INSTRUKCJA ZARZĄDZANIA

SYSTEMAMI INFORMATYCZNYMI

W ZESPOLE SZKÓŁ NR 1

IM. KOMISJI EDUKACJI NARODOWEJ

W NOWYM SĄCZU

§ 1

Postanowienia ogólne

1. Cel instrukcji

1) Niniejszy dokument o nazwie Instrukcja Zarządzania Systemami Informatycznymi (zwana dalej: „Instrukcją") stanowi zbiór zasad zarządzania systemem informatycznym w Zespole Szkół nr 1 im. Komisji Edukacji Narodowej w Nowym Sączu (dalej jako: Szkoła) 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 Szkole, rozumianego, jako zapewnienie: poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.

2) Instrukcja jest zbiorem zasad mających na celu właściwe zarządzanie systemami teleinformatycznymi służącymi do elektronicznego przetwarzania danych osobowych z uwzględnieniem warunków technicznych i organizacyjnych, jakim powinny odpowiadać wchodzące w jego skład urządzenia, odpowiednio do skali zagrożeń i kategorii danych objętych ochroną.

3) Stosowanie zasad bezpieczeństwa określonych w niniejszym dokumencie ma na celu zapewnienie prawidłowej ochrony danych osobowych przetwarzanych przez podmiot o nazwie: Zespół Szkół nr 1 im. Komisji Edukacji Narodowej w Nowym Sączu w systemach teleinformatycznych, jednocześnie przeciwdziałając zagrożeniom, jakimi są:

   a) udostępnianie danych osobom nieupoważnionym,

   b) zmiana lub zabranie danych przez osobę nieuprawnioną,

   c) przetwarzanie z naruszeniem przepisów,

   d) utrata, uszkodzenie lub zniszczenie danych.

2. Definicje legalne:

Ilekroć w niniejszej Instrukcji 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 Zespół Szkół nr 1 im. Komisji Edukacji Narodowej w Nowym Sączu - reprezentowaną przez Dyrektora placówki dalej zwanego „Administratorem";

2) **Inspektorze Ochrony Danych** – rozumie się przez to osobę, której Administrator powierzył pełnienie obowiązków określonych w art. 39 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016;

3) **Administratorze Systemu Informatycznego** – rozumie się przez to osobę, której Administrator powierzył pełnienie obowiązków nadzoru nad przestrzeganiem zasad ochrony danych osobowych pod kątem zabezpieczeń teleinformatycznych;

4) **Danych osobowych** – rozumie się przez to dane oznaczające informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. 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;

5) **Przetwarzaniu** – rozumie się przez to operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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;

6) **Zbiorze danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

7) **Osobie upoważnionej**– rozumie się przez to osobę posiadającą formalne upoważnienie do przetwarzania danych osobowych wydane przez Administratora;

8) **Identyfikatorze użytkownika** – rozumie się przez to nazwę przypisaną określonemu użytkownikowi. Używany jest podczas logowania, umożliwia uprawniony dostęp do danego komputera, systemu bądź sieci. Identyfikator jest ciągiem znaków o ograniczonej długości, wybranych z określonego zestawu znaków. Do identyfikatora przypisane jest konto użytkownika oraz ściśle określone uprawnienia, jakie ma dany użytkownik. Główną cechą identyfikatora jest jego unikalność w ramach danego systemu informatycznego;

9) **Użytkowniku systemu** - rozumie się przez to osobę fizyczną posiadającą formalne upoważnienie do przetwarzania danych osobowych wydane przez Administratora, oraz nadane uprawnienia do przetwarzania w systemie teleinformatycznym;

10) **Systemie teleinformatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;

11) **Identyfikatorze użytkownika** – rozumie się przez to nazwę przypisaną określonemu użytkownikowi. Używany jest podczas logowania, umożliwia uprawniony dostęp do danego komputera, systemu bądź sieci. Identyfikator jest ciągiem znaków o ograniczonej długości, wybranych z określonego zestawu znaków. Do identyfikatora przypisane jest konto użytkownika oraz ściśle określone uprawnienia, jakie ma dany użytkownik. Główną cechą identyfikatora jest jego unikalność w ramach danego systemu informatycznego;

12) **Użytkowniku systemu/Użytkownik systemu teleinformatycznego - rozumie** się przez to osobę fizyczną posiadającą formalne upoważnienie do przetwarzania danych osobowych wydane przez Administratora, oraz nadane uprawnienia do przetwarzania w systemie teleinformatycznym;

13) **Kryptografii** – rozumie się przez to gałąź wiedzy o utajnianiu wiadomości z dziedziny kryptologii - dziedziny wiedzy o przekazywaniu informacji w sposób zabezpieczony przed niepowołanym dostępem. Istotnym elementem technik kryptograficznych jest proces zamiany tekstu jawnego w szyfrogram (inaczej kryptogram); proces ten nazywany jest szyfrowaniem, a proces odwrotny, czyli zamiany tekstu zaszyfrowanego na powrót w możliwy do odczytania, deszyfrowaniem komunikacyjne (Dz.U.2021.576 tj.);

14) **Polityce Bezpieczeństwa Informacji** – rozumie się przez to zestaw formalnych zasad, procedur oraz odnoszących się do ochrony danych osobowych w Zespole Szkół nr 1 im. Komisji Edukacji Narodowej w Nowym Sączu;

15) **Analizie Ryzyka** – rozumie się przez to dokumentację zawierającą opis metodologii, częstotliwości oraz zakresu przeprowadzanego procesu szacowanie ryzyka;

16) **CRWDE** – rozumie się przez to Centralne Repozytorium Wniosków Dokumentacji Elektronicznej;

17) **ESP** – rozumie się przez to elektroniczną skrzynkę podawczą;

18) **ePUAP** – rozumie się przez to elektroniczną platformę usług administracji publicznej;

19) **SLA** – (ang. Service Level Agreement) rozumie się przez to umowę utrzymania i systematycznego poprawiania ustalonego między organizacją a usługodawcą poziomu, jakości usług poprzez stały cykl obejmujący uzgodnienia, monitorowanie usługi, raportowanie oraz przegląd osiąganych wyników.

3. Zakres zastosowania

Niniejsza Instrukcja znajduje zastosowanie do systemów informatycznych zastosowanych w Zespole Szkół nr 1 im. Komisji Edukacji Narodowej w Nowym Sączu 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 oraz awariami zasilania;

i) sposoby realizacji w Systemie wymogów dotyczących przetwarzania danych;

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

4. Podstawa prawna

Niniejsza Instrukcja została opracowana w oparciu o:

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);
2) Ustawę z dnia 10 maja 2018 o ochronie danych osobowych;
3) Wytyczne Grupy Roboczej art. 29 / EROD;
4) Ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2021.670 t.j. ze zm);
5) Rozporządzenie 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.2017.2247 t.j.);
6) Normy:
    a) PN-EN ISO/IEC 27001: 2017 (Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji - Wymagania),

b) PN-EN ISO/IEC 27002: 2017 (Technika Informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji),

c) PN-ISO/IEC 27005: 2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-EN ISO/IEC 27001:2017),

d) PN-ISO 31000: 2018-08 (Zarządzanie ryzykiem – Zasady i wytyczne),

e) PN-ISO/IEC 29134: 2018-11 (Technika informatyczna - Techniki bezpieczeństwa - Wytyczne dotyczące oceny skutków dla prywatności).

W oparciu o:

- Norma PN-EN ISO/IEC 27001: 2017 zał. A.18.1

5. Obszar stosowania

20) Za obszar stosowania traktuje się pomieszczenia budynku Zespołu Szkół nr 1 im. Komisji Edukacji Narodowej w Nowym Sączu przy ul. Jagiellońskiej 84.

W oparciu o:

- Norma PN-EN ISO/IEC 27001: 2017 pkt 4.3

§ 2

Odpowiedzialność

1. Administrator

Do obowiązków Administratora należy zarządzanie bezpieczeństwem informacji, a w szczególności:

1) zapewnienie warunków aktualizacji wobec regulacji wewnętrznych w stosunku do zmieniającego się otoczenia;
2) zapewnienie aktualności inwentaryzacji sprzętu i oprogramowania, co do rodzaju i konfiguracji;
3) umożliwienie/wykonanie okresowej analizy ryzyka wraz z adekwatnymi do wyniku działaniami minimalizującymi ryzyko;
4) podejmowanie działań zapewniających weryfikację stosownych uprawnień wobec osób uczestniczących w procesie przetwarzania danych;
5) zapewnienie warunków technicznych, organizacyjnych i fizycznych ze szczególnym naciskiem na:
   a) szkolenia obejmujące tematykę zagrożeń, skutków naruszenia bezpieczeństwa informacji oraz zapewnienie bezpieczeństwa wraz z minimalizacją ryzyka błędów ludzkich;
   b) ochrona przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami;

6) stosowanie umów powierzenia danych.

Podstawa prawna:

- Zgodnie z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017.2247 tj.)

W oparciu o:

- Norma PN-EN ISO/IEC 27001: 2017 pkt 5.3, zał. A.6.1

2. Inspektor Ochrony Danych

Do obowiązków Inspektora Ochrony Danych należy:

1) nadzór nad stosowaniem środków bezpieczeństwa w systemach teleinformatycznych;
2) nadzór nad przestrzeganiem procedur bezpieczeństwa przez Administratora oraz użytkowników;
3) proponowanie i uzgadnianie procedur w systemach teleinformatycznych z Administratorem oraz Administratorem Systemu Informatycznego;
4) zapewnienie punktu kontaktowego dla Administratora, użytkowników i organizacji współpracujących;
5) prowadzenie ewidencji użytkowników systemów teleinformatycznych, w których przetwarzane są dane osobowe, stanowiącej część ewidencji osób upoważnionych do przetwarzania danych osobowych oraz wszelkiej dokumentacji opisującej sposób realizacji i stopień ochrony danych osobowych w organizacji;
6) kontrolowanie nadanych w systemach teleinformatycznych uprawnień do przetwarzania danych osobowych pod kątem ich zgodności z wpisami umieszczonymi w ewidencji osób upoważnionych do przetwarzania danych osobowych.

Podstawa prawna:

- Zgodnie z art. 39 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

W oparciu o:

- Norma PN-EN ISO/IEC 27001: 2017 pkt 5.3, zał. A.6.1

3. Administrator Systemu Informatycznego

Do obowiązków Administratora Systemu Informatycznego należy:

1) opracowywanie i przestrzeganie procedur bezpieczeństwa systemów teleinformatycznych;
2) kontrola przepływu informacji pomiędzy systemem teleinformatycznym a siecią rozległą (z uwzględnieniem komunikacji poprzez sieć publiczną), oraz kontrola działań inicjowanych z sieci rozległej (z uwzględnieniem komunikacji poprzez sieć publiczną) a systemem teleinformatycznym;

3) zarządzanie stosowanymi w systemach teleinformatycznych środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień na podstawie uprzednio zaakceptowanego przez Administratora wniosku o udzielenie upoważnienia do przetwarzania danych osobowych;
4) utrzymanie systemu teleinformatycznego w należytej kondycji technicznej;
5) współtworzenie i doradztwo w zakresie Polityki Bezpieczeństwa Informacji, służącej do określenia zasad elektronicznego przetwarzania danych osobowych;
6) regularne tworzenie kopii zapasowych elektronicznych zasobów danych osobowych, programów służących do ich przetwarzania, oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych celem uzyskania ciągłości zarządzania;
7) wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji sprzętu IT, systemów teleinformatycznych, aplikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe.

W oparciu o:

- Norma PN-EN ISO/IEC 27001: 2017 pkt 5.3, zał. A.6.1

4. Użytkownik Systemu teleinformatycznego

Do obowiązków użytkownika systemu teleinformatycznego przy przetwarzaniu danych osobowych należy znajomość, zrozumienie i stosowanie w możliwie największym stopniu środków ochrony danych osobowych przy jednoczesnym uwzględnieniu przepisów prawa, oraz uniemożliwienie osobom nieuprawnionym dostępu do danych organizacji na swojej stacji roboczej. Dodatkowo użytkownik systemu teleinformatycznego zobligowany jest do:

1) współpracy przy ustaleniu przyczyn naruszenia ochrony danych osobowych, oraz usuwania skutków tych naruszeń, w tym zapobieganie ich ewentualnemu ponownemu wystąpieniu;
2) przestrzegania opracowanych dla systemu teleinformatycznego zasad przetwarzania danych osobowych oraz procedur i instrukcji;
3) informowania Inspektora Ochrony Danych o wszelkich naruszeniach, podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych;
4) wykonywania bez zbędnej zwłoki poleceń Inspektora Ochrony Danych w zakresie ochrony danych osobowych, jeśli są one zgodne z przepisami prawa powszechnie obowiązującego.

W oparciu o:

- Norma PN-EN ISO/IEC 27001: 2017 pkt 5.3, zał. A.6.1

§ 3

Zarządzanie pracą użytkownika w systemach teleinformatycznych

I. Nadawanie uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym wraz z ich rejestracją

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

1) **Minimalnych przywilejów** – każdy użytkownik posiada prawa dostępu do zasobów ograniczone wyłącznie do tych, które są niezbędne do wykonywania powierzonych mu obowiązków,
2) **Wiedzy koniecznej** – pracownicy posiadają wiedzę o zasobach ograniczoną wyłącznie do zagadnień, które są niezbędne do realizacji powierzonych im zadań
3) **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:
    1) pracownicy Administratora w zakresie niezbędnym do właściwego wykonywania obowiązków służbowych;
    2) osoby zatrudnione na podstawie umowy cywilnoprawnej;
    3) pracownicy lub osoby działające w imieniu podmiotu zewnętrznego świadczącego usługi na rzecz administratora danych
        a. stażyści, na podstawie umowy z Urzędem Pracy;
        b. praktykanci;
        c. wolontariusze, na podstawie umowy o wolontariat.
3. Przetwarzać dane, w tym dane osobowe w systemie teleinformatycznym może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych wydane przez Administratora.
4. Administrator nadaje upoważnienie do przetwarzania danych osobowych w systemie informatycznym, w którym wskazuje zakres upoważnienia.
5. Nadanie przez Administratora upoważnienia do przetwarzania danych osobowych w systemie teleinformatycznym oraz rejestracja użytkownika przetwarzającego dane osobowe w systemie teleinformatycznym następuje na wniosek bezpośrednio przełożonego użytkownika na rzecz, którego będą wykonywane czynności związane z przetwarzaniem danych osobowych.
6. Dostęp do danych osobowych przetwarzanych w systemie informatycznym odbywa się na podstawie uwierzytelnienia, poprzez podanie indywidualnej nazwy (identyfikatora/loginu) i hasła Użytkownika;
7. Administrator Systemu Informatycznego przydziela użytkownikowi konto użytkownika opatrzone identyfikatorem (login) i hasłem dostępu wraz z wykazem systemów teleinformatycznych do których dostęp w Szkole uzyskał użytkownik.
8. Użytkownik ponosi pełną odpowiedzialność za tworzone hasła (poza pierwszym hasłem do systemu nadawanego przez administratora systemu informatycznego) i jego przechowywanie.
9. Hasło jest niepowtarzalne i składa się z minimum 8 znaków.
10. Hasła powinny zawierać duże litery + małe litery + cyfry.
11. 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. udostępnianie haseł innym użytkownikom;
d. przeprowadzanie prób łamania haseł;
e. stosowanie rozwiązań programowych pozwalających na zapamiętywanie identyfikatorów i haseł.

12. Użytkownik systemu informatycznego posiadający dostęp do systemów informatycznych Administratora przetwarzających dane osobowe jest obowiązany 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 wystąpienia w Szkole incydentu teleinformatycznego w zakresie poufności/integralności/ dostępności danych w obrębie stanowiska komputerowego lub całej infrastruktury IT;
    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 60 dni.
13. Inspektor Ochrony Danych w ramach podejmowanych czynności audytowych sprawuje nadzór nad procesem nadawania uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym.

W oparciu o:

- Norma PN/ISO/IEC 27001: 2017 zał. A.9.2

Uwagi:

- Administrator jest zaznajomiony z wytycznymi Rozporządzenia MSWiA z dnia 29 kwietnia 2004 (Dz. U. z 2004 r. Nr 100, poz. 1024) „w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych", jednakże mając na uwadze uchylenie przepisu oraz branżowe doświadczenie, zastosował własne wytyczne.

II. Modyfikacja uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym

1) Modyfikacja uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym następuje na wniosek bezpośredniego przełożonego użytkownika w następujących przypadkach:
    a) modyfikacja uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym z powodu zmiany zakresu czynności.

2) Zgłoszenie modyfikacji uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym zgłasza się poprzez „ Wniosek o założenie konta w systemach informatycznych o Administratora. Wniosek po pozytywnym rozpatrzeniu przez Administratora zostaje przekazany do Administratora Systemu Informatycznego.
3) Administrator Systemu Informatycznego dokonuje modyfikacji uprawnień użytkownika w terminie 7 dni od dnia akceptacji wniosku przez Administratora.
4) Inspektor Ochrony Danych w ramach podejmowanych czynności audytowych sprawuje nadzór nad procesem modyfikacji uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym.

W oparciu o:

- Norma PN-EN ISO/IEC 27001: 2017 zał. A.9.2

III. Wycofywanie uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym

1) Wycofanie uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym może nastąpić na wniosek bezpośredniego przełożonego użytkownika w następujących przypadkach:
   a) wycofanie uprawnień użytkownika z powodu zakończenia przetwarzania danych osobowych w obrębie systemu teleinformatycznego;
   b) wycofanie uprawnień użytkownika z powodu ustania stosunku pracy, ustania umowy cywilnoprawnej, zakończenia stażu lub praktyki.
2) Pisemny wniosek o wycofanie uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym należy złożyć do Administratora. Wniosek po pozytywnym rozpatrzeniu przez Administratora zostaje przekazany do Administratora Systemu Informatycznego.
3) Administrator Systemu Informatycznego dokonuje wycofania uprawnień użytkownika w tym samym dniu w którym otrzymał wniosek od wycofanie uprawnień od Administratora.
4) Po wycofaniu uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym, Administrator Systemu Informatycznego dokonuje zablokowania identyfikatora użytkownika celem uniemożliwienia przydzielenia innemu użytkownikowi.
5) Inspektor Ochrony Danych w ramach podejmowanych czynności audytowych sprawuje nadzór nad procesem wycofywania uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym.

W oparciu o:

- Norma PN-EN ISO/IEC 27001: 2017 zał. A.9.2

IV. Rozpoczęcie pracy przez użytkownika w systemie teleinformatycznym

1) Przed przystąpieniem do pracy w systemie teleinformatycznym użytkownik zobowiązany jest sprawdzić urządzenie komputerowe i stanowisko pracy zwracając uwagę, czy nie zaszły okoliczności wskazujące na naruszenie danych osobowych. W przypadku stwierdzenia naruszenia danych osobowych użytkownik zobowiązany jest do niezwłocznego powiadomienia Administratora Systemu Informatycznego oraz Inspektora Ochrony Danych.
2) Celem zalogowania się do systemu teleinformatycznego użytkownik wpisuje swój identyfikator i hasło. Jeżeli jest to pierwsze logowanie użytkownika od momentu nadania uprawnień do przetwarzania w sieci teleinformatycznej, użytkownik jest zobligowany do zmiany hasła, chyba, że konfiguracja systemu teleinformatycznego samoczynnie wymusza takową zmianę.
3) Użytkownik zobowiązany jest do zmiany haseł, zgodnie z zapisami § 3 niniejszej Instrukcji.
4) Wpisywanie hasła lub jego modyfikacja nie może się odbywać w obecności innych osób.
5) Hasło nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób nieuprawnionych.
6) W przypadku zagubienia hasła, użytkownik musi się skontaktować z Administratorem Systemu Informatycznego, który o zaistniałym zdarzeniu informuje Inspektora Ochrony Danych.
7) Niedopuszczalne jest uwierzytelnianie się poprzez identyfikator i hasło innego użytkownika, lub praca w systemie teleinformatycznym na koncie innego użytkownika.

W oparciu o:

- Norma PN-EN ISO/IEC 27001: 2017 zał. A.9.3

V. Zawieszenie/odwieszenie pracy przez użytkownika w systemie teleinformatycznym

1) W celu zawieszenia pracy w systemie teleinformatycznym służącym do przetwarzania danych osobowych użytkownik zobowiązany jest się „wylogować" się lub jednoczesne wcisnąć kombinację klawiszy „⊞ + L", celem zablokowania ekranu z opcją ponownego logowania po podaniu hasła.
2) Celem ponownego zalogowania się w systemie teleinformatycznym użytkownik podaje hasło i rozpoczyna pracę z uwzględnieniem zasad rozpoczęcia pracy użytkownika w systemie teleinformatycznym zawartych w niniejszej Instrukcji.
3) Zabrania się pozostawienia stanowiska komputerowego z uruchomionym systemem bez uprzedniej aktywacji blokady ekranu poprzez kombinację klawiszy „⊞ + L".

W oparciu o:

- Norma PN-EN ISO/IEC 27001: 2017 zał. A.9.3

VI. Zakończenie pracy przez użytkownika w systemie teleinformatycznym

1) Celem zakończenia pracy w systemie teleinformatycznym, użytkownik zamyka wszystkie aktywne programy.
2) Użytkownik wylogowuje się, zamyka system operacyjny i wyłącza komputer (przeważnie wszystkie trzy opcje są ze sobą powiązane).
3) Po zakończeniu pracy użytkownik sprawdza swoje stanowisko pracy i zabezpiecza wszelakie nośniki danych takie jak dokumenty, pendrive, dyski przenośne, płyty CD/DVD/BD zawierające dane osobowe, przed dostępem osób nieupoważnionych.
4) W przypadku wystąpienia nieprawidłowości podczas procesu wylogowywania się, zamknięcia systemu lub fizycznego wyłączenia komputera, użytkownik musi powiadomić Administratora Systemu Informatycznego.

W oparciu o:

- Norma PN-EN ISO/IEC 27001: 2017 zał. A.9.3

§ 4

Zarządzanie bezpieczeństwem w systemach teleinformatycznych

1. Zabezpieczenia kryptograficzne

1) Za bezpieczeństwo informacji w Szkole odpowiada Inspektor Ochrony Danych.
2) Za bezpieczeństwo informacji w systemach teleinformatycznych odpowiada Administrator Systemu Informatycznego, przy jednoczesnym uwzględnieniu wymagań związanych z kompatybilnością mechanizmu kryptograficznego.
3) Wprowadzenie zabezpieczenia kryptograficznego wykonywane jest przez Administratora Systemu Informatycznego na zlecenie Inspektora Ochrony Danych o uprzedniej z nim konsultacji, co do następujących warunków:
   a) adekwatność zabezpieczenia kryptograficznego wobec przetwarzanych danych osobowych;
   b) poziom ryzyka utraty poufności danych;
   c) rodzaj usługi kryptograficznej (szyfrowanie symetryczne, asymetryczne, podpis cyfrowy, znakowanie czasem itp.);
   d) odpowiednia moc mechanizmów kryptograficznych (zastosowane algorytmy, długości kluczy);
   e) sposób zarządzania kluczami kryptograficznymi;
   f) wydajność mechanizmu kryptograficznego;
   g) kompatybilność z istniejącą infrastrukturą teleinformatyczną organizacji;
   h) rodzaj zabezpieczanych danych (dane przechowywane na nośniku, przesyłane przez sieci lokalne, transmitowane w sieciach rozległych lub publicznych);
   i) wymagania dotyczące certyfikacji produktu (o ile występują);
   j) wymagania dotyczące zgodności z normami branżowymi i wykorzystanie standardowych protokołów dla mechanizmów kryptograficznych (o ile występują);

k) łatwość wdrożenia mechanizmu i integracji z systemem teleinformatycznym organizacji;

l) odporność na próby kompromitacji mechanizmu kryptograficznego;

m) wymagany stopień interakcji z użytkownikiem.

4) Procedura dystrybucji kluczy powinna zapewnić, by w czasie przesyłania klucz nie był czytelny w całości. Gdy używane są klucze zabezpieczające hasła (tak jak w przypadku plików samo rozszyfrowujących się), hasło powinno być przesłane osobno, a nie razem z plikiem zaszyfrowanym drogą e-mail. Jeśli to tylko możliwe, hasło powinno być przesyłane przy użyciu innego kanału dystrybucji (np. telefon komórkowy).

Podstawa prawna:

- Zgodnie z art. 32 pkt 1 lit. a) oraz motywem nr 83 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.

W oparciu o:

- Norma PN-EN ISO/IEC 27001: 2017 zał. A.10

2. Zarządzanie bezpieczeństwem i komunikacją w sieciach teleinformatycznych

1) Bezpieczeństwo sieci

a) Za zarządzanie infrastrukturą teleinformatyczną odpowiedzialny jest Administrator Systemu Informatycznego, którego zakres obowiązków ma na celu zapewnienie właściwej ochrony, adekwatnie do zagrożeń mogących powodować utratę bezpieczeństwa przetwarzania danych osobowych.

b) Administrator Systemu Informatycznego zapewnia bezpieczeństwo teleinformatyczne względem zagrożeń pochodzących z sieci publicznej poprzez wdrożenie logicznych zabezpieczeń takich jak programy antywirusowe (stacje robocze i serwer/y) oraz środka kontroli przepływu informacji na poziomie bramy sieciowej.

c) Podłączanie we własnym zakresie wszelakich urządzeń sieciowych takich jak modemy, karty sieciowe, urządzenia wzmacniające, koncentratory, mosty, przełączniki, punkty dostępowe, routery, bramy sieciowe, bramki VoIP, zapory sieciowe do infrastruktury teleinformatycznej organizacji jest surowo zabronione.

d) Podłączanie nieautoryzowanych stacji roboczych do sieci publicznej poprzez wewnętrzna sieć LAN organizacji jest surowo zabronione.

e) Sieci bezprzewodowe uwierzytelniane są zabezpieczeniem kryptograficznym w postaci klucza WPA2-PSK z opcją 256 bitowego hasła (standard AES).

f) Użytkownicy używają połączenia z siecią publiczną wyłącznie w celach służbowych.

g) Użytkownicy nie mogą ściągać za pośrednictwem sieci LAN, WAN, oprogramowania do wymiany plików p2p (np. BitTorrent, µTorrent itp…) żadnego oprogramowania, utworów muzycznych, filmów, które mogą być niezgodne z prawem.

2) Bezpieczeństwo komunikacji

Szkoła w przypadku przesyłania informacji z użyciem środków komunikacji uwzględnia i stosuje następujące elementy:

a) ochrona przesyłanej informacji przed przechwyceniem, kopiowaniem, modyfikacją, błędnym routingiem i zniszczeniem za pomocą oprogramowania antywirusowego oraz bramy sieciowej;
b) wykrywanie i ochrona przed szkodliwym kodem, który może być przesyłany za pomocą środków komunikacji elektronicznej;
c) ochrona wrażliwych informacji elektronicznych przekazywanych w formie załączników do poczty e-mail;
d) zalecenia określające akceptowalny sposób korzystania z elektronicznych urządzeń komunikacyjnych opisanych w wytycznych co do rozpoczęcia, zawieszenia/odwieszenia, zakończenia pracy przez użytkownika w systemie teleinformatycznym;
e) korzystanie z technik kryptograficznych, np. do ochrony poufności, integralności i autentyczności informacji;
f) doradzanie pracownikom w kwestii stosowania odpowiednich środków ostrożności, aby nie ujawniali informacji poufnych.

Podstawa prawna:

- Zgodnie z art. 32 pkt 1 lit. b) oraz motywem nr 83 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.

W oparciu o:

- Norma PN-EN ISO/IEC 27001:2017 zał. A.13

3. Ochrona przed szkodliwym oprogramowaniem

Administrator stosuje następujące środki bezpieczeństwa przed szkodliwym oprogramowaniem:

1) zakaz korzystania z nieautoryzowanego oprogramowania na terenie całego Urzędu.
2) zabezpieczenia wykrywające lub zapobiegające użyciu znanych szkodliwych stron webowych lub podejrzewanych o to (np. czarne listy).
3) zabezpieczenia przed ryzykami związanymi z otrzymywaniem złośliwego oprogramowania malware z sieci zewnętrznych albo za pośrednictwem innych mediów w postaci wymiennych nośników danych typu pendrive. Na oprogramowanie malware składają się: wirusy, robaki, wabbit, konie trojańskie, backdoory, programowanie szpiegujące (w tym scumware, stealware/parasiteware, oprogramowanie reklamowe, elementy typu hijacker), exploit, rootkit, rejestratory klawiszy, dialery, oprogramowanie szantażujące.
4) instalacja i regularna aktualizacja oprogramowania do wykrywania oraz usuwania szkodliwego oprogramowania poprzez skanowanie komputerów i nośników informacji. Skanowanie obejmuje:
   a) skanowanie wszystkich plików odbieranych poprzez sieci lub na innych nośnikach pamięci pod kątem obecności szkodliwego oprogramowania;

b) skanowanie załączników poczty elektronicznej oraz ściąganych danych pod kątem obecności szkodliwego oprogramowania;
c) sprawdzanie stron internetowych pod kątem obecności szkodliwego oprogramowania.

5) plan ciągłości działania w celu odtwarzania po ataku szkodliwego oprogramowania, będący procedurą wykonywania kopii zapasowych danych elektronicznych;
6) izolowanie środowisk, dla których skutki działania szkodliwego oprogramowania mogą być katastrofalne.

Podstawa prawna:

- Zgodnie z art. 32 pkt 1 lit. b) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.

W oparciu o:

- Norma PN-EN ISO/IEC 27001:2017 zał. A.12.2

4. Postępowanie z urządzeniami mobilnymi

1) Administrator wprowadza wewnętrzny podział urządzeń mobilnych na:
   a) mobilna stacja robocza typu notebook/ultrabook/netbook;
   b) smartfon - przenośne urządzenie telefoniczne łączące w sobie funkcje telefonu komórkowego i komputera kieszonkowego.
2) Wobec urządzeń mobilnych będących własnością Szkoły stosuje się następujące środki bezpieczeństwa:
   a) rejestracja urządzeń mobilnych;
   b) wydającym sprzęt mobilny w imieniu Administratora jest Administrator Systemu Informatycznego, który prowadzi ewidencje powierzonego mienia poprzez dokument o nazwie;
   c) ograniczenie instalacji oprogramowania oraz kontrola dostępu w postaci konta użytkownika i administratora w przypadku mobilnej stacji roboczej;
   d) automatyczna aktualizacja oprogramowania przez Administratora Systemu Informatycznego;
   e) zabezpieczenia kryptograficzne;
   f) ochrona przed szkodliwym oprogramowaniem w postaci oprogramowania antywirusowego.
3) Wobec komputerów mobilnych organizacja stosuje środek techniczny w postaci szyfrowania. Dobór oprogramowania szyfrującego należy do decyzji Administratora w oparciu o wiedze i doświadczenie administratora systemu Informatycznego lub firmy zewnętrznej. Organizacja wprowadza następujące zasady wobec szyfrowania:
   a) po zaszyfrowaniu, na terenie organizacji przetrzymywane są klucze kryptograficzne w formie wydrukowanej lub elektronicznej z zachowaniem poufności danych;
   b) organizacja przy wyborze metody szyfrowania stosuje minimum metodę AES-256;

c) szyfrowaniu podlega cały wolumen dyskowy.

Podstawa prawna:

- Zgodnie z art. 32 pkt 1 lit. b) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
- Zgodnie z § 20 ust. 2 pkt 8, 12 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. 2017 poz. 2247).

W oparciu o:

- Norma PN-EN ISO/IEC 27001:2017 zał. A.6.2.1

5. Nadzór nad oprogramowaniem oraz zarządzanie zmianami i konfiguracją

1) Ilość i rodzaj oprogramowania instalowanego na stanowiskach roboczych oraz serwerze/ach jest nadzorowany przez Administratora Systemu Informatycznego.
2) Elementami składowymi nadzoru nad oprogramowaniem są:
   a) modyfikacje oprogramowania/systemu wynikające z bieżących potrzeb;
   b) parametryzacje i konfiguracje;
   c) instalacje nowych wersji oprogramowania oraz aktualizacji;
   d) konsultacje i przeszkolenia użytkowników;
   e) usuwanie błędów i awarii oprogramowania/systemu;
   f) opieka zdalna, z wykorzystaniem narzędzi zdalnego dostępu do danych.
3) Nadzór nad oprogramowaniem w organizacji wykonywany jest wymiennie poprzez:
   a) ewidencję oprogramowania
   b) elektroniczną ewidencję w postaci oprogramowania do inwentaryzacji zasobów sieciowych.
4) Zmiany konfiguracji oraz jej kopie wykonywane są tylko i wyłącznie przez Administratora Systemu Informatycznego lub wyspecjalizowanej firmy zewnętrznej.
5) Testy oprogramowania i konfiguracji wykonywane są przez Administratora Systemu Informatycznego lub firmę zewnętrzną na poziomie wyboru programu lub metodologii konfiguracji. W przypadku wystąpienia błędu, jest on natychmiast niwelowany poprzez poprawienie błędnej konfiguracji, zmianę metodologii konfiguracji lub zaniechanie instalacji oprogramowania lub wdrożenia konfiguracji.
6) Szkoła stosuje procedurę określania specyfikacji technicznych wymagań odbioru systemów IT. Tworząc wymagania (np. SIWZ) Administrator posiłkuje się wiedzą i doświadczeniem Administratora Systemu Informatycznego (lub firma zewnętrzna) oraz Inspektora Ochrony Danych. Wymagania bezwzględnie zawierają wytyczne w zakresie poufności, integralności i dostępności danych osobowych mając na uwadze zasadę rozliczalności. Każdy z tych elementów jest składową ryzyka wiążącego się z wprowadzaniem nowych technologii, zatem uwzględnia się całość.

7) Urząd wprowadza podział logów na sieciowe (router, firewall, UTM, switch) i stanowiskowe (komputer, serwer, NAS, drukarki i skanery).
8) Dostęp do logów posiada Administrator, Administrator Systemów Informatycznych oraz Inspektor Ochrony Danych. Logi są przechowywane wymiennie na urządzeniach je generujące lub serwerze syslog. Dostęp do logów ograniczony jest hasłem i loginem dostępowym do urządzenia.

Podstawa prawna:

- Zgodnie z art. 32 pkt 1 lit. b) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
- Zgodnie z § 20 ust. 1, 2, 2 pkt 2, § 21 ust. 2, 3, 4 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. 2017 poz. 2247).

W oparciu o:

- Norma PN-EN ISO/IEC 27001:2017 zał. A.12.5

6. Inwentaryzacja sprzętu

1) Proces inwentaryzacji sprzętu ma zapobiec utracie, uszkodzeniu, kradzieży lub utracie integralności aktywów oraz zakłóceniom w działaniu organizacji.
2) Wyniki kontroli i inwentaryzacji sprzętu zawierają się w **Ewidencji urządzeń elektronicznych przetwarzających dane osobowe.**

Podstawa prawna:

- Zgodnie z art. 32 pkt 1 lit. d) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.

W oparciu:

- Norma PN-EN ISO/IEC 27001:2017 zał. A.11.2

7. Kopie zapasowe

1) Dane, w tym dane osobowe przetwarzane w systemach teleinformatycznych podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada Administrator Systemu Informatycznego lub osoba specjalnie do tego celu wyznaczona.
2) Każdorazowo oraz okresowo po wykonaniu kopii bezpieczeństwa baz danych Administrator Systemu Informatycznego weryfikuje poprawność jej wykonania w sposób wymienny tj.:
   a) w przypadku serwera / programu archiwizacyjnego: oprogramowanie archiwizujące wykonuje automatyczną analizę poprawności wykonania i odczytu po wykonaniu kopii;

b) w przypadku samodzielnych stacji roboczych poprzez „ręczne" sprawdzenie poprawności wykonania kopii;
c) sposób oraz poprawność wykonania kopii potwierdzana jest w dokumencie „**Ewidencja kopii zapasowych"**

3) Nośniki kopii zapasowych, które zostały wycofane z użycia pozbawiane są zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych. W przeciwnym wypadku podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika, w sposób uniemożliwiający odczytanie zapisanych na nich danych.
4) Ponadto:
   a) Zbiory danych przechowywane są na serwerze obsługującym system teleinformatyczny. Wszelkie dane przetwarzane w pamięci poszczególnych stacji roboczych oraz komputerów przenośnych są niezwłocznie umieszczane w odpowiednich, przydzielonych dla danego użytkownika przez Administratora Systemu Informatycznego miejscach na serwerze lub innych wskazanych i określonych lokalizacjach.
   b) Zakazuje się zapisywania danych chronionych, w tym danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych, półprzewodnikowych i innych bez zaszyfrowania.
   c) Kopie zapasowe programów i aktualizowane kopie systemu teleinformatycznego przechowywane są w szafie zamykanej na klucz, stojącej w innym pomieszczeniu niż serwery.
   d) Po wygaśnięciu okresu przydatności kopii zapasowych (zastąpieniu ich przez aktualne wersje lub zakończeniu okresu trwałości), są one trwale kasowane lub nośniki je przechowujące niszczone są mechanicznie.

Podstawa prawna:

- Zgodnie z art. 32 pkt 1 lit. c) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.

W oparciu o:

- Norma PN-EN ISO/IEC 27001:2017 zał. A.12.3

8. Postępowanie z nośnikami

1) Administrator stosuje oraz dopuszcza wedle zapotrzebowania nośniki danych takie jak:
   a) nośnik magnetyczny: dysk twardy (HDD), RDX,
   b) nośnik optyczny: CD, DVD, BD,
   c) nośnik półprzewodnikowy: dysk SSD, pendrive oraz karta pamięci FLASH.

2) W przypadku posługiwania się nośnikiem danych pochodzącym od organizacji zewnętrznej, obligatoryjnym jest sprawdzenie go programem antywirusowym przez przynajmniej jedną osobę spośród wymienionych:
   a) Administrator,
   b) Inspektor Ochrony Danych,
   c) Administrator Systemu Informatycznego,
3) Nośniki danych mogą być używane tylko i wyłącznie na terenie organizacji lub na terenie organizacji, której to powierzono przetwarzanie danych poprzez stosowną umowę.
4) Nośniki magnetyczne i półprzewodnikowe raz użyte do przetwarzania danych osobowych mogą być wykorzystywane do innych celów, tylko po nadpisaniu danych w trybie kasowania formatującego przy zastosowaniu specjalistycznego oprogramowania lub demagnetyzacji. Nośniki, na których nie można powtórnie zapisać informacji, powinny być niszczone poprzez zniszczenie mechaniczne (pocięcie, zgniecenie, spopielenie itp.). Proces ten każdorazowo protokołowany jest za pomocą „**Protokołu utylizacji sprzętu pamięcionośnego" –**
5) Nośniki optyczne, których okres archiwizacji lub przydatności do przetwarzania zakończył się, niszczone są w sposób mechaniczny (pocięcie, zgniecenie, spopielenie itp.) . Proces ten każdorazowo protokołowany jest za pomocą „**Protokołu utylizacji sprzętu pamięcionośnego" –**
6) Zaszyfrowane nośniki półprzewodnikowe (dyski SSD, pendrive oraz karty pamięci FLASH) z jednostkowymi danymi osobowymi są – na czas ich użyteczności, przechowywane w zamkniętych na klucz szafach, a po wykorzystaniu dane na nich zawarte trwale usuwane, lub nośniki są niszczone w sposób mechaniczny (pocięcie, zgniecenie itp.). Proces ten każdorazowo protokołowany jest za pomocą „**Protokołu utylizacji sprzętu pamięcionośnego**" –

Podstawa prawna:

- Zgodnie z art. 32 pkt 1 lit. c) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
- Zgodnie z § 20 ust. 1, 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. 2017 Poz. 2247).

W oparciu o:

- Norma PN-EN ISO/IEC 27001: 2017 zał. A.8.3

9. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

1) Administrator zapewnia warunki dla uzyskania odpowiedniej funkcjonalności, niezawodności, używalności, wydajności, przenaszalności i pielęgnowalności systemów informatycznych w fazie ich projektowania, wdrażania i eksploatacji.
2) Regulacje wewnętrzne opisują wymagania w zakresie projektowania systemów teleinformatycznych w podmiocie w zakresie:
   a) Architektury systemu;
   b) Sposobu licencjonowania i wykorzystania praw autorskich → tylko oprogramowanie zakupione lub z otwartą licencją;
   c) Zgodności z obowiązującym prawem m.in. ustawą o informatyzacji podmiotów realizujących zadania publiczne → organizacja zapewnia edytowalność i odczytywalność plików zgodnie z Rozporządzeniem 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. 2017 poz. 2247).
   d) sposobu i poziomu zabezpieczeń → określonego niniejszą Instrukcją,
   e) zastosowania norm i standardów przemysłowych → określonych w legislacji niniejszej Polityki,
   f) zastosowania rozwiązań funkcjonalnych odpowiednich dla osiągnięcia założonych celów → określonych w legislacji niniejszej Polityki,
   g) wydajności, poziomu niezawodności SLA → określone w legislacji niniejszej Polityki,
   h) mechanizmów kontroli i audytu → określonych w Analizie Ryzyka Ogólnego oraz Ocenie Skutków (DPIA).
3) Regulacje wewnętrzne opisujące wymagania w zakresie wdrażania systemów teleinformatycznych w organizacji w zakresie: sposobu dostarczenia i instalacji systemu teleinformatycznego, wymagań sprzętowych i środowiskowych dla systemu, sposobu i zakresu testów odbiorowych oraz rodzaju i zakresu dokumentacji, a także warunków i kryteriów odbioru ustalane są indywidualnie wobec zamówienia.

Podstawa prawna:

- Zgodnie z § 15 ust. 1 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. 2017 poz. 2247).

§ 5

Minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej

1. Usługi elektroniczne

1) Administrator realizuje usługi elektroniczne wobec obywateli i innych podmiotów celem załatwiania spraw urzędowych w sposób elektroniczny za pomocą ESP udostępnionej na platformie ePUAP.
2) Administrator zamieszcza na swojej głównej stronie internetowej (lub/oraz na BIP lub/oraz portalu interesanta) odesłania do opisów usług, które zawierają wymagane informacje dotyczące:
   a) aktualnej podstawy prawnej świadczonych usług;
   b) nazwy usług, miejsca świadczenia usług (złożenia dokumentów);
   c) terminu składania i załatwiania spraw;
   d) nazwy komórek odpowiedzialnych za załatwienie spraw.

Podstawa prawna:

- Zgodnie z § 5 ust. 2 pkt 1; 4 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. 2017 poz. 2247).
- Zgodnie z art. 16 ust. 1a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

2. Centralne repozytorium wzorów dokumentów elektronicznych (CRWDE)

1) Szkoła przekazuje do centralnego repozytorium (prowadzonego w ramach ePUAP przez Ministra właściwego do spraw informatyzacji) wzory dokumentów elektronicznych zgodnie z § 12 ust. 1 rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych.

2) Szkoła zgodnie z ww. rozporządzeniem stosuje się do:

   a) zasad tworzenia i oznaczania metadanych opisujących wzór;

   b) trybu przekazywania wzorów dokumentów elektronicznych do centralnego repozytorium;

   c) sposobu oznaczania w pismach w postaci elektronicznej niezbędnych elementów struktury.

3) Szkoła kompletuje i archiwizuje wnioski przekazania wzorów dokumentów elektronicznych do CRWDE za pomocą ESP udostępnionej na platformie ePUAP.

Podstawa prawna:

- Zgodnie z art. 19b ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.
- Zgodnie z § 12 ust. 1 rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych.

3. Model usługowy

1) Szkoła stosuje model usługowy SOA, w którym dla użytkowników zdefiniowano stanowiące odrębną całość funkcje systemu teleinformatycznego (usługi sieciowe). Model ten kładzie główny nacisk na definiowanie usług, które spełnią wymagania użytkownika.

4. Współpraca systemów teleinformatycznych z innymi systemami

1) Szkoła osiąga interoperacyjność na poziomie semantycznym przez stosowanie we własnych prowadzonych rejestrach odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań.

2) Systemy teleinformatyczne używane przez organizację wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.

3) W przypadku współpracy z podmiotami prowadzącymi rejestry referencyjne dotyczące dostępu do danych referencyjnych uzyskiwanych w drodze wymiany organizacja stosuje umowę powierzenia z uwzględnieniem atrybutów poufności, dostępności i integralności oraz opisane są interfejsy dostępowe systemu teleinformatycznego – sposób wymiany informacji.

Podstawa prawna:

- Zgodnie z § 5 ust. 3 pkt 3 oraz § 16 ust. 1 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. 2017 poz. 2247).

5. Obieg dokumentów

1) Szkoła stosuje zabezpieczanie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie zgodnie z:

   a) wymienionymi zapisami niniejszej Instrukcji oraz,

   b) procedurami i zasadami postępowania z dokumentami zawartymi w instrukcjach kancelaryjnych, oraz ustawie z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

Podstawa prawna:

- Zgodnie z § 20 ust. 2 pkt 9 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. 2017 poz. 2247).

6. Formaty danych udostępniane przez systemy teleinformatyczne

1) Szkoła stosuje kodowanie znaków wg standardu Unicode UTF-8 lub/oraz UTF-16 w dokumentach wysyłanych z systemu teleinformatycznego (także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji). W przypadku systemów z rodziny Windows dopuszcza się normy zamienne, kompatybilne ze standardem UTF-8.

2) System teleinformatyczny organizacji udostępnia zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 (formaty danych oraz standardy zapewniające dostęp do zasobów informacji udostępnianych za pomocą systemów teleinformatycznych używanych do realizacji zadań publicznych) do 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. 2017 poz. 2247).

3) System teleinformatyczny organizacji umożliwia przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu działania podmiotu w formatach danych określonych w załącznikach nr 2 (formaty danych oraz standardy zapewniające dostęp do zasobów informacji udostępnianych za pomocą systemów teleinformatycznych używanych do realizacji zadań publicznych) i 3 (formaty danych obsługiwane przez podmiot realizujący zadanie publiczne w trybie odczytu) do 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. 2017 poz. 2247).

Podstawa prawna:

- Zgodnie z § 17 ust. 1; § 18 ust. 1; § 18 ust. 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. 2017 poz. 2247).

W oparciu o:

- Norma ISO/IEC 10646:2017