WIELOZAWODOWY ZESPÓŁ SZKÓŁ

W ZATORZE

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM w WIELOZAWODOWYM ZESPOLE SZKÓŁ W ZATORZE

ZATOR, ...02.01.2017 r.

§1
Postanowienia ogólne

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Wielozawodowym Zespole Szkół w Zatorze, zwana dalej „Instrukcją" określa zasady, tryb postępowania i zalecenia Administratora Danych, które muszą być stosowane przez osoby przez niego upoważnione do przetwarzania danych osobowych w systemach informatycznych.
2. Podstawowymi celami zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych jest zapewnienie jak najwyższego poziomu bezpieczeństwa przetwarzanych danych osobowych w systemach informatycznych.
3. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania w systemach, charakteru poufnego wraz z zachowaniem ich integralności i rozliczalności.

§ 2
Obowiązki Administratora Danych

1. Administrator danych zobowiązany jest do zapewnienia, aby dane osobowe były:
   a) przetwarzane zgodnie z prawem,
   b) zbierane dla oznaczonych, zgodnych z prawem celów,
   c) merytorycznie poprawne i adekwatne w stosunku do celów.
2. Wyznacza osobę, zwaną dalej Administratorem Bezpieczeństwa Informacji, odpowiedzialnym za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.
3. Opracowuje instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych.
4. Określa budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.
5. Opracowuje instrukcję, określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.
6. Prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych w poszczególnych systemach.
7. Organizuje szkolenia mające na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.
8. Odpowiada za to by zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych określał odpowiedzialność tej osoby za:
   a) ochronę danych przed niepowołanym dostępem,
   b) nieuzasadnioną modyfikację lub zniszczenie danych,
   c) nielegalne ujawnienie danych.

w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.

§ 3
Obowiązki Administratora Bezpieczeństwa Informacji

1. Nadzór na przestrzeganiem instrukcji określającej sposób zarządzania systemem informatycznym.
2. Nadzór nad właściwym zabezpieczeniem sprzętu oraz pomieszczeń, w których przetwarzane są dane osobowe.

3. Nadzór nad wykorzystywanym w szkole oprogramowaniem oraz jego legalnością.
4. Przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe.
5. Podejmowanie odpowiednich działań w celu właściwego zabezpieczenia danych.
6. Badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych.
7. Podejmowanie decyzji o instalowaniu nowych urządzeń oraz oprogramowania wykorzystywanego do przetwarzania danych osobowych.
8. Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe.
9. Definiowanie użytkowników i haseł dostępu.
10. Nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności.
11. Wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych.
12. Sporządzanie raportów z naruszenia bezpieczeństwa systemu informatycznego.

§ 4

Obowiązki pełnomocnika dyrektora ds. konserwacji i zabezpieczeń szkolnej sieci komputerowej, aktualizacji oprogramowania i zabezpieczeń komputerów

1. Naprawa, konserwacja oraz likwidacja urządzeń komputerowych zawierających dane osobowe.
2. Aktualizowanie oprogramowania antywirusowego i innego, chyba że aktualizacje te wykonywane są automatycznie.
3. Regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych.
4. Wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami, sprzętu IT, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe.
5. Współdziałanie z ABI w ochronie szkolnych systemów informatycznych.
6. Konsultacje, udzielanie wsparcia ABI w podejmowaniu decyzji i instalacji aktualizacji, instalacji wdrażania nowych programów, ustalania sposobów generowania haseł zabezpieczających informację.
7. Odpowiedzialność za bezpieczne korzystanie ze sprzętu komputerowego, jego sprawność techniczną i używanie zgodnie z przeznaczeniem.

§5

Obowiązki użytkowników

Do obowiązków użytkowników systemu informatycznego w zakresie ochrony danych osobowych w systemach informatycznych należy w szczególności:

1. Przestrzeganie opracowanych dla systemu zasad przetwarzania danych osobowych.
2. Przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa.
3. Udostępnianie danych osobowych wyłącznie osobom upoważnionym lub uprawnionym do ich uzyskania.
4. Uniemożliwianie dostępu lub podglądu danych osobowych w systemie dla osób nieupoważnionych.
5. Informowanie Administratora Bezpieczeństwa Informacji o wszystkich naruszeniach, podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych.

6. Wykonywanie bez zbędnej zwłoki poleceń ABI w zakresie ochrony danych osobowych jeśli są one zgodne z przepisami prawa powszechnie obowiązującego.

§6
Bezpieczna eksploatacja systemów informatycznych

Bezpieczna eksploatacja systemów informatycznych przetwarzających dane osobowe zostaje zapewniona przez przestrzeganie następujących zasad:

1. Użytkownikom zabrania się wprowadzania zmian do oprogramowania, sprzętu informatycznego poprzez jego samodzielne konfigurowanie i wyposażanie.
2. Użytkownikom zabrania się umożliwiania stronom trzecim uzyskiwania nieupoważnionego dostępu do systemów informatycznym.
3. Użytkownikom nie wolno instalować nowego lub aktualizować już zainstalowanego oprogramowania.
4. Użytkownikom nie wolno korzystać z systemów informatycznych dla celów innych niż związane z wykonywaniem obowiązków służbowych.
5. Użytkownikom nie wolno podejmować prób testowania, modyfikacji i naruszenia zabezpieczeń systemów informatycznych lub jakichkolwiek działań noszących takie znamiona.
6. Informacje przetwarzane przy użyciu współdzielonych aplikacji sieciowych na stacjach roboczych muszą być zapisywane na dyskach serwera.
7. Wszystkie aplikacje sieciowe, współdzielone zasoby użytkowe muszą być ulokowane na przeznaczonych do tego celu serwerach.
8. Nieautoryzowane podłączenie własnego lub strony trzeciej urządzenia teleinformatycznego do systemu informatycznego Wielozawodowego Zespołu Szkół w Zatorze jest zabronione.

§ 7
Nadawanie uprawnień do przetwarzania danych osobowych

1. Użytkownicy systemu przetwarzającego dane osobowe przed przystąpieniem do przetwarzania danych osobowych w tym systemie informatycznym, zobowiązani są zapoznać się z:
   a) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135 z późn. zm.).
   b) Polityką bezpieczeństwa przetwarzania danych osobowych w Wielozawodowym Zespole Szkół w Zatorze.
2. Użytkownicy przed dopuszczeniem do obsługi systemu informatycznego, w którym przetwarzane są dane osobowe powinni podlegać przeszkoleniu w zakresie obsługi sprzętu informatycznego, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, którą będą wykorzystywali.
3. Pierwsze zarejestrowanie użytkownika w systemie i nadanie odpowiednich uprawnień do systemu przetwarzającego dane osobowe musi być poprzedzone złożeniem przez użytkownika oświadczenia o:
   a) Zachowaniu w tajemnicy danych osobowych i sposobów ich zabezpieczania oraz przetwarzaniu danych osobowych zgodnie z przepisami.
   b) Uzyskanie formalnego upoważnienia do przetwarzania danych osobowych.
4. Wzory oświadczenia oraz upoważnienia stanowią załączniki nr 1 i 2 do „Polityki bezpieczeństwa przetwarzania danych osobowych w Wielozawodowym Zespole Szkół w Zatorze"
5. Identyfikator oraz zakres dostępu użytkownika powinien być rejestrowany w ewidencji osób upoważnionych do przetwarzania danych osobowych. Ewidencja osób upoważnionych do przetwarzania danych osobowych stanowi załącznik nr 3 do „Polityki bezpieczeństwa przetwarzania danych osobowych w Wielozawodowym Zespole Szkół w Zatorze".

6. Administratorzy Systemu powinni przekazywać użytkownikom tymczasowe hasła dostępowe w sposób bezpieczny. W tym celu powinni unikać pośrednictwa osób trzecich lub korzystania do tego celu z niechronionych wiadomości poczty elektronicznej.
7. Procedurę nadawania uprawnień do przetwarzania danych osobowych w systemach należy stosować odpowiednio, w przypadku zmiany uprawnień w systemach lub w przypadku odebrania uprawnień w systemach. Wzór odwołania upoważnienia stanowi załącznik nr 2A do „Polityki bezpieczeństwa".
8. Zmiany dotyczące użytkownika, takie jak rozwiązanie umowy o pracę lub utrata upoważnienia, są przesłanką do natychmiastowego wyrejestrowania użytkownika z systemu oraz unieważnienia hasła i odnotowanie tego faktu w ewidencji osób upoważnionych do przetwarzania danych osobowych, o której mowa w ust. 3.
9. Prawa dostępu przyznane użytkownikom, którzy nie są pracownikami etatowymi Wielozawodowego Zespołu Szkół w Zatorze powinny mieć charakter czasowy i mogą być przyznawane na okres odpowiadający wykonywanemu zadaniu.
10. Dostęp do systemu informatycznego, a także do poszczególnych aplikacji i baz danych przetwarzających dane osobowe powinien być możliwy tylko po podaniu identyfikatora odrębnego dla każdego użytkownika i poufnego hasła.

§8
Metody i środki uwierzytelniania w systemie

1. Identyfikatory i hasła są sposobem zagwarantowania rozliczalności, poufności i integralności danych osobowych przetwarzanych w systemach informatycznych. Służą do weryfikowania tożsamości użytkownika, uzyskania dostępu do określonych zasobów, kont uprzywilejowanych lub uruchomienia określonej funkcjonalności.
2. Mając na uwadze zagwarantowanie wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych oraz zagwarantowania użytkownikom pełnej rozliczalności wykonywanych przez nich operacji w systemach informatycznych, wszyscy użytkownicy przy uwierzytelnianiu do systemów informatycznych powinni stosować się do poniższych zasad:
   a) Użytkownik systemu powinien posiadać unikalny identyfikator do swojego osobistego i wyłącznego użytku.
   b) Hasła dostępu do systemów informatycznych powinny być tworzone przez użytkownika i stanowią tajemnicę służbową.
   c) Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła dostępu oraz jego przechowywanie.
   d) Hasła nie mogą być ujawniane lub przekazywane komukolwiek, bez względu na okoliczności.
   e) Użytkownik nie powinien przechowywać haseł w widocznych miejscach, nie powinien umieszczać haseł w żadnych automatycznych procesach logowania (skryptach, makrach lub pod klawiszami funkcyjnymi).
3. Użytkownicy są odpowiedzialni za wszelkie działania w systemach informatycznych prowadzone z użyciem ich identyfikatora i hasła.
4. Administratorzy Systemu są odpowiedzialni za okresowe sprawdzanie, usuwanie lub blokowanie zbędnych identyfikatorów użytkowników oraz kont w systemach, za które są odpowiedzialni.

§9
Wymogi dotyczące uwierzytelniania

1. Wszystkie konta dostępowe (identyfikatory) do systemów informatycznych powinny być chronione hasłem lub innym bezpiecznym, zaakceptowanym przez Administratora Bezpieczeństwa Informacji sposobem uwierzytelniania.
2. Identyfikator oraz nadane uprawnienia powinny umożliwiać wykonywanie czynności wyłącznie zgodnych z zakresem powierzonych obowiązków.

3. Identyfikator użytkownika powinien być niepowtarzalny, a po wyrejestrowaniu się z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.
5. Hasło początkowe, które jest przydzielane przez Administratora Systemu, powinno umożliwiać użytkownikowi zarejestrowanie się w systemie tylko jeden raz i powinno być natychmiast zmienione przez użytkownika.
6. **Użytkownicy powinny wybierać hasła dobrej jakości:**
   a) **Długości co najmniej 8 znaków.**
   b) **Które są łatwe do zapamiętania, a trudne do odgadnięcia.**
   c) **Nie są oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących właściciela konta (np. imię, nazwisko, numer telefonu, data urodzenia itp.).**
   d) **W których występuje przynajmniej jedna duża litera, jedna mała litera, jedna cyfra lub znak specjalny.**
   e) **W których nie występują kolejne znaki, które nie są topologiczne (tzn. wynikające z układu klawiszy na klawiaturze, typu „qwer5,itp.**
7. Hasła nie mogą być takie same jak identyfikator użytkownika oraz nie mogą być zapisywane w systemach w postaci jawnej.
8. Hasła powinny być utrzymywane w tajemnicy również po upływie ich ważności.
9. Należy unikać ponownego lub cyklicznego używania starych haseł.
10. Hasła użytkowników o wysokich uprawnieniach powinny być przechowywane w miejscu zabezpieczonym przed dostępem osób nieupoważnionych.
11. Rutynowe działania użytkownika nie powinny być prowadzone z wykorzystaniem kont uprzywilejowanych.
12. Udostępnienie hasła osobie postronnej należy traktować jako poważny incydent naruszenia ochrony danych osobowych.

§10
Wymogi dotyczące zmiany haseł

1. Użytkownik jest zobowiązany zmieniać hasło, w którego posiadaniu się znajduje:
   a) Okresowo, zgodnie z wymaganiami dla danego systemu informatycznego (przed upływem terminu ważności hasła).
   b) W przypadku ujawnienia lub podejrzenia ujawnienia hasła.
2. W przypadku braku dostępu do konta chronionego hasłem, w którego posiadaniu się znajduje, użytkownik zobowiązany jest wystąpić o zmianę hasła do właściwego Administratora Systemu, w sytuacji:
   a) Zapomnienia/zgubienia hasła.
   b) Wygaśnięcia ważności hasła.
   c) Zablokowania konta spowodowanego nieprawidłowym wprowadzeniem hasła.
   d) Braku uprawnień/interfejsu umożliwiających samodzielną zmianę hasła.
3. Zmiana haseł użytkowników powinna być wymuszana przez system co 30 dni, w przypadku braku wymuszenia przez system, użytkownik sam jest zobowiązany do zmiany hasła co 30 dni.

§ 11
Procedury rozpoczęcia, zawieszenia i zakończenia pracy.

1. Dane osobowe, których administratorem jest Wielozawodowy Zespół Szkół w Zatorze mogą być przetwarzane sposobem tradycyjnym lub z użyciem systemu informatycznego tylko na potrzeby realizowania zadań statutowych i organizacyjnych szkoły;
2. Rozpoczęcie pracy użytkownika w systemie informatycznym następuje po poprawnym uwierzytelnieniu (zalogowaniu się do systemu);

3. Rozpoczęcie pracy w aplikacji musi być przeprowadzone zgodnie z instrukcją zawartą w dokumentacji aplikacji;
4. Zakończenie pracy użytkownika następuje po poprawnym wylogowaniu się z systemu oraz poprzez uruchomienie odpowiedniej dla danego systemu opcji jego zamknięcia zgodnie z instrukcją zawartą w dokumentacji;
5. Niedopuszczalne jest zakończenie pracy w systemie bez wykonania pełnej i poprawnej operacji wylogowania z aplikacji i poprawnego zamknięcia systemu;
6. Monitory stanowisk komputerowych znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, a na których przetwarzane są dane osobowe należy ustawić w taki sposób, aby uniemożliwić osobom postronnym wgląd w dane;
7. Użytkownik ma obowiązek wylogowania się w przypadku zakończenia pracy. Stanowisko komputerowe nie może pozostać z uruchomionym i dostępnym systemem bez nadzoru pracującego na nim pracownika;
8. Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym ich odczytanie przez osoby postronne. Wydruki nieprzydatne należy zniszczyć w stopniu uniemożliwiającym ich odczytanie w niszczarce dokumentów;
9. Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania;
10. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać, na czas nieobecności osób zatrudnionych, w sposób uniemożliwiający dostęp do nich osobom trzecim;
11. Użytkownik niezwłocznie powiadamia Administratora Bezpieczeństwa Informacji w przypadku podejrzenia fizycznej ingerencji w przetwarzane dane osobowe lub użytkowane narzędzia programowe lub sprzętowe. Wówczas, użytkownik jest zobowiązany do natychmiastowego wyłączenia sprzętu.

§ 17

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi do ich przetwarzania.

1. Zbiory danych osobowych w systemie informatycznym są zabezpieczane przed utratą lub uszkodzeniem za pomocą:
    a) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,
    b) sporządzanie kopii zapasowych (kopie pełne).
2. Pełne kopie zapasowe zbiorów danych tworzone są 2 razy w ciągu roku;
3. W szczególnych sytuacjach, np. przed aktualizacją lub zmianą oprogramowania lub systemu należy wykonać bezwzględnie pełną kopię zapasową systemu;
4. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Za przeprowadzenie tych czynności odpowiada Administrator Bezpieczeństwa Informacji;
5. Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych

§ 18

Przechowywanie nośników elektronicznych zawierających dane osobowe

1. Dane osobowe mogą być przechowywane:

a) Na serwerach zlokalizowanych w obszarach wyznaczonych do przetwarzania danych osobowych.
b) Na wymiennych nośnikach elektronicznych.

2. Po wykorzystaniu dane osobowe w postaci elektronicznej należy niezwłocznie usunąć z nośnika elektronicznego w sposób uniemożliwiający ich ponowne odtworzenie.
3. Wykorzystanie wymiennych nośników elektronicznych (CD/DVD, pamięć USB, wymienna karta pamięci, dyskietka) powinno być ściśle kontrolowane i dozwolone wyłącznie dla upoważnionych użytkowników.
4. Wymienne nośniki elektroniczne, o ile nie są użytkowane, powinny być przechowywane w zamykanych szafkach.
5. Nośniki zawierające kopie zapasowe powinny być przechowywane w innym pomieszczeniu niż to, w którym umieszczony jest serwer przetwarzający dane osobowe.
6. Kopie zapasowe powinny być przechowywane w odpowiednio zabezpieczonej, ognioodpornej szafie, do której dostęp mogą mieć wyłącznie osoby upoważnione.
7. Nośniki magnetyczne i optyczne z danymi osobowymi powinny być:
   a) Oznaczane i przechowywane w zamykanych szafach lub sejfach.
   b) Przechowywane maksymalnie przez okres wskazany dla danego rodzaju danych osobowych przez Administratora Bezpieczeństwa Informacji.
8. Informację o maksymalnym okresie przechowywania nośników magnetycznych oraz optycznych, na których zapisane są dane osobowe przekazują Właściciele zasobów danych osobowych do Administratora Bezpieczeństwa Informacji.

§ 19

Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. W związku z istnieniem zagrożenia dla zbiorów danych osobowych, ze strony wirusów komputerowych, których celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, konieczna jest ochrona sieci komputerowej i stanowisk komputerowych.
2. Wirusy komputerowe mogą pojawić się w systemach szkoły poprzez: Internet, nośniki informacji takie jak: dyskietki, płyty CD, dyski przenośne, itp.
3. Przeciwdziałanie zagrożeniom ze strony wirusów komputerowych realizowane jest następująco:
   a) Komputer z dostępem do Internetu musi być zabezpieczony za pomocą oprogramowania antywirusowego.
   b) Zainstalowany program antywirusowy powinien być tak skonfigurowany, by co najmniej raz w tygodniu dokonywał aktualizacji bazy wirusów oraz co najmniej raz w tygodniu dokonywane było automatycznie sprawdzenie komputera pod kątem obecności wirusów komputerowych.
   c) Elektroniczne nośniki informacji takie jak dyskietki, dyski przenośne, należy każdorazowo sprawdzać programem antywirusowym przed użyciem, po zainstalowaniu ich w systemie. Czynność powyższą realizuje użytkownik systemu. W przypadku problemów ze sprawdzeniem zewnętrznego nośnika danych użytkownik jest zobowiązany zwrócić się z tym do Administratora Bezpieczeństwa Informacji.
   d) Komputery i systemy pracujące muszą mieć zainstalowany program antywirusowy, a w przypadku komputerów z dostępem do Internetu, również posiadać oprogramowanie i mechanizmy zabezpieczające przed nieautoryzowanym dostępem z sieci (firewall).
   e) W przypadku, gdy użytkownik stanowiska komputerowego zauważy komunikat oprogramowania zabezpieczającego system wskazujący na zaistnienie zagrożenia lub rozpozna tego typu zagrożenie, zobowiązany jest zaprzestać jakichkolwiek czynności

w systemie i niezwłocznie skontaktować się z Administratorem Bezpieczeństwa Informacji.

f) 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.

g) Zabrania się użytkownikom komputerów, wyłączania, blokowania odinstalowywania programów zabezpieczających komputer (skaner antywirusowy, firewall) przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem.

§
20

Udostępnianie danych osobowych i sposób odnotowania informacji o udostępnionych danych.

1. Udostępnienie danych instytucjom może odbywać się wyłącznie na pisemny uzasadniony wniosek lub zgodnie z przepisami prawa (OKE, CKE, Urząd Gminy, itp.).

§21
Zasady monitorowania, przeglądu i konserwacji systemu informatycznego

1. Przeglądy i konserwacje systemu oraz zbiorów danych wykonuje Pełnomocnik dyrektora ds. konserwacji i zabezpieczeń szkolnej sieci komputerowej na bieżąco.
2. Administrator Bezpieczeństwa Informacji okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej.
3. Umowy dotyczące instalacji i konserwacji sprzętu należy zawierać z podmiotami, których kompetencje nie budzą wątpliwości, co do wykonania usługi oraz których wiarygodność finansowa zostały sprawdzone na rynku.
4. Naprawy sprzętu należy zlecać podmiotom, których kompetencje nie budzą wątpliwości, co do wykonania usługi. Naprawa sprzętu, na którym mogą znajdować się dane osobowe powinna odbywać się pod nadzorem osób użytkujących sprzęt oraz Pełnomocnika dyrektora ds. konserwacji i zabezpieczeń szkolnej sieci komputerowej w miejscu jego użytkowania.
5. W przypadku konieczności naprawy poza miejscem użytkowania, sprzęt komputerowy, przed oddaniem do serwisu, powinien być odpowiednio przygotowany. Dane należy zarchiwizować na nośniki informacji, a dyski twarde, bezwzględnie, wymontować na czas naprawy.
6. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą Administratora Bezpieczeństwa Informacji.

§ 22.

Ustalenia końcowe

1. Osobom korzystającym z systemu informatycznego, w którym przetwarzane są dane osobowe w szkole zabrania się:
   a) ujawniania loginu i hasła współpracownikom i osobom z zewnątrz,
   b) pozostawiania haseł w miejscach widocznych dla innych osób,
   c) udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,
   d) udostępniania osobom nieuprawnionym programów komputerowych zainstalowanych w systemie,
   e) używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna,

f) przenoszenia programów komputerowych, dysków twardych z jednego stanowiska na inne,

g) kopiowania danych na nośniki informacji, kopiowania na inne systemy celem wynoszenia ich poza szkołę,

h) samowolnego instalowania i używania jakichkolwiek programów komputerowych w tym również programów do użytku prywatnego; programy komputerowe instalowane są przez Administratora Bezpieczeństwa Informacji,

i) używania nośników danych udostępnionych przez osoby postronne,

j) przesyłania dokumentów i danych z wykorzystaniem konta pocztowego prywatnego (niesłużbowego),

k) otwierania załączników i wiadomości poczty elektronicznej od nieznanych i „niezaufanych" nadawców,

l) używania nośników danych niesprawdzonych, niewiadomego pochodzenia lub niezwiązanych z wykonywaną pracą; w przypadku konieczności użycia niesprawdzonych przenośnych nośników danych, należy zgłosić te nośniki, w celu sprawdzenia - przeskanowania programem antywirusowym, Administratorowi Bezpieczeństwa Informacji,

m) tworzenia kopii zapasowych niechronionych hasłem i/lub bez odpowiednich zabezpieczeń miejsca ich przechowywania.

2. Ponadto zabrania się:
   a) wyrzucania dokumentów zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia,
   b) pozostawiania dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach,
   c) pozostawiania kluczy w drzwiach, szafach, biurkach, zostawiania otwartych pomieszczeń, w których przetwarza się dane osobowe,
   d) pozostawiania bez nadzoru osób trzecich przebywających w pomieszczeniach szkoły, w których przetwarzane są dane osobowe,
   e) pozostawiania dokumentów na biurku po zakończonej pracy, pozostawiania otwartych dokumentów na ekranie monitora bez blokady konsoli,
   f) ignorowania nieznanych osób z zewnątrz poruszających się w obszarze przetwarzania danych osobowych,
   g) przekazywania informacji będącymi danymi osobowymi osobom nieupoważnionym,
   h) ignorowania zapisów Polityki Bezpieczeństwa szkoły.
3. Konieczne jest:
   a) posługiwanie się własnym loginem i hasłem w celu uzyskania dostępu do systemów informatycznych,
   b) tworzenia haseł trudnych do odgadnięcia dla innych,
   c) traktowanie konta pocztowego szkoły jako narzędzia pracy i wykorzystywanie go jedynie w celach służbowych,
   d) nie przerywanie procesu skanowania przez program antywirusowy na komputerze,
   e) wykonywanie kopii zapasowych danych przetwarzanych na stanowisku komputerowym,
   f) zabezpieczenie sprzętu komputerowego przed kradzieżą lub nieuprawnionym dostępem do danych.
4. Wszelkie przypadki naruszenia niniejszej Instrukcji należy zgłaszać Administratorowi Bezpieczeństwa Informacji lub bezpośredniemu przełożonemu.

5. **Dane kontaktowe**

- Administrator Danych Osobowych – Marta Bies – dyrektor szkoły, nr telefonu : 602 491 724, e-mail : wzs@zator.pl

- Administrator Bezpieczeństwa Informacji – Karol Matyjasik, nr telefonu : 668198973 , e-mail : wzs@zator.pl

- Pełnomocnik dyrektora ds. konserwacji i zabezpieczeń szkolnej sieci komputerowej – ,: …….. e-mail : ……

§ 23.

Zalecenia w zakresie przetwarzania danych osobowych sposobem tradycyjnym

1. Miejscem tworzenia, uzupełniania, przechowywania dokumentacji dotyczącej przetwarzania danych osobowych sposobem tradycyjnym są pomieszczenia w szkole: sekretariat, administracja, pokój nauczycielski, gabinet dyrektora, gabinet wicedyrektora, gabinet pedagoga, biblioteka, świetlica, sale lekcyjne.
2. Osoby prowadzące dokumentację zobowiązane są do zachowania tajemnicy służbowej.
3. Dokumentacji, o której mowa w punkcie 1 nie można wynosić poza teren szkoły.
4. Dokumentację, o której mowa w punkcie 1 archiwizuje się zgodnie z Instrukcją kancelaryjną.
5. Osoby prowadzące dokumentację zobowiązane są do niezwłocznego poinformowania Administratora Bezpieczeństwa Informacji o podejrzeniu dostępu do dokumentacji przez osoby nieupoważnione.