Regulamin

OCHRONY DANYCH OSOBOWYCH

POWIAT
KIELECKI

POWIATOWY ZESPÓŁ SZKÓŁ W BODZENTYNIE

BODZENTYN, 2018.

SPIS TREŚCI

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO dla:

- Pracowników, stażystów i praktykantów,
- Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora (tzw. podmioty przetwarzające),
- Użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora.

Każda z w/w osób powinna zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych.

1 ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, PROGRAMÓW

W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT zobowiązany jest do jego zabezpieczenia przed zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony

Użytkownik jest zobowiązany

- zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT,
- do uniemożliwienia osobom niepowołanym (np. klientom) wgląd do danych wyświetlanych na monitorach komputerowych – **tzw. Polityka czystego ekranu,**
- do usuwania plików z nośników/dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów).

Samowolne

instalowanie otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.

Przed czasowym opuszczeniem stanowiska pracy
użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (**WINDOWS + L**) lub wylogować się z systemu bądź z programu.

Po zakończeniu pracy, użytkownik zobowiązany jest:

- wylogować się z systemu informatycznego, a jeśli to wymagane - następnie wyłączyć sprzęt komputerowy,
- zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne na których znajdują się dane osobowe.

Niszczenie nośników

sprzętowych odbywa się wyłącznie za pośrednictwem Dyrektora Zespołu Szkół.

Użytkownicy komputerów przenośnych

na których znajdują się dane osobowe lub z dostępem do danych osobowych przez Internet zobowiązani są do stosowania zasad bezpieczeństwa zawartych w niniejszym regulaminie nawet poza siedzibą Zespołu Szkół.

2 ZARZĄDZANIE UPRAWNIENIAMI - PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

Każdy użytkownik zasobów IT

za które uważa się np. komputery stacjonarne, laptopy, dyski sieciowe, programy, w których użytkownik pracuje czy też pocztę elektroniczną, musi posiadać swój własny indywidualny identyfikator (login) do logowania się.

Tworzenie kont użytkowników
wraz z uprawnieniami do zasobów IT odbywa się na wniosek przełożonych a wykonywane jest przez ASI.

Każdy użytkownik musi
posiadać indywidualny identyfikator.

Użytkownik nie może
samodzielnie zmieniać swoich uprawnień (np. zostać administratorem Windows na swoim komputerze).

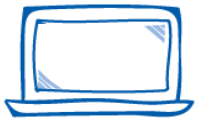
Zabronione jest umożliwianie innym osobom (jeżeli nie są uprawnione) pracy na swoim koncie użytkownika.

Zabrania się pracy wielu użytkowników na wspólnym koncie.

Użytkownik zasobów IT
rozpoczyna pracę z użyciem identyfikatora i hasła.

Użytkownik jest zobowiązany

- do powiadomienia ASI o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje bądź w inny sposób stwierdzą ten fakt.
- do uniemożliwienia osobom niepowołanym (np. uczniom, klientom) wglądu do danych wyświetlanych na monitorach – tzw. **Polityka czystego ekranu**



W przypadku zablokowania systemu

podczas próby zalogowania się bądź w trakcie pracy, zobowiązany jest powiadomić o tym ASI.

Przed czasowym opuszczeniem stanowiska pracy

użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu. Jeżeli tego nie uczyni, po upływie 10 minut system automatycznie aktywuje wygaszacz.

Zabrania się

uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana jako Administrator Danych lub ASI. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.

Po zakończeniu pracy, użytkownik zobowiązany jest:

- wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
- zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

3 POLITYKA HASEŁ

Hasła powinny:

- składać się z 8 znaków,
- zawierać duże litery + małe litery + cyfry (lub znaki specjalne).

Hasła nie powinny:

- być łatwe do odgadnięcia,
- być powszechnie używanymi słowami,
- być ujawnianie innym osobom.

W szczególności nie należy

jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty. Nie powinno się też stosować haseł, w których któryś z członów stanowi imię, nazwę lub numer miesiąca lub inny możliwy do odgadnięcia klucz.

Nie wolno:

- zapisywać haseł na kartkach i w notesach,
- naklejać haseł na monitorze komputera,
- zapisywać pod klawiaturą lub w szufladzie lub na "myszy",
- definiować haseł, w których jeden człon pozostaje niezmienny, a drugi zmienia się według przewidywalnego wzorca (np. Anna001, Anna002, Anna003 itd.),
- używać w serwisach internetowych takich samych lub podobnych haseł jak w systemie komputerowym Zespołu Szkół,
- stosować tego samego hasła jako zabezpieczenia w dostępie do różnych systemów.

W przypadku ujawnienia hasła – należy natychmiast go zmienić!

Hasła muszą być zmieniane co 30 dni

Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło w dowolnym momencie. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.

Użytkownik zobowiązuje się

do zachowania hasła w poufności, nawet po upływie jego ważności.

4 ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

Upoważnieni pracownicy są zobowiązani:

- do stosowania tzw. „**Polityki czystego biurka**”. Polega ona na zabezpieczaniu (zamykaniu) dokumentów oraz nośników np. w szafach, biurkach, pomieszczeniach w celu zabezpieczenia przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy,
- do niszczenia dokumentów i wydruków w niszczarkach.

Zabrania się:

- **pozostawiania dokumentów** z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych,

- **wyrzucania niezniszczonych dokumentów** na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych miejskich lub w lesie.

5 ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI POZA SIEDZIBĘ

Użytkownicy nie mogą
wynosić na zewnątrz Zespołu Szkół wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Pracodawcy. Do takich nośników zalicza się: wymienne twarde dyski, pendrive, płyty CD, DVD, pamięci typu Flash.

Dane osobowe wynoszone poza siedzibę
muszą być zaszyfrowane (szyfrowane dyski lub zahasłowane pliki).

Należy zapewnić

ochronę przed zalaniem lub innym uszkodzeniem dokumentacji papierowej poprzez przewożenie w odpowiednich teczkach.

W przypadku, gdy dokumenty przewozi pracownik
zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą

W sytuacji przekazywania nośników z danymi osobowymi
poza obszar organizacji można stosować następujące zasady bezpieczeństwa:

- adresat powinien zostać powiadomiony o przesyłce
- dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą

- stosować bezpieczne koperty depozytowe
- przesyłkę należy przesyłać przez kuriera lub sprawdzonego usługodawcę pocztowego

Użytkownik zobowiązany jest
do korzystania z sieci „Internet" wyłącznie w celach służbowych

Zabrania się

- **zgrywania na dysk twardy komputera** oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT (np. ASI) i tylko w uzasadnionych przypadkach,
- **wchodzenia na strony,** na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem),
- **samowolnego podłączania do komputerów** modemów, telefonów komórkowych i innych urządzeń dostępowych (np.: typu BlueConnect, iPlus, OrangeGo). Zabronione jest też łączenie się przy pomocy takich urządzeń z Internetem w chwili, gdy komputer użytkownika podłączony jest do sieci firmowej.

Użytkownik ponosi odpowiedzialność
za szkody spowodowane przez oprogramowanie instalowane z Internetu.

Nie należy w opcjach przeglądarki internetowej

włączać opcji autouzupełniania formularzy i zapamiętywania haseł.

W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę
należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.

Należy zachować szczególną ostrożność

w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty

mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

7 ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

Przesyłanie danych osobowych
z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione.

W przypadku przesyłania danych osobowych poza organizację

należy wysyłać pliki zaszyfrowane/spakowane (np. programem 7 zip,) i zahasłowane, gdzie hasło powinno być przesłane do odbiorcy telefonicznie lub SMS.

W przypadku zabezpieczenia plików hasłem
obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem na inny adres lub inną metodą, np. telefonicznie lub SMS.

Użytkownicy powinni zwracać szczególną uwagę
na poprawność adresu email zarówno nadawcy przy odbieraniu poczty, jak również odbiorcy dokumentu w przypadku wysyłki.

Zaleca się, aby użytkownik
podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

WAŻNE: Nie otwierać załączników (.zip, .xlsm, .exe) w mailach!!!!! Są to zwykle „wirusy", które infekują komputer oraz często pozostałe komputery w sieci. WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH

WAŻNE: Nie wolno „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron z „wirusami". Użytkownik „klikając" na taki hiperlink infekuje komputer oraz inne komputery w sieci. WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH

Należy zgłaszać ASI wszelkie przypadki podejrzanych e-maili.

Użytkownicy nie powinni

rozsyłać „niezawodowych” e-maili w formie „łańcuszków szczęścia", np. Życzenia Świąteczne adresowane do dziesiątek osób.

Podczas wysyłania maili do wielu adresatów jednocześnie
należy użyć metody **„Ukryte do wiadomości – UDW”**. Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości”!

Użytkownicy powinni okresowo kasować niepotrzebne maile.

Konta pocztowe służbowe
są odseparowane od poczty prywatnej. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.

Zakazuje się:

- wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób,
- korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania,
- wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej bez wyraźnej zgody Pracodawcy.

Użytkownicy mają prawo
korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.

Korzystanie z maila dla celów prywatnych
nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.

Zabrania się użytkownikom poczty elektronicznej

konfigurowania swoich kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny.

Przy korzystaniu z maila

Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.

8 OCHRONA ANTYWIRUSOWA

Użytkownicy zobowiązani są

do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada.

Zakazane jest wyłączanie systemu antywirusowego

podczas pracy systemu informatycznego przetwarzającego dane osobowe.

W przypadku stwierdzenia zainfekowania systemu

lub pojawienia się komunikatów „np.; Twój system jest zainfekowany! Zainstaluj program antywirusowy”, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie ASI lub Administratora Danych.

9 SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Każda osoba upoważniona

do przetwarzania danych osobowych zobowiązana jest do powiadomienia Pracodawcy w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.

Do sytuacji wymagających powiadomienia, należą:

- **niewłaściwe zabezpieczenie fizyczne pomieszczeń,** urządzeń i dokumentów,
- **niewłaściwe zabezpieczenie sprzętu IT**, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
- **nieprzestrzeganie zasad ochrony danych osobowych** przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

Do incydentów wymagających powiadomienia, należą:

- **zdarzenia losowe zewnętrzne** (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),

- **zdarzenia losowe wewnętrzne** (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),

- **umyślne incydenty** (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

Typowe przykłady incydentów wymagające reakcji:

- ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
- dokumentacja jest niszczona bez użycia niszczarki,
- fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
- otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
- ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe,
- wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz Zespołu Szkół bez upoważnienia Pracodawcy,
- udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
- telefoniczne próby wyłudzenia danych osobowych,

- kradzież, zagubienie komputerów lub CD, twardych dysków, pendrive z danymi osobowymi,
- maile zachęcające do ujawnienia identyfikatora i/lub hasła,
- pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
- hasła do systemów przyklejone są w pobliżu komputera.

10 OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:

- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym przez Pracodawcę,
- zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem zadań powierzonych przez Pracodawcę,
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Pracodawcę,
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
- ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

Jeśli jest to przewidziane
osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych.

Osoby zapoznane z treścią niniejszego Regulaminu

i przeszkolone zobowiązane są podpisać Zobowiązania do zachowania tajemnicy informacji.

Zabrania się:

- **przekazywania bezpośrednio lub przez telefon** danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego,

- **przekazywania lub ujawniania danych osobom lub instytucjom**, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych,
- **ujawniania na grupach dyskusyjnych, forach internetowych, blogach itp.** jakichkolwiek szczegółów dotyczących funkcjonowania Zespołu Szkół, w tym informacji na temat sprzętu i oprogramowania, z jakiego korzysta Zespół Szkół, oraz informacji kontaktowych innych niż ogólnodostępne w materiałach zewnętrznych.

11 POSTĘPOWANIE DYSCYPLINARNE

Przypadki nieuzasadnionego zaniechania obowiązków

wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.

Postępowanie sprzeczne z powyższymi zobowiązaniami

może też być uznane przez Pracodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016r. - RODO.