każdy pracownik, który stwierdził naruszenie bezpieczeństwa informacji ma obowiązek zgłosić ten fakt ASI i/lub IOD.

2. Każdy pracownik, który stwierdził niewłaściwe funkcjonowanie systemu teleinformatycznego ma obowiązek zgłosić ten fakt do Dyrekcji Szkoły lub ASI. Jeśli nieprawidłowe funkcjonowanie systemu ma związek z naruszeniem PBI, ASI natychmiast informuje o tym IOD.
3. IOD po przyjęciu zgłoszenia, wspólnie z ASI, podejmuje niezwłoczne działania zabezpieczające, sprawdzające i wyjaśniające. Po wykonaniu tych czynności sporządza szczegółowy Protokół obsługi incydentu z przeprowadzonego postępowania, którego wzór stanowi załącznik nr 9 i przedstawia go ADO.
4. Każdy przypadek wystąpienia incydentu jest odnotowywany w Rejestrze incydentów – Wzór stanowi załącznik nr 10.
5. W celu zapewnienia dowodów dla celów wyjaśniającego, postępowania sądowego i procedury dyscyplinarnej, w przypadku podejrzenia przestępstwa lub nadużycia komputerowego, należy zgromadzić odpowiednie informacje o incydencie.
6. Informacje, które należy zgromadzić natychmiast po wystąpieniu incydentu obejmują dzienniki systemowe, zapisy przebiegu przetwarzania, inne wskaźniki aktualnego stanu systemu, jak również kopie zbiorów będących przedmiotem potencjalnego naruszenia bezpieczeństwa.
7. IOD wspólnie z ASI podejmuje postępowanie wyjaśniające, mające na celu ustalenie przyczyn i osób odpowiedzialnych za naruszenie bezpieczeństwa informacji. IOD sporządza szczegółowy raport z przeprowadzonego postępowania i przedstawia go ADO.
8. Przygotowany Protokół jest podstawą zgłoszenia przez ADO Organowi nadzorczemu, nie później niż w ciągu 72 godzin, faktu stwierdzenia naruszenia bezpieczeństwa ochrony danych osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało naruszeniem praw lub wolności osób fizycznych.
9. Zgłoszenie do organu nadzorczego, zgodnie z art. 33 RODO musi co najmniej:
   1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorię i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
   2) zawierać imię i nazwisko oraz dane kontaktowe IOD, od którego można uzyskać więcej informacji,
   3) opisywać konsekwencje naruszenia danych osobowych,
   4) opisywać środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
10. Wobec Pracowników winnych naruszenia bezpieczeństwa informacji na skutek nie przestrzegania obowiązujących zasad może zostać wszczęte postępowanie dyscyplinarne.

§ 22

1. Na naruszenie ochrony danych osobowych mogą wskazywać:
   1) uszkodzenia dokumentacji,
   2) nieuprawniony dostęp do systemów teleinformatycznych lub pomieszczeń,
   3) naruszenie lub próba naruszenia integralności systemu teleinformatycznego,
   4) zmiana lub utrata danych zapisanych na kopiach zapasowych, dokonana w sposób nieautoryzowany,
   5) zniszczenie lub próba zniszczenia w sposób nieuprawniony danych,
   6) inny stan pomieszczeń lub systemu teleinformatycznego niż pozostawiony po zakończeniu pracy lub przerwie w pracy.

Przykładowe incydenty ujęte są w załączniku nr 8. Lista przykładowych incydentów nie stanowi zamkniętego katalogu incydentów.

V. Zasady bezpieczeństwa

§ 23

Podstawowe zasady

Pracownicy zobowiązani są do bezwzględnego przestrzegania podstawowych zasad korzystania z urządzeń oraz nośników zawierających informacje chronione tj.:

1) nie ujawnianie haseł przypisanych do użytkownika,
2) umiejscowienie lub zabezpieczenie filtrami ekranowymi monitorów w pomieszczeniach biurowych w taki sposób, aby maksymalnie ograniczyć oglądanie zawartości ekranu osobom nieuprawnionym,
3) nie podłączanie do sieci komputerowej prywatnych urządzeń komputerowych,
4) nie korzystanie w komputerach stacjonarnych, laptopach, serwerach oraz innych urządzeniach komputerowych pracujących w systemie teleinformatycznym Szkoły z prywatnych nośników informacji,
5) natychmiastowe zgłoszenie Dyrekcji Szkoły, IOD lub ASI wszystkich zauważonych nieprawidłowości, zdarzeń, incydentów lub zagrożeń.

§ 24

Zasada „czystego biurka i ekranu"

Pracownicy Szkoły zobowiązani są do bezwzględnego przestrzegania zasady „czystego biurka i ekranu", która w szczególności obejmuje następujące wytyczne:

1) wszelkie dokumenty papierowe i nośniki komputerowe, kiedy nie są używane, przechowuje się w odpowiednich, zamykanych szafach lub innego rodzaju zabezpieczonych meblach, szczególnie poza godzinami pracy Szkoły,
2) nośniki zawierające dane osobowe, jeśli nie są aktualnie wykorzystywane, zamykane są w meblach biurowych, szafkach metalowych lub sejfach, w zależności od ich ważności,
3) w przypadku opuszczenia stanowiska pracy komputer należy zabezpieczyć przed niepowołanym dostępem innych osób poprzez zablokowanie go lub wylogowanie się,
4) komputery nie mogą być pozostawione bez nadzoru w stanie zarejestrowania do systemów teleinformatycznych,
5) pracownicy zobowiązani są do niezwłocznego odbioru swoich wydruków z urządzeń drukujących (szczególnie dotyczy to wydruków zawierających dane osobowe).

§ 25

Odpowiedzialność za sprzęt komputerowy

1. Odpowiedzialność za właściwe użytkowanie sprzętu służącego do przetwarzania informacji, w szczególności sprzętu komputerowego, spoczywa na jego użytkowniku.
2. Przesunięcie do użytkowania urządzeń komputerowych pomiędzy użytkownikami, w wyniku którego następuje zmiana osoby odpowiedzialnej za urządzenie, może nastąpić tylko za wiedzą i zgodą Dyrekcji Szkoły.
3. Wynoszenie urządzeń komputerowych poza Szkołę odbywa się jedynie na podstawie ważnych dokumentów przekazania za zgodą Dyrekcji Szkoły.

§ 26

Dostęp do urządzeń drukujących i powielających

1. Użytkownik, który oczekuje na wydrukowanie informacji musi być upoważniony do jej przeglądania oraz w przypadku drukowania informacji zawierających dane osobowe, nie odchodzić od urządzenia drukującego.
2. Wszystkie zbędne kopie informacji powstałe w trakcie ich przetwarzania, kopiowania lub drukowania muszą być trwale zniszczone.

§ 27

Po zakończeniu pracy

1. Po zakończonej pracy, przed opuszczeniem stanowiska pracy, pracownicy zobowiązani są do sprawdzenia czy dokumenty papierowe lub nośniki informacji zostały umieszczone

w zamkniętych szafach/biurkach oraz czy nastąpiło wylogowanie z systemu teleinformatycznego i/lub komputera.

2. Jeżeli pomieszczenie opuszczają wszyscy pracownicy, należy je zamknąć na klucz, a następnie przekazać do miejsca określonego w instrukcji. Po zamknięciu nie wolno zostawiać klucza w drzwiach.

VI. Hasła dostępu

§ 28

Użytkownik ponosi odpowiedzialność za użycie zasobów teleinformatycznych Szkoły przy wykorzystaniu jego hasła do momentu powiadomienia ASI o ujawnieniu hasła.

§ 29

1. Korzystanie z haseł ma na celu utrudnienie uzyskania nieautoryzowanego dostępu do zasobów teleinformatycznych Szkoły. Zasady te obejmują wszystkie systemy teleinformatyczne należące do Szkoły i/lub zarządzane i wykorzystywane w ramach wykonywanych obowiązków przez Szkołę.
2. Wszyscy użytkownicy systemów teleinformatycznych Szkoły muszą stosować hasła zgodnie z niniejszymi zasadami.
3. Hasło jest znane jedynie przez użytkownika.
4. Hasło administracyjne przechowywane jest w bezpiecznym miejscu, do którego dostęp ma Dyrekcja Szkoły.
5. Zabronione jest przekazywania hasła innym osobom. Bez względu na okoliczności, hasła nie wolno ujawniać. W szczególności nie należy go ujawniać przez telefon lub pocztę elektroniczną osobom, które mogą podawać się np. za pracowników pomocy technicznej.
6. Jeśli istnieje podejrzenie, że hasło zostało ujawnione, należy je natychmiast zmienić i powiadomić Dyrekcję Szkoły.

§ 30

1. Użytkownik ma obowiązek stosować hasła trudne do odgadnięcia.
2. Zaleca się aby użytkownicy nie używali haseł takich samych lub podobnych do używanych przez nich poprzednio. Hasło musi być różne od ostatnio wykorzystywanych 5 haseł.
3. Hasła powinny być unikalne tj. inne niż używane w jakimkolwiek innym systemie/aplikacji oraz inne niż używane przez Użytkowników poza systemami Szkoły.

4. Użytkownik korzystający z zewnętrznych usług internetowych zabezpieczanych hasłem nie powinien używać w celu dostępu do nich takiego samego hasła, jak w przypadku dostępu do systemów Szkoły.
5. Haseł nie należy zapisywać i pozostawiać w miejscu, w którym mogłyby zostać ujawnione.
6. Hasła nie powinny być wpisywane w obecności osób nieupoważnionych, jeśli mogą one zauważyć treść wpisywanego hasła.
7. Niedopuszczalne jest podglądanie haseł wprowadzanych do systemu przez innych użytkowników.

§ 31

Użytkownicy są zobowiązani do przestrzegania poniższych reguł odnośnie długości i złożoności hasła oraz okresu jego wymiany:

1) hasło do systemu musi składać się z min. 8 znaków - zawiera małe i duże litery oraz cyfry lub znaki specjalne,
2) zmiana hasła następuje nie rzadziej niż co 180 dni,
3) jeżeli system nie wymusza zmiany haseł użytkownik zobowiązany jest samodzielnie zmieniać hasło nie rzadziej niż co 180 dni.

§ 32

Hasło nie powinno być:

1) słowem ze słownika w żadnym popularnym języku,
2) nazwiskiem, nazwą geograficzną, terminem technicznym lub określeniem potocznym,
3) związane z życiem zawodowym lub osobistym Użytkownika np. nie powinno być numerem rejestracyjnym samochodu, numerem telefonu, imieniem członka rodziny, częścią adresu, inicjałami itp.
4) sekwencją kolejnych znaków na klawiaturze np. 123456, qwerty,
5) sekwencją tych samych znaków np. 33333, aaaaa,
6) oparte na ciągu znaków ulegających zmianie w zależności od daty lub przewidywalnego czynnika,
7) dowolnym elementem spośród wymienionych powyżej z dodaną na końcu cyfrą lub liczbą.

§ 33

Użytkownicy powinni stosować łatwe do zapamiętania hasła, które są jednocześnie trudne do odgadnięcia, spełniające co najmniej jeden z niżej wymienionych warunków:

1) łącząc kilka słów razem,
2) zastępując w określonym słowie kilka małych liter dużymi,

3) zastępując poszczególne znaki w haśle wcześniejszymi lub dalszymi znakami w alfabecie lub na klawiaturze,
4) zastępując w określonym słowie litery numerami odzwierciedlającymi ich pozycję w alfabecie,
5) łącząc znaki przestankowe i cyfry ze słowami,
6) wykorzystując pierwsze litery słów piosenki, wiersza lub innego znanego powiedzenia,
7) celowo stosując słowo z błędem (nie popełnianym jednak często lub nietypowym).

VII. Zarządzanie hasłami

§ 34

1. Wszystkie systemy teleinformatyczne Szkoły (o ile producent systemu przewidział taką możliwość) powinny umożliwiać ustalenie minimalnej długości hasła, okresu maksymalnej ważności hasła oraz mieć możliwość wymuszenia zmiany hasła przez użytkownika po upływie terminu jego ważności oraz przy pierwszym logowaniu.
2. ASI ustawia w systemie (jeżeli jest to możliwe) zasady wymuszenia zmiany hasła maksymalnie co 180 dni, długości i złożoności hasła.
3. Hasło użytkownika jest składowane w systemie przetwarzania w bezpieczny sposób.
4. Hasło użytkownika nie może być przesyłane przez sieć otwartym tekstem.
5. Hasło użytkownika nie jest pokazywane na ekranie lub wydrukach w postaci otwartego tekstu.

§ 35

1. Systemy używane przez wielu użytkowników powinny mieć możliwość ustawienia unikatowych identyfikatorów użytkowników i haseł przyporządkowanych poszczególnym użytkownikom, a także posiadać mechanizmy ograniczające przywileje użytkowników.
2. Systemy wykorzystywane przez pojedynczych użytkowników zaleca się, aby posiadały mechanizmy kontrolujące ich uruchamianie oraz automatycznie blokujące dostęp w przypadku przerwy w korzystaniu z systemu.
3. W przypadku stosowania jednego hasła do wspólnie użytkowanego systemu (np. poczta elektroniczna zlokalizowana na zewnętrznych serwerach) istnieje konieczność ograniczenia dostępu do hasła jedynie do osób, które w ramach wykonywania swoich obowiązków zawodowych potrzebują dostępu do danego systemu.

4. Przed przekazaniem do użytkowania systemów teleinformatycznych konieczna jest zmiana wszystkich haseł domyślnych ustawionych przez dostawcę lub ich zablokowanie.
5. ASI oraz inni pracownicy Szkoły nie będą zapoznawać się z treścią informacji zawartych w innych profilach użytkowników, z wyjątkiem sytuacji, gdy jest to niezbędne do usunięcia awarii systemu.

§ 36

Profile uprzywilejowane

1. Hasła dostępu do profili uprzywilejowanych powinny składać się z 12 znaków, zawierać małe i duże litery, cyfry oraz znaki specjalne.
2. Hasła dostępu do profili uprzywilejowanych powinny być przechowywane w bezpiecznym miejscu, w sposób zapewniający utrzymanie ich w tajemnicy. Powinny zostać stworzone procedury określające sytuacje, w których hasła dostępu do profili uprzywilejowanych będą udostępniane osobom innym, niż ich właściciele. Hasła przechowywane w bezpiecznym miejscu powinny być aktualizowane przy każdej ich zmianie. Hasła nieaktualne powinny być niszczone.
3. W przypadku konieczności udzielenia osobom trzecim dostępu do profilu uprzywilejowanego, hasło dostępu powinno być przed udzieleniem takiego dostępu zmienione na tymczasowe, a po wykorzystaniu przywrócone do stanu poprzedniego lub zmienione na nowe w ramach standardowej procedury.

VIII. Użytkowanie oraz ochrona przed szkodliwym oprogramowaniem

§ 37

Zakresy odpowiedzialności

Odpowiedzialność za zainstalowanie, odinstalowanie oraz obsługę techniczną oprogramowania ponosi ASI.

§ 38

Dyrekcja Szkoły zapewnia, że:

1) wszystkie użytkowane w Szkole programy, aplikacje oraz systemy operacyjne są legalne i posiadają odpowiednie licencje oraz zezwolenie na użytkowanie,
2) oprogramowanie jest zainstalowane maksymalnie na takiej liczbie stanowisk na jaką pozwala liczba licencji,
3) nośniki z oprogramowaniem pochodzą ze sprawdzonego i wiarygodnego źródła.

§ 39

Opis postępowania

1. Ochrona przed szkodliwym oprogramowaniem jest kluczowa dla utrzymania systemu bezpieczeństwa informacji. Szkoła stosuje wszelkie rozwiązania, które zapobiegają niepożądanym efektom wywoływanym przez szkodliwe oprogramowanie.
2. Za ochronę przed szkodliwym oprogramowaniem odpowiada ASI.
3. Systemy teleinformatyczne razem z przechowywanymi w nich informacjami są narażone na szkody wyrządzane przez działanie niepożądanego/szkodliwego oprogramowania. Z tego względu wszyscy użytkownicy powinni być świadomi zagrożeń związanych z działaniem niepożądanego oprogramowania.
4. W celu wykrycia oraz zapobieżenia pojawianiu się niepożądanego oprogramowania wdrożone są odpowiednie mechanizmy kontrolne. W szczególności uwaga zwrócona jest na ochronę komputerów użytkowników przed pojawianiem się wirusów komputerowych.
5. Zabezpieczenia przed niepożądanym oprogramowaniem opierają się na świadomości użytkowników, stosowaniu odpowiednich aplikacji zapobiegawczych oraz na prawidłowej kontroli dostępu do systemu.
6. Pracownicy są szkoleni i uświadamiani odnośnie korzystania z zabezpieczeń oraz w zakresie korzyści wynikających z działań zapobiegawczych.
7. Środkami, które zabezpieczają przed szkodliwym oprogramowaniem, są m.in.:
   1) przestrzeganie przez użytkowników zasad bezpieczeństwa,
   2) stosowanie programów zabezpieczających,
   3) stosowanie aktualizacji oprogramowania poprawiających bezpieczeństwo aplikacji oraz systemów,
   4) inne działania ASI i IOD np. szkolenia, spotkania
8. Wdrożone i monitorowane są wszystkie możliwe działania w celu zabezpieczenia komputerów oraz serwerów.
9. Nośniki zewnętrzne należy sprawdzić oprogramowaniem antywirusowym zainstalowanym na stacji roboczej lub przekazać ASI.
10. W przypadku wykrycia wirusa należy go usunąć i niezwłocznie poinformować ASI. Do czasu usunięcia wirusa lub otrzymania innych poleceń od ASI, pracę na komputerze należy wstrzymać.
11. Przy korzystaniu z poczty elektronicznej należy zwrócić szczególną uwagę na otrzymywane załączniki dołączane do treści wiadomości. Zabrania się otwierania załączników i wiadomości poczty elektronicznej od „niezaufanych" nadawców.

12. Zabrania się użytkownikom komputerów, wyłączania, blokowania, odinstalowywania programów zabezpieczających komputer np. skaner antywirusowy, firewall przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem.
13. Każdy użytkownik zobowiązany jest do korzystania na swoim komputerze z aktualnego oprogramowania antywirusowego.

§ 40

Szczególne obowiązki użytkowników

Wszyscy użytkownicy komputerów, w szczególności komputerów przenośnych lub innych urządzeń, które są narażone na działanie szkodliwego oprogramowania, zobowiązani są do:

1) uważnego korzystania z zasobów sieciowych (Internet, sieć lokalna) oraz nośników zewnętrznych kierując się przy tym ograniczonym zaufaniem,
2) sprawdzenia programem antywirusowym wszystkich nośników z danymi dostarczonych z zewnątrz Szkoły przed ich użyciem,
3) niezwłocznego powiadomienia Dyrekcji Szkoły lub ASI w przypadku stwierdzenia nieprawidłowego działania komputera lub innego urządzenia czy nośnika, które może być spowodowane przez złośliwe oprogramowanie.

IX. Zasady korzystania z internetu i poczty elektronicznej

§ 41

1. Dostęp do Internetu z sieci Szkoły powinien odbywać się wyłącznie za pośrednictwem środków i rozwiązań dostarczonych przez Szkołę. Zabronione jest zestawianie z sieci Szkoły indywidualnych połączeń z Internetem przez poszczególnych pracowników przy wykorzystaniu modemów lub innych urządzeń dostępowych.
2. Jakiekolwiek wykorzystanie systemów teleinformatycznych do działań niezgodnych z prawem lub takich, które mogą zostać uznane za obraźliwe lub łamiące inne zasady obowiązujące w Szkole, może stanowić podstawę do podjęcia działań dyscyplinarnych.

§ 42

1. Poczta elektroniczna Szkoły (konta e-mail) jest udostępniana Pracownikom do wypełniania obowiązków służbowych.

2. Dostęp do konta pocztowego zarządzanego przez wiele osób ograniczony zostaje do minimalnej liczby osób obsługujących dane konto pocztowe.
3. Pracownikom nie wolno używać do wypełniania obowiązków służbowych poczty elektronicznej innej niż wskazana przez ASI.
4. Zabrania się rozsyłania za pomocą poczty elektronicznej Szkoły wiadomości mających charakter niechcianych lub reklamowych (tzw. Spam).

§ 43

1. Wiadomości przychodzące do Szkoły są skanowane pod kątem obecności Spamu.
2. Maksymalny rozmiar przesyłek pocztowych może zostać ograniczony przez ASI.
3. Pracownicy powinni być świadomi, że poczta elektroniczna nie gwarantuje dostatecznej ochrony przesyłanych informacji. Z tego względu jeśli przesłaniu mają podlegać dane osobowe, należy przed wysłaniem przesyłki zaszyfrować ją przy użyciu rekomendowanych mechanizmów.
4. Kopia poczty e-mail użytkownika powinna być przechowywana na serwerze poczty przez czas przechowywania ustalany z Administratorem poczty e-mail i uzależniony od dostępnej przestrzeni oraz decyzji użytkownika lub Dyrekcji Szkoły.

§ 44

1. W trakcie korzystania z internetu należy przestrzegać poniższych zasad, które zwiększają bezpieczeństwo użytkownika w internecie:

    - Weryfikować adresy odwiedzanych stron internetowych, tak aby unikać podejrzanych stron internetowych, które mogą doprowadzić do zainfekowania komputera oraz sieci;
    - Unikać wchodzenia w linki, które zostały przesłane przez nieznanych nadawców lub mogą wydawać się podejrzane, ponieważ treść linku może być inna niż jego lokalizacja;
    - Nieotwieranie podejrzanych załączników dołączonych do wiadomości e-mail;
    - W plikach generowanych poprzez oprogramowanie wykorzystywane do prac biurowych należy unikać otwierania makr, tym bardziej gdy plik został dostarczony od niezidentyfikowanego nadawcy.

X. Postępowanie z nośnikami i ich bezpieczeństwo

§ 45

Dane na stacjach roboczych

1. Dokumenty na stacjach roboczych należy przechowywać w folderze „Moje dokumenty".
2. W szczególności nie należy przechowywać dokumentów na Pulpicie oraz w katalogu głównym dysku.

§ 46

Zarządzanie nośnikami informacji

1. Nośniki informacji zawierające dane osobowe, w szczególności wydruki, nośniki oprogramowania wraz z kodami aktywacyjnymi produktów przechowuje się w miejscach uniemożliwiających dostęp do nich osób nieuprawnionych.
2. Wymienne nośniki danych oraz dyski w komputerach przenośnych zawierające dane osobowe powinny być zabezpieczone poprzez ich zaszyfrowanie.
3. Komputery przenośne oraz stacjonarne powinny być zabezpieczone przed niepowołanym uruchomieniem poprzez zastosowanie hasła logowania do systemu operacyjnego.
4. W przypadku stosowania szyfrowania danych Dyrekcja Szkoły odpowiada za administrowanie kluczami szyfrowymi oraz przechowywanie w przeznaczonym do tego miejscu.
5. W przypadku utraty komputera przenośnego Użytkownik natychmiast powiadamia o tym fakcie Dyrekcję Szkoły, IOD i ASI, a w przypadku kradzieży dokonuje również niezwłocznego zgłoszenia popełnienia przestępstwa na policję. W zawiadomieniu użytkownik, poza danymi przekazanymi do ASI, podaje okoliczności utraty komputera, opis charakteru utraconych danych wraz z podaniem ich znaczenia dla Szkoły. W zawiadomieniu należy określić w szczególności charakter utraconych danych.

§ 47

Wycofywanie sprzętu i niszczenie nośników informacji

1. W przypadku tymczasowego (np. w celach serwisowych) lub trwałego (np. sprzedaż, darowizna) przekazywania osobom trzecim sprzętu komputerowego:
   1) wszelkie wymienne nośniki danych muszą być usunięte;
   2) usunięte powinny zostać dane osobowe zawarte na trwałych nośnikach poprzez ich skasowanie (w przypadku posiadania kopii) lub usunięcie trwałego nośnika.
2. W przypadku zbywania sprzętu należy skutecznie usunąć z niego wszystkie dane lub zbyć sprzęt bez nośników danych.

3. Za usunięcie wszelkich danych przed przekazaniem sprzętu komputerowego osobom trzecim odpowiada ASI.
4. Dyski twarde, płyty CD/DVD oraz inne komputerowe nośniki danych, zawierające dane osobowe, należy komisyjnie niszczyć w sposób uniemożliwiający odczytanie zapisanych na nich informacji np. poprzez zgniatanie, łamanie, działanie impulsu elektromagnetycznego. ASI jest zobowiązany do sporządzenia protokołu zniszczenia sprzętu, a następnie do przekazania go IOD.
5. Jeżeli zaistnieje potrzeba zniszczenia nośników zawierających dane osobowe, informacje chronione, takich jak zbędne kopie dokumentów papierowych, bądź przechowywanych na płytach CD/DVD itd., każdy pracownik ma obowiązek zniszczyć je w niszczarce.
6. Zbędne wydruki, notatki, kopie dokumentów itp. muszą być bezwzględnie niszczone w sposób uniemożliwiający odtworzenie ich treści.
7. Sposób postępowania z dokumentacją określa rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych oraz inne przepisy w tym zakresie.

XI. Zapasowe kopie informacji

§ 48

1. Dla Szkoły niezwykle ważne jest, aby wszystkie istotne dane miały kopie zapasowe dzięki czemu w przypadku uszkodzenia systemów komputerowych możliwe będzie odtworzenie danych i kontynuowanie działalności. Kopie zapasowe mają również stanowić gwarancję, że okresowe problemy związane z systemem teleinformatycznym nie będą miały wpływu na działalność operacyjną Szkoły.
2. Użytkownicy są odpowiedzialni za wykonywanie kopii zapasowych danych przechowywanych na swoich komputerach.
3. ASI wykonuje regularnie kopie zapasowe baz danych przetwarzanych w systemach.
4. Kopie ważnych plików z komputerów ASI przegrywa na nośniki zewnętrzne lub inne urządzenie fizyczne oddzielone od komputerów.
5. Nośniki zawierające kopie zapasowe powinny być przechowywane co najmniej do czasu utworzenia piątej kopii, tzn. zawsze powinny być dostępne co najmniej cztery ostatnie kopie.

6. Nośniki zawierające kopie zapasowe są wyposażone w etykiety, na których znajdują się informacje o numerze ewidencyjnym nośnika, zawartości kopii zapasowej, czasie jej wykonania oraz osobie wykonującej kopie.
7. Kopie zapasowe przechowywane są poza pomieszczeniami, w których zostały utworzone, w pomieszczeniach na tyle oddalonych, aby lokalny pożar czy zalanie wodą nie zniszczył jednocześnie nośników w obu pomieszczeniach.
8. Harmonogram wykonywania kopii zapasowych stanowi załącznik nr 14.

XII. Zarządzanie oprogramowaniem

§ 49

Ewidencja oprogramowania

Oprogramowanie działające w Szkole jest ewidencjonowane przez ASI w ramach Rejestru Oprogramowania (RO).

Ewidencja powinna zawierać:

1) nazwę programu,
2) dysponenta,
3) ilość licencji,
4) rodzaj oprogramowania,
5) osoby wyznaczone do administracji,
6) datę, od której oprogramowanie zaczęło działać w Szkole,
7) datę wycofania z użytkowania,
8) potwierdzenie legalności oprogramowania,
9) uwagi.

§ 50

Nowe oprogramowanie

1. Szkoła może wejść w posiadanie nowego oprogramowania:
   1. w drodze zakupu lub nabycia praw do użytkowania,
   2. tworzenia oprogramowania we własnym zakresie,
   3. przekazania w użytkowanie zgodnie z podpisanymi umowami.

2. Po nabyciu praw do użytkowania, oprogramowanie jest przekazywane do ASI w celu zainstalowania aplikacji jeśli nie zostało to wykonane przez np. wykonawcę umowy w ramach jej zakresu. ASI uzupełnia niezwłocznie Rejestr Oprogramowania.
3. Wszystkie licencje, jeśli zawarte umowy nie stanowią inaczej, z uwagi na wartość materialną oraz znaczenie prawne, stanowią aktywa, a ich dysponentem jest Dyrekcja Szkoły, która przechowuje je w miejscu zapewniającym bezpieczeństwo.

§ 51

Aktualizacje oprogramowania

1. Aktualizacje oprogramowania podzielone są na:
   1) poprawki i tzw. „łaty" poprawiające bezpieczeństwo,
   2) poprawki błędów polepszające funkcjonowanie oprogramowania,
   3) nowe wersje oprogramowania zagwarantowane w umowie licencyjnej i nie zmieniające w znaczący sposób funkcjonalności i walorów użytkowych oprogramowania,
   4) nowe wersje oprogramowania, które wymagają nabycia nowej licencji lub zmieniają w znaczący sposób funkcjonalność i walory użytkowe oprogramowania.
2. Przed dokonaniem aktualizacji wrażliwego oprogramowania aplikacyjnego, wskazanego w Rejestrze Oprogramowania, zalecane jest wykonanie kopii bezpieczeństwa danych przetwarzanych za pomocą oprogramowania, w celu ich zabezpieczenia. Decyzję w tym zakresie podejmuje ASI.
3. Po dokonaniu aktualizacji ASI sprawdza poprawność działania oprogramowania. W przypadku błędnego funkcjonowania podejmuje odpowiednie działania.

§ 52

Administracja oprogramowaniem antywirusowym

1. Oprogramowanie antywirusowe powinno być zarządzane przez ASI.
2. Program antywirusowy należy skonfigurować w sposób umożliwiający jego automatyczną aktualizację bez interwencji użytkownika.
3. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, ASI podejmuje działania zmierzające do usunięcia zagrożenia.
4. Sposób zabezpieczenia systemu teleinformatycznego przed działalnością szkodliwego oprogramowania:
   1) ruch w sieci komputerowej Szkoły jest zabezpieczony za pomocą zapór sieciowych;

2) aktualizacje baz danych oprogramowania zabezpieczającego pobierane są automatycznie z serwerów producenta oprogramowania.

5. Programy zabezpieczające należą do aktywów chronionych. Powinny być one zainstalowane na serwerach oraz na komputerach.
6. Wdrożone oprogramowanie zabezpieczające musi spełniać podstawowe zadania takie jak:
   1) ochronę przed wirusami komputerowymi,
   2) ochronę przed innym szkodliwym i złośliwym oprogramowaniem,
   3) monitorowanie transmisji poprzez interfejsy sieciowe,
   4) monitorowanie zewnętrznych nośników danych (płyty CD/DVD, pamięci flash i inne),
   5) monitorowanie poczty elektronicznej na serwerze poczty oraz stacjach roboczych.
7. ASI zobowiązany jest do:
   1) aktualizacji programów zabezpieczających,
   2) natychmiastowej reakcji w przypadku zdarzeń lub incydentów, które zostały wykryte przez oprogramowanie zabezpieczające, mającej na celu zminimalizowanie zagrożenia, naprawę powstałych luk w bezpieczeństwie oraz zabezpieczenie informacji, które mogą okazać się istotne w ustaleniu przyczyn incydentu lub zdarzenia.

XIII. Zarządzanie systemami

§ 53

Procedury eksploatacyjne oraz zakresy odpowiedzialności

1. W przypadku korzystania z komputera przez kilku użytkowników, określone zostają przez Dyrekcję Szkoły uprawnienia i obowiązki wszystkich współużytkowników tego sprzętu.
2. W celu realizacji wymogu kontroli dostępu do systemów teleinformatycznych wykorzystuje się wchodzące w skład tych systemów mechanizmy uwierzytelniania użytkowników.
3. Do systemów teleinformatycznych Szkoły mogą uzyskać dostęp wyłącznie uprawnieni użytkownicy.
4. Wszystkie systemy teleinformatyczne, na których przetwarzane są dane osobowe powinny posiadać uaktywnioną opcję wygaszacza ekranu i blokowania dostępu do systemu w przypadku braku aktywności użytkownika. Czas, po którym następuje uaktywnienie wygaszacza ekranu i zablokowanie systemu nie może być dłuższy niż 10 minut. Odblokowanie systemu ekranu wymaga podania hasła.
5. Wniosek o nadanie uprawnień zawiera załącznik nr 11

6. Pracownicy mogą zgłaszać wnioski dotyczące:
   1) funkcjonowania systemu teleinformatycznego – do ASI,
   2) bezpieczeństwa systemu teleinformatycznego – do IOD i ASI.
7. Po nadaniu lub zmianie uprawnień ASI dokonuje aktualizacji w RST. Rejestr Systemów Teleinformatycznych (RST) powinien zawierać:
   1) nazwę systemu,
   2) imię i nazwisko pracownika,
   3) identyfikator pracownika,
   4) datę oraz podstawę nadania Pracownikowi uprawnień do systemu,
   5) datę oraz podstawę odebrania uprawnień Pracownikowi.

§ 54

Dostęp do systemów operacyjnych

1. Identyfikacja użytkownika odbywa się na podstawie identyfikatora skojarzonego z hasłem. Z identyfikatorem związane są również prawa dostępu określające uprawnienia użytkownika.
2. W przypadku możliwości technicznych, stosowane są konta indywidualne, zapewniające możliwość jednoznacznego wskazania osób wykonujących operacje na systemach lub danych.
3. Zbędne oprogramowanie narzędziowe i systemowe usuwane jest z systemu przez ASI.
4. Sprzęt komputerowy musi być odpowiednio przetestowany przez ASI przed rozpoczęciem pracy przez Użytkownika.