REGULAMIN OCHRONY DANYCH OSOBOWYCH W ZESPOLE SZKÓŁ NR 1 IM. GEN. JERZEGO ZIĘTKA W KATOWICACH
ul. Staszica 2, 40-230 Katowice

Pieczęć firmowa:	Podpis Administratora Danych Osobowych:	Data:
ZESPÓŁ SZKÓŁ Nr 1 im. gen. Jerzego Ziętka 40-230 Katowice, ul. Staszica 2 tel./fax 32 255-20-84 REGON 000724270 NIP 954-11-87-836	WICEDYREKTOR Zespołu Szkół Nr 1 im. gen. Jerzego Ziętka w Katowicach mgr Hanna Marszałek	13 dn. 2018

WSTĘP

Realizując postanowienia ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 poz. 1182 i 1662) oraz wydane w oparciu o delegacje ustawą przepisy rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz. U. 2004 r. Nr 100 poz. 1024 z zm.) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informacyjne służące do przetwarzania danych osobowych wprowadza się zestaw reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony
i dystrybucji informacji wrażliwej pozwalający na zapewnienie ochrony danych osobowych.

Niniejszy regulamin stanowi wyciąg najistotniejszych zapisów zawartych w Polityce Bezpieczeństwa Ochrony Danych Osobowych oraz Instrukcji zarządzania systemami informatycznymi. Obowiązuje pracowników etatowych oraz współpracowników (użytkowników), mających upoważnienia do przetwarzania danych osobowych.

SPIS TREŚCI

1 Zasady bezpiecznego użytkowania sprzętu stacjonarnego IT 3
2 Zasady korzystania z oprogramowania 3
3 Zasady korzystania z internetu 3
4 Zasady korzystania z poczty elektronicznej 4
5 Ochrona antywirusowa 5
6 Nadawanie upoważnień i uprawnień do przetwarzania danych osobowych 5
7 Polityka haseł 5
8 Procedura rozpoczęcia, zawieszenia i zakończenia pracy 6
9 Postępowanie z elektronicznymi nośnikami zawierającymi dane osobowe 6
10 Postępowanie z danymi osobowymi w wersji papierowej 7
11 Zapewnienie poufności danych osobowych 7
12 Skrócona instrukcja postępowania w przypadku naruszenia ODO 7
13 Postępowanie dyscyplinarne 8

1.

Zasady bezpiecznego użytkowania sprzętu stacjonarnego IT

1. Sprzęt IT służący do przetwarzania zbioru danych osobowych składa się z komputerów stacjonarnych połączonych z serwerem .....
2. Użytkownik zobowiązany jest korzystać ze Sprzętu IT w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem.
3. Użytkownik zobowiązany jest do zabezpieczenia Sprzętu IT przed dostępem osób nieupoważnionych, a w szczególności zawartości ekranów monitorów.
4. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT.
5. Samowolne otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek nie zatwierdzonych urządzeń do systemu informatycznego jest zabronione.

2.

Zasady korzystania z oprogramowania

1. Użytkownik zobowiązuje się do korzystania wyłącznie z oprogramowania objętego prawami autorskimi.
2. Użytkownik nie ma prawa kopiować oprogramowania zainstalowanego na Sprzęcie IT przez Pracodawcę / Zleceniodawcę na swoje własne potrzeby ani na potrzeby osób trzecich.
3. Instalowanie jakiegokolwiek oprogramowania na Sprzęcie IT może być dokonane wyłącznie przez osobę upoważnioną.
4. Użytkownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez Pracodawcę / Zleceniodawcę.
Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych dyskietek, płyt CD, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe.
5. Użytkownicy nie mają prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez osobę upoważnioną.
6. W przypadku naruszenia któregokolwiek z powyższych postanowień Pracodawca / Zleceniodawca ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.

3.

Zasady korzystania z Internetu

1. Użytkownicy mają prawo korzystać z Internetu wyłącznie w celu wykonywania obowiązków służbowych.
2. Przy korzystaniu z Internetu, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i praw autorskich.
3. Korzystanie z Internetu dla celów służbowych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych, a także na wydajność systemu informatycznego Pracodawcy / Zleceniodawcy.
4. Użytkownicy nie mają prawa korzystać z Internetu w celu przeglądania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec obowiązujących zasad postępowania, a także grać w gry komputerowe w Internecie lub w systemie informatycznym Pracodawcy / Zleceniodawcy, ściągać z Internetu jakichkolwiek plików muzycznych lub wideo.
5. W zakresie dozwolonym przepisami prawa, Pracodawca / Zleceniodawca zastrzega sobie prawo kontrolowania sposobu korzystania przez Użytkownika z Internetu pod kątem wyżej opisanych zasad. Ponadto, w uzasadnionym zakresie, Pracodawca / Zleceniodawca zastrzega sobie prawo kontroli czasu spędzanego przez Użytkownika w Internecie. Pracodawca może również blokować dostęp do niektórych treści dostępnych przez Internet.

4.

Zasady korzystania z poczty elektronicznej

1. System Poczty Elektronicznej jest przeznaczony wyłącznie do wykonywania obowiązków służbowych
2. Przy korzystaniu z Systemu Poczty Elektronicznej, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego
3. Użytkownicy nie mają prawa korzystać z Systemu Poczty Elektronicznej dla celów prywatnych.
4. Korzystanie z Systemu Poczty Elektronicznej dla celów służbowych, nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych,
a także na wydajność Systemu Poczty Elektronicznej.
5. Użytkownik jest świadomy, że wszelkie wiadomości o charakterze prywatnym utworzone lub odebrane za pośrednictwem Systemu Poczty Elektronicznej przetwarzane są wyłącznie na jego własną odpowiedzialność. Użytkownik wyraża zgodę na prowadzenie kontroli tych wiadomości przez Pracodawcę / Zleceniodawcę. Pracodawca nie będzie w tej sytuacji odpowiadać za przypadkowe naruszenie dóbr osobistych Użytkownika w postaci naruszenia tajemnicy korespondencji.
6. Użytkownicy nie mają prawa korzystać z Internetu
w celu przeglądania lub rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

7. Użytkownik nie ma prawa wysyłać wiadomości zawierających informacje poufne dotyczące Pracodawcy i jego pracowników, pacjentów lub klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej
8. Zakazuje się uczestnictwa w tzw. „łańcuszkach szczęścia"
9. Użytkownicy nie powinni otwierać przesyłek od nieznanych sobie osób, których tytuł nie sugeruje związku z wypełnianymi przez nich obowiązkami służbowymi.
10. Użytkownicy nie powinni uruchamiać wykonywalnych załączników dołączonych do wiadomości przesyłanych pocztą elektroniczną.
11. W przypadku przesyłania plików danych osobowych do podmiotów zewnętrznych, Użytkownik zobowiązany jest do ich spakowania i opatrzenia hasłem (8 znaków: duże i małe litery i cyfry lub znaki specjalne). Hasło należy przesłać odrębnym mailem lub sms.

5.

Ochrona antywirusowa

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym,
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe,
3. W przypadku stwierdzenia zainfekowania systemu, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Właściciela lub osobę upoważnioną.

6.

Nadawanie upoważnień i uprawnień do przetwarzania danych osobowych

1. Za nadawanie upoważnień odpowiada ADO.
2. Każdy użytkownik systemu przed nadaniem upoważnienia musi:
a. zapoznać się z niniejszym regulaminem;
b. odbyć szkolenie z zasad ochrony danych osobowych;
c. podpisać oświadczenie o poufności.
3. ADO nadaje pisemne upoważnienia Pracownikom i Zleceniobiorcom.
4. Upoważnienie nadawane jest do zbiorów w wersji papierowej.
5. ADO odpowiada za aktualizację i anulowanie Upoważnień

7.
Polityka haseł

1 Hasło dostępu do zbioru danych składa się co najmniej z 8 znaków (dużych i małych liter oraz z cyfr lub znaków specjalnych).
2 Zmiana hasła do systemu następuje nie rzadziej, niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.
3 Zmianę hasła wymusza system lub użytkownik zobowiązany jest do manualnej zmiany hasła.
4 Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
5 Hasła są rejestrowane w taki sposób, że nie jest możliwe ich ujawnienie

6. Przekazywanie nośników z danymi osobowymi powinno być przeprowadzane z uwzględnieniem zasad bezpieczeństwa. Adresat powinien zostać powiadomiony o przesyłce, zaś nadawca powinien sporządzić kopię przesyłanych danych. Adresat powinien powiadomić nadawcę o otrzymaniu przesyłki. Jeżeli nadawca nie otrzymał potwierdzenia, zaś adresat twierdzi, że nie otrzymał przesyłki, użytkownik będący nadawcą powinien poinformować o zaistniałej sytuacji Administratora Danych Osobowych.

10.
Postępowanie z danymi osobowymi w wersji papierowej

1. Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe odpowiedzialne są osoby upoważnione (użytkownicy) oraz pracownicy właściwych jednostek organizacyjnych (filii).
2. Dokumenty i wydruki zawierające dane osobowe przechowuje się w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieupoważnionych.
3. Użytkownicy są zobowiązani do stosowania „polityki czystego biurka". Polega ona na zabezpieczaniu dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych.
4. Użytkownicy zobowiązani są do przewożenia dokumentów w sposób zapobiegający ich kradzieży, zagubieniu lub utracie.
5. Użytkownicy zobowiązani są do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.

11.
Zapewnienie poufności danych osobowych

1. Użytkownik zobowiązany jest do zachowania w tajemnicy danych osobowych, do których ma lub będzie miał/a dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych lub zadań zleconych przez Pracodawcę / Zleceniodawcę.
2. Użytkownik zobowiązany jest do niewykorzystywania danych osobowych w celach pozasłużbowych bądź niezgodnych ze zleceniem o ile nie są one jawne.
3. Użytkownik zobowiązany jest do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych o ile nie są one jawne.
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym.

12.
Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

1. Użytkownik zobowiązany jest do powiadomienia Administratora Danych Osobowych(Właściciela) w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych
2. Typowe sytuacje, gdy użytkownik powinien powiadomić ADO:
a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania;

b. dokumentacja jest niszczona z użyciem niszczarki;
c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
e. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe;
f. ustawienie monitorów pozwala na wgląd osób postronnych na dane osobowe;
g. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz firmy bez upoważnienia ADO;
h. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej;
i. telefoniczne próby wyłudzenia danych osobowych;
j. kradzież komputerów lub CD, twardych dysków, Pen-drive z danymi osobowymi;
k. maile zachęcające do ujawnienia identyfikatora i/lub hasła;
l. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
m. hasła do systemów przechowywane są w pobliżu komputera.

13.
Postępowanie dyscyplinarne

2. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
3. Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych (Dz. U. 2014 poz. 1182 i 1662) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

ZESPÓŁ SZKÓŁ Nr 1
im. gen. Jerzego Ziętka
40-230 Katowice, ul. Staszica 2
tel./fax 32 255-20-84
REGON 000724270 NIP 954-11-87-836

WICEDYREKTOR
Zespołu Szkół Nr 1
im. gen. Jerzego Ziętka w Katowicach
23.04.2018
mgr Hanna Marszałek