Zespół Szkolno-Przedszkolny Nr 2
ul. Jagiellońska 67, 05-120 Legionowo
tel. 22 774 27 54, fax 22 764 10 65
REGON 146091860 NIP 536-191-15-24

ZSP2.021.2.49.2022

Zarządzenie nr 49/2022

Dyrektora Zespołu Szkolno-Przedszkolnego nr 2 w Legionowie

z dnia 14.11.2022 r.

w sprawie: **Polityki Bezpieczeństwa Informacji**

§1

Załącznik nr 13 w Polityce Bezpieczeństwa Informacji, przyjętym Zarządzeniem Dyrektora Zespołu Szkolno-Przedszkolnego nr 2 w Legionowie z dnia 14.11.2022 r. otrzymuje brzmienie stanowiące załącznik nr 1 do niniejszego Zarządzenia.

§2

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik 1/5:

1. Załącznik nr 13 do Polityki Bezpieczeństwa Informacji

Dyrektor
Zespołu Szkolno-Przedszkolnego Nr 2
w Legionowie
mgr Dorota Kuchta

AKTUALIZACJA 12.2022 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

WSTĘP

Instrukcja stanowi wykaz procedur oraz stosowanych środków technicznych i organizacyjnych mających na celu, zgodnie z Art. 32 RODO, zabezpieczyć przetwarzane dane osobowe przed: przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych oraz nieuprawnionym dostępem do danych osobowych

1. ZABEZPIECZENIA FIZYCZNE

1. drzwi do pomieszczeń biurowych, archiwów zamykane są na klucz
2. drzwi do serwerowni zamykane są na klucz oraz kartę dostępową
3. dokumentację papierową i nośniki elektroniczne przechowywaną w pomieszczeniach zabezpieczono w szafach zamykanych na klucz
4. stosowany jest system alarmowy oraz rolety okienne
5. zapewniono ochronę obiektu - ochrona własna

2. ZABEZPIECZENIA TECHNICZNE

1. zastosowano UPS do serwera, sieć stabilizowana
2. zastosowano monitoring wizyjny w obrębie obiektu i w otoczeniu
3. serwerownia wyposażona w gaśnice
4. powiadamianie administratora systemu informatycznego o alertach temperatury serwerowni
5. system gaszenia pożaru
6. klimatyzacja w serwerowni
7.

3. UPRAWNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH.

Procedurę nadawania uprawnień do przetwarzania danych osobowych określa **Regulamin Ochrony Danych Osobowych** stanowiący **Załącznik nr 7 do PBI.**

AKTUALIZACJA 12.2022 r.

4. METODY I ŚRODKI UWIERZYTELNIENIA (POLITYKA HASEŁ)

Metody i środki uwierzytelnienia określa procedura opisana w **Regulaminie Ochrony Danych Osobowych** stanowiącym **Załącznik nr 7 do PBI.**

5. PROCEDURA TWORZENIA KOPII ZAPASOWYCH

Celem procedury jest minimalizacja ryzyka przetwarzania danych przez osoby nieupoważnione.

1. Dostęp do systemów informatycznych nadawany jest każdemu użytkownikowi w formie indywidualnego identyfikatora (loginu)
2. Nadawanie, zmiana, odbieranie uprawnień użytkownika do systemów informatycznych odbywa się na polecenie przełożonych (lub innych osób upoważnionych) w formie maila od przełożonego
3. Za wykonanie czynności nadawania, zmiany, odbierania uprawnień użytkownikowi odpowiada kierownik administracyjny lub informatyk
4. Obowiązuje zasada minimalizacji uprawnień
5. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika. Zasada ta obowiązuje również administratorów systemów.

6. UTYLIZACJA ELEKTRONICZNYCH NOŚNIKÓW I WYDRUKÓW ORAZ CZYSZCZENIE DANYCH

1. Podlegające likwidacji uszkodzone lub przestarzałe nośniki są niszczone w sposób fizyczny
2. Nośniki informacji muszą być wyczyszczone specjalistycznym oprogramowaniem zanim zostaną przekazane poza obszar organizacji
3. Dokumentacja papierowa niszczona jest w niszczarkach/za pośrednictwem zewnętrznej firmy

7. PROCEDURA ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO

7.1.Bezpieczeństwo przetwarzania danych poza organizacją

1. Użytkownicy komputerów przenośnych wynoszonych poza obszar organizacji są zobowiązani do stosowania **Regulaminu użytkowania komputerów przenośnych** stanowiącego **Załącznik nr 1** do niniejszej instrukcji.
2. Dane osobowe na komputerach przenośnych wynoszonych poza obszar organizacji muszą być przechowywane na zaszyfrowanych partycjach.
3. Dyski przenośne / pendrive wynoszone poza organizację muszą być zaszyfrowane.

Zespół Szkolno-Przedszkolny Nr 2
ul. Jagiellońska 67, 05-120 Legionowo
tel. 22 774 27 54, fax 22 764 10 65
REGON 146091860 NIP 536-191-15-24

AKTUALIZACJA 12.2022 r.

4. Sprzęt mobilny (smartfony/tablety) zabezpieczono mechanizmem uwierzytelniania.

7.2.Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów

1. Dokonuje się konfiguracji urządzeń sieciowych oraz sprzętu IT w celu zabezpieczenia przed nieuprawnionym dostępem do nich
2. Dokonuje się aktualizacji oprogramowania systemów i aplikacji.
3. Stosowany jest monitoring usług sieciowych w celu dezaktywacji nieużywanych
4. Zastosowano system antywirusowy i filtr antyspamowy
5. Stosowany jest Firewall
6. Zastosowano mechanizmy kontroli dostępu do sieci w postaci: (IDS/IPS do wykrywania i blokowania ataków do sieci komputerowej, technikę NAT
7. Zastosowano Sewery proxy/bramki filtrujące
8. Separacja sieci wewnętrznej od sieci przeznaczonej dla gości (dla wifi i dla Ethernet) np. w salach konferencyjnych
9. Zabezpieczenie baz i katalogów webowych przed indeksacją wyszukiwarek

7.3. Zabezpieczenia infrastruktury IT

1. Zapewniono redundantne łącze internetowe.
2. Serwer wyposażono w macierz dyskową.
3. Zastosowano wirtualizację serwera.
4. Zabezpieczono hasłem dostęp do portów fizycznych.
5. Ustawienie monitorów uniemożliwiające wgląd w dane przez osoby postronne.
6. Prowadzenie monitoringu sposobu korzystania przez pracowników z komputerów służbowych, z zastrzeżeniem poszanowania dóbr osobistych pracownika, przepisów o ochronie danych osobowych oraz innych powszechnie obowiązujących przepisów prawa.

7.4 Zabezpieczenia aplikacji

1. W kluczowych aplikacjach stosuje się terminację sesji.
2. Stosuje się szyfrowanie poczty wychodzącej (SSL).
3. Dla aplikacji webowych stosowane jest szyfrowanie z użyciem protokołu SSL.
4. Formularze kontaktowe na stronach www zabezpieczono protokołem SSL.

AKTUALIZACJA 12.2022 r.

8. PROCEDURA WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI

1. Administrator odpowiada za optymalizację zasobów IT.
2. Administrator/Informatyk odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach oraz za poprawność działania zasobów IT.
3. W przypadku napraw dokonywanych na zewnątrz, z komputerów i urządzeń mobilnych należy usunąć nośniki danych lub usunąć te dane.
4. W przypadku naprawy sprzętu z danymi osobowymi na nośniku wymaga się „usługi bezpiecznej naprawy".
5. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw on-site.
6. Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych muszą być wykonywane pod nadzorem osób upoważnionych.

INSPEKTOR OCHRONY DANYCH
Izabela Remjasz

Inspektor Ochrony Danych

Dyrektor
Zespołu Szkolno-Przedszkolnego Nr 2
w Legionowie
mgr Dorota Kuchta

Administrator Systemów Informatycznych