ZARZĄDZENIE Nr 8/2025

DYREKTORA CENTRUM KSZTAŁCENIA ZAWODOWEGO W TORUNIU

z dnia 14 Listopada **2025r.**

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Centrum Kształcenia Zawodowego w Toruniu

Na podstawie art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz.UE L119 z 4 maja 2016r.) zarządza się, co następuje:

§1. Wprowadzam Politykę Bezpieczeństwa Informacji w Centrum Kształcenia Zawodowego w Toruniu oraz Instrukcję zarzadzania systemem informatycznym służącym do przetwarzania danych osobowych w Centrum Kształcenia Zawodowego w Toruniu stanowiące odpowiednio załącznik nr 1 oraz załącznik nr 2 do niniejszego zarządzenia.

§2. Wzór oświadczenia pracowników o zapoznaniu się z ww. dokumentami zawarty jest w załączniku nr 2 do Polityki Bezpieczeństwa Centrum Kształcenia Zawodowego w Toruniu stanowiący załącznik nr 1 do niniejszego zarządzenia.

§3. Traci moc zarządzenie Dyrektora Centrum Kształcenia Praktycznego w Toruniu Nr 3/2018 z dnia 23 maja 2018r. w sprawie wprowadzenia „Polityki bezpieczeństwa Centrum Kształcenia Praktycznego w Toruniu" oraz „Instrukcji zarzadzania systemem informatycznym służącym do przetwarzania danych osobowych w Centrum Kształcenia Praktycznego w Toruniu".

§4. Zarządzenie wchodzi w życie z dniem podpisania, z mocą obowiązująca od dnia 01.01.2026r.

DYREKTOR

mgr inż. Tomasz Borowski

14.11.2025

Do Zarządzenia nr CKZ 8/2025
Dyrektora
Centrum Kształcenia Zawodowego w Toruniu
z dnia 14.11.2025 r.

Polityka bezpieczeństwa
Centrum Kształcenia Zawodowego w Toruniu

Podstawa prawna

§ 1.
Regulacje zawarte w dokumencie, dotyczące bezpieczeństwa informacji to zbiór wytycznych, które określają odpowiednie środki i najlepsze praktyki, których organizacja musi przestrzegać, aby chronić się przed cyberatakami i naruszeniami danych. Zostały opracowane na podstawie analizy kluczowych obszarów normy ISO/IEC 27001:2023-08.

Postanowienia ogólne

§ 2.

1. Ilekroć mowa w niniejszym dokumencie o Polityce, należy przez to rozumieć „Politykę bezpieczeństwa Centrum Kształcenia Zawodowego w Toruniu".
2. Ilekroć mowa w niniejszym dokumencie o Centrum lub CKZ należy przez to rozumieć Centrum Kształcenia Zawodowego w Toruniu.
3. Ilekroć mowa w niniejszym dokumencie o Dyrektorze należy przez to rozumieć Dyrektora Centrum Kształcenia Zawodowego w Toruniu
4. Ilekroć mowa w niniejszym dokumencie o rozporządzeniu, należy przez to rozumieć Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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).

§ 3.
Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Centrum jest Dyrektor.

§ 4.
Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Centrum. W celu zrealizowania tych obowiązków administrator danych wprowadza Politykę bezpieczeństwa jako dokument obowiązujący w Centrum.

§ 5.

1. Do Dyrektora Centrum należy zapewnienie odpowiednich pomieszczeń, stosownie zabezpieczonych i wyposażonych do przetwarzania i przechowywania danych osobowych, zaznajomienie pracowników z prawnymi oraz pracowniczymi konsekwencjami naruszenia bezpieczeństwa danych osobowych.
2. Pracownicy upoważnieni do przetwarzania danych osobowych w systemie informatycznym jak i ręcznym, zobowiązani są do zapoznania się i przestrzegania Polityki.
3. Osoba przetwarzająca dane osobowe składa oświadczenie o zapoznaniu się z przepisami i odpowiedzialności karnej za naruszenie ochrony danych osobowych oraz zachowaniu tajemnicy, którego wzór stanowi załącznik nr 1 do Polityki.
4. Fakt zapoznania się z Polityką pracownik potwierdza własnoręcznym podpisem na stosownym wykazie, którego wzór stanowi załącznik nr 2 do Polityki.
5. Pracownikom wolno przebywać na terenie Centrum tylko w godzinach ich pracy, a po godzinach pracy- po zawiadomieniu bezpośredniego przełożonego.
   Przebywanie na terenie Centrum w dni wolne od pracy wymaga zezwolenia Dyrektora.
6. Korzystanie z systemu informatycznego służącego do przetwarzania danych osobowych może odbywać się tylko w godzinach pracy Centrum, a po godzinach pracy - po uzyskaniu zgody dyrektora Centrum.

Wykaz zasobów przetwarzania danych osobowych

§ 6.

Dostęp do systemów informatycznych zasobów wymienionych w poniższej tabeli jest możliwy tylko po zalogowaniu się indywidualnym loginem i hasłem. Wykaz dostępów do poszczególnych zbiorów danych w budynku Centrum Kształcenia Zawodowego w Toruniu, zamieszczono w tabeli.

).	**Nazwa zbioru**	**Cel przetwarzania**	**Zasoby:** **1) Program** **2) Sprzęt, lokalizacje i personel**	**Podstawy przetwarzania**	**Okres przechowywania**	**DPI**
	Zbiór pracowników	Obsługa procesów związanych z zatrudnieniem, prowadzeniem dokumentacji ubezpieczeniowej i przyznawaniem świadczeń socjalnych.	1) Platforma oświatowa Miasta Torunia (Vulcan Sp. z o. o); 2) Komputer stacjonarny – p. 3 - sekretarka, Komputer stacjonarny – p. 2 - wicedyrektor, Laptop – p. 4 – dyrektor;	Kodeks Pracy; Art. 6 ust. 1 lit. a, c Art. 9 ust. 2 lit. b rozporządzenia Parlamentu Europejskiego nr 2016/679 z 27.04.2016 r. ; Art. 23 ust. 1 pkt. 1), 2) Art. 27 ust. 2 pkt.1), 6)	50 lat 10 lat (dotyczy dokumentów wytworzonych dla pracowników zatrudnionych począwszy od 1.01.2019 r.)	N
	Zbiór uczniów	Obsługa procesów związanych z prowadzeniem	1) Platforma E-dziennik (Vulcan Sp. z o. o); 2) Komputer	§ 8. pkt. 1-3 oraz 5; § 21. pkt. 1-3 rozporządzenia ministra edukacji	5 lat	Ni

		Laptop – p. 21- administrator dziennika;			
Zbiór kandydatów na pracowników	Obsługa procesów związanych z rekrutacją pracowników.	1) Wersje papierowe - kwestionariusze osobowe dla kandydatów do pracy, formularze kandydatów, CV; 2) p. 3 – pracownik kadrowy.	Ustawy-Kodeks Pracy, o pracownikach samorządowych, Karta Nauczyciela Art. 6 ust. 1 lit. a, c Art. 9 ust. 2 lit. b rozporządzenia Parlamentu Europejskiego nr 2016/679 z 27.04.2016 r. ; Art. 23 ust. 1 pkt. 1),2) Art. 27 ust. 2 pkt. 1),6)	Do zakończenia procesu rekrutacji lub 3 miesiące od nawiązania stosunku pracy z kandydatem z naboru	
Zbiór Zakładowego Funduszu Świadczeń Socjalnych i Funduszu Zdrowotnego dla Nauczycieli	Obsługa procesów związanych z przyznawaniem i rozliczaniem świadczeń socjalnych i mieszkaniowych	1) Wersje papierowe – wnioski o świadczenie, o pożyczkę na cele mieszkaniowe, dokumenty poręczeń; 2) p.3 – sekretarka, 3) komisja socjalna.	Karta Nauczyciela, ustawa o zakładowym funduszu świadczeń socjalnych	5 lat	Nie
Zbiór umów cywilnoprawnych	Obsługa procesów związanych z obsługą prac zleconych podmiotom zewnętrznym.	1) Wersje papierowe, z wykorzystaniem oprogramowania biurowego 2) Komputer stacjonarny - p.3 – pracownik kadrowy, Komputer stacjonarny - p. 5 - pracownik administracyjno-gospodarczy.	Kodeks Cywilny; Statut CKZ	10 lat	Nie
Zbiór uczestników kursów	Obsługa procesów związanych z organizacją kursów zawodowych.	1) Informatyczna Platforma Spawalnicza (Instytut Spawalnictwa w Gliwicach); 2) Komputer stacjonarny – p. 2 – wicedyrektor. Laptop – p. 5 – specjalista ds. administracyjno-gospodarczych	Rozporządzenie w sprawie kształcenia ustawicznego w formach pozaszkolnych; Statut CKZ	5 lat	Nie
Zbiór monitoringu	Obsługa systemu kontroli	1) System monitorowania		14 dni	Nie

		Parchiwizacja zapisu.			
Zbiór zdających egzaminy zewnętrzne.	Obsługa procesów związanych z wymianą dokumentów z Okręgową Komisją Egzaminacyjną (dokumentacja egzaminacyjna).	1) Platforma internetowa SIOEPKZ, Serwis OKE (OKE w Gdańsku); 2) Komputer stacjonarny – p. 2 – wicedyrektor; Laptop – p. 4 – dyrektor.	Ustawa o systemie oświaty (t.j. Dz.U.2025.881); Rozporządzenie MEiN z dnia 10.10.2023 r. (Dz.U.2023.2175)	5 lat	Nie
Zbiór danych zawartych w Systemie Informacji Oświatowej	Obsługa procesów związanych z obowiązkiem przekazania danych do SIO	1) Platforma internetowa SIO; 2) p. 3 – sekretarka; Laptop – p. 4 - dyrektor	Ustawa o systemie informacji oświatowej z 15.04.2011 r. (t.j. Dz.U.2024.152)	5 lat	Nie
Zbiór rejestru korespondencji	Obsługa procesów związanych z wymianą dokumentów z podmiotami zewnętrznymi	1) Wersja papierowa – książka korespondencji; 2) p. 3 – sekretarka.	Kodeks Postępowania Administracyjnego	5 lat	Nie

Zasady przetwarzania danych osobowych

§ 7.

1. Gromadzenie danych następuje przez pozyskiwanie ich:
   1) bezpośrednio od osób, których dotyczą;
   2) z systemów informatycznych, do których dostęp posiada uprawniony pracownik CKZ;
   3) a także z innych zasobów, wynikających z wymogów ustawowych.
2. Gromadzone dane osobowe są udostępnianie pracownikom w zakresie niezbędnym do ich pracy i wynikającym z przepisów prawa poprzez posiadane systemy informatyczne. Dane udostępniane są poprzez moduły do przetwarzania lub przeglądania danych, np. zewnętrzny plik wymiany lub przy wykorzystaniu specjalnych mechanizmów baz danych.
3. O wyborze systemu informatycznego do przetwarzania i przechowywania zbioru pracowników (poz. 1) decyduje organ prowadzący CKZ – Gmina Miasta Toruń.
4. O wyborze systemu informatycznego do przetwarzania i przechowywania zbioru uczniów (poz. 2) - decyduje dyrektor CKZ.
5. Systemy informatyczne do przetwarzania i przechowywania zbiorów uczestników kursów (poz. 6) oraz zdających egzaminy zewnętrzne (poz. 8) są dostarczone i administrowane przez podmiot zewnętrzny, z którym CKZ współpracuje w celu realizacji zadań.

Opis struktury zbiorów danych

pozwalają na uzupełnienie tych samych danych z innych posiadanych zasobów w ramach jednostki.

2. Dane osobowe gromadzone są również w tradycyjnej formie papierowej, w ograniczonym zakresie w postaci:
   1) teczek akt osobowych,
   2) dziennika korespondencji,
   3) umów cywilnoprawnych,
   4) kwestionariusza kandydata na pracownika,
   5) kwestionariusza pracownika,
   6) wniosków o świadczenie socjalne,
   7) wniosków o pożyczkę na cele mieszkaniowe,
   8) dokumentów poręczeń spłaty pożyczki (żyrantów),
   9) formularz zgłoszeniowy i kwestionariusz osobowy uczestnika kursu,.

Nadawanie upoważnień i powierzanie przetwarzania

§ 9.

1. Przetwarzanie danych osobowych odbywa się wyłącznie na podstawie pisemnego upoważnienia udzielonego przez dyrektora CKZ.
2. Upoważnienie zawiera:
   1) podstawę prawną,
   2) imię i nazwisko oraz stanowisko osoby upoważnionej,
   3) zakres przetwarzanych danych osobowych,
   4) termin trwania upoważnienia,
   5) obowiązki osoby upoważnionej.
3. Upoważniony składa pisemne oświadczenie o poufności.
4. Upoważnienie obowiązuje do momentu nadania nowego, jego odwołania lub wygaśnięcia.
5. Upoważnienia wydane na podstawie dotychczas obowiązujących przepisów zachowują moc do czasu wydania nowych upoważnień.
6. W CKZ prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
7. Powierzenie przetwarzania danych osobowych podmiotom zewnętrznym odbywa się na podstawie pisemnej umowy.
8. Umowa ta zawiera:
   1) Przedmiot i czas trwania przetwarzania,
   2) Charakter i cel przetwarzania,
   3) Rodzaj danych osobowych,
   4) Kategorie osób, których dane dotyczą,
   5) Obowiązki i prawa administratora
9. Podmiot przetwarzający daje administratorowi gwarancję o zapewnieniu środków bezpieczeństwa danych, wymaganych przepisami prawa.
10. CKZ uznaje jako gwarancje wystarczające przedstawienie zatwierdzonego kodeksu postępowania lub certyfikacji podmiotu przetwarzającego.
11. Podmiot przetwarzający informuje pisemnie administratora danych o wszelkich zmianach w zakresie przetwarzania.

Zabezpieczenia

1) głównym – chronionym zamkiem drzwiowym i alarmem;
2) bocznym- chronionym zamkiem drzwiowym i alarmem.

2. Poszczególne pokoje, w których odbywa się przetwarzanie danych i ich składowanie są wyposażone w niezależne zamki i są zamykane podczas nieobecności pracownika.
3. Stanowiska komputerowe w pomieszczeniach, gdzie mogą przebywać osoby nieupoważnione do przetwarzania danych osobowych (np. interesanci, uczniowie albo inni pracownicy Centrum) są umieszczone w sposób, który uniemożliwia takim osobom wgląd do tych danych. W pokoju, do którego dostęp mają petenci monitory komputerowe ustawione są w ten sposób, by petenci nie widzieli zapisów na ekranie.
4. W przypadku dłuższej bezczynności uruchamiane są tzw. wygaszacze ekranu lub blokowanie systemu, których dezaktywacja jest możliwa po podaniu prawidłowego hasła użytkownika.
5. Wydruki zawierające dane osobowe znajdują się w miejscu, które uniemożliwia dostęp osobom postronnym.
6. Kopie bezpieczeństwa (kopie zapasowe) wykonują okresowo pracownicy w ramach swoich obowiązków. Kopie bezpieczeństwa pracownik przechowuje w swoim pokoju służbowym w szafce zabezpieczonej zamkiem. Dostęp do nośników zawierających kopie danych mają tylko uprawnione osoby.
7. Wydruk z ważnym hasłem jest przechowywany tak, aby uniemożliwić dostęp do niego osobom postronnym (innym niż sam użytkownik , przełożeni i administrator).

Obowiązki Administratora danych

§ 11.

1. Do obowiązków Administratora danych należy w szczególności:
   1) zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym;
   2) zapobieganie zabraniu danych przez osobę nieuprawnioną;
   3) zapobieganie przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych;
   4) zbieranie danych dla oznaczonych, zgodnych z prawem celów;
   5) dbałość o merytoryczną poprawność danych i adekwatność w stosunku do celów w jakich są przetwarzane;
   6) określenie pomieszczeń lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego;
   7) prowadzenie ewidencji osób uprawnionych do przetwarzania danych osobowych.

2. Administrator danych odpowiada za to by zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych określał odpowiedzialność tej osoby za:
   1) ochronę danych przed niepowołanym dostępem;
   2) nieuzasadnioną modyfikację lub zniszczenie danych;
   3) nielegalne ujawnienie danych w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.

3. Zgłasza naruszenia danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych.

§ 12.

1. Obowiązki Inspektora ochrony danych osobowych pełni osoba zatrudniona przez organ prowadzący – Gminę Miasta Torunia i wyznaczona przez administratora danych – dyrektora CKZ.

2. Do obowiązków Inspektora ochrony danych należy w szczególności:
   1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia i doradzanie im w tej sprawie;
   2) monitorowanie przestrzegania rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art.35 rozporządzenia;
   4) współpraca z organem nadzorczym;
   5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art.36 rozporządzenia, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
   6) pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy powyższego rozporządzenia;
   7) prowadzenie rejestru czynności lub rejestru kategorii czynności;
   8) wsparcie przy prowadzeniu niezbędnych analiz ryzyka dla poszczególnych systemów czy zbiorów danych osobowych;
   9) monitorowanie skuteczności zastosowanych u Administratora środków ochrony danych osobowych;
   10) monitorowanie prowadzenia ewidencji udzielonych przez Administratora upoważnień do przetwarzania danych osobowych i przechowywania upoważnień.

Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 13.

1. Każdy pracownik Centrum, który powezmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany fakt ten niezwłocznie zgłosić Administratorowi danych osobowych lub Inspektorowi ochrony danych osobowych.

2. W przypadku wykrycia naruszenia ochrony danych osobowych Dyrektor Centrum niezwłocznie zawiadamia Inspektora ochrony danych osobowych o zaistniałym zdarzeniu oraz przeprowadza wstępne dochodzenie, po czym sporządza raport opisujący okoliczności zdarzenia. Jeśli zdarzenie ma charakter przestępstwa sprawa kierowana jest

§ 14.

1. Osoba, której dane osobowe są przetwarzane w CKZ ma prawo do:
   1) uzyskania dostępu do wszystkich treści;
   2) sprostowania;
   3) usunięcia;
   4) ograniczenia przetwarzania;
   5) przenoszenia;
   6) sprzeciwu;

   danych osobowych zgromadzonych w CKZ.
2. W celu uzyskania jednego z powyższych działań należy złożyć pisemny wniosek, zawierający opis czynności, które administrator ma wykonać.
3. Administrator danych osobowych dokonuje niezwłocznie zmian wskazanych we wniosku, o ile jest do tego upoważniony i nie jest to sprzeczne z przepisami prawa.
4. Administrator danych osobowych informuje pisemnie wnioskującego o przyjętych rozwiązaniach.

Polityka kluczy

§ 15.

1. Klucze do wszystkich pomieszczeń w CKZ znajdują się w zamykanej na klucz gablocie, znajdującej się w zamykanym pomieszczeniu.
2. Klucze do pomieszczeń, w których odbywa się przetwarzanie danych osobowych są umieszczane w oddzielnej gablocie, zamykanej na klucz, w pomieszczeniu również zamykanym na klucz.
3. Po zakończonym dniu pracy dostęp do tych pomieszczeń ma tylko wyznaczona osoba, która wykonuje czynności sprzątające, bez możliwości dostępu do jakichkolwiek danych osobowych.

do Polityki bezpieczeństwa
Centrum Kształcenia Zawodowego w Toruniu

.....
(pieczęć nagłówkowa)

Toruń, dnia .....

Upoważnienie nr: .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art.29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE ((dalej RODO),

upoważniam

Pana/Panią

Zatrudnionego/ą na stanowisku: .....

w zakresie pełnionych obowiązków służbowych względem Administratora do przetwarzania danych osobowych .

I. Zakres upoważnienia obejmuje dane przetwarzanie na nośnikach.....
(wpisać odpowiednie)

.....

Procesy	**Nazwa czynności przetwarzania danych osobowych**

II. Okres upoważnienia:

- ..... .

III. Upoważniony/a zobowiązany/a jest do zachowania poufności danych.

IV. Upoważnienie traci ważność z chwilą jego pisemnego cofnięcia. Wygaśnięcie upoważnienia nie zwalnia z zachowania przez upoważnionego poufności informacji oraz sposobów ich zabezpieczenia.

.....

do Polityki bezpieczeństwa
Centrum Kształcenia Zawodowego w Toruniu

Wykaz osób zatrudnionych przy przetwarzaniu danych osobowych, które zostały zapoznane z „Polityką bezpieczeństwa Centrum Kształcenia Zawodowego w Toruniu" oraz „Instrukcją zarządzania systemem informatycznym w Centrum Kształcenia Zawodowego w Toruniu".

L.p.	Nazwisko i Imię	Stanowisko	Data	Podpis

Do Zarządzenia nr CKZ 8/2025
Dyrektora
Centrum Kształcenia Zawodowego w Toruniu
z dnia 14.11.2025 r.

Instrukcja
zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Centrum Kształcenia Zawodowego w Toruniu

Podstawa prawna

§ 1.

1. Instrukcja zarządzania systemem informatycznym określa podstawowe zasady, których realizacja ma na celu ochronę systemu informatycznego Centrum Kształcenia Zawodowego w Toruniu, przetwarzanych w nim danych oraz określenie obowiązków pracowników Centrum korzystających z tych zasobów. Jako system informatyczny CKZ należy rozumieć sumę wszystkich elementów składających się na informatyczne środowisko pracy;
2. Zasady zawarte w tym dokumencie dotyczą również urządzeń przenośnych, które są wykorzystywane do przetwarzania danych osobowych.

Postanowienia ogólne

§ 2.

1. Ilekroć mowa w niniejszym dokumencie o Instrukcji, należy przez to rozumieć „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Centrum Kształcenia Zawodowego w Toruniu".
2. Ilekroć mowa w niniejszym dokumencie o Centrum należy przez to rozumieć Centrum Kształcenia Zawodowego w Toruniu.

Zagadnienia organizacyjne

§ 3.

1. Pracownicy upoważnieni do przetwarzania danych osobowych w systemie informatycznym jak i ręcznym, zobowiązani są do zapoznania się z treścią Instrukcji i jej przestrzegania.
2. Fakt zapoznania się z Instrukcją pracownik potwierdza własnoręcznym podpisem na stosownym wykazie, którego wzór stanowi załącznik nr 2 do „Polityki bezpieczeństwa w Centrum Kształcenia Zawodowego w Toruniu".

Procedury nadawania, zmieniania i zakończenia pracy w systemie

niezwłocznie powiadomić o tym fakcie Administratora.

2. Każdy pracownik zobowiązany jest do stosowania osobistego profilu użytkownika, wykorzystywanego w celu uruchomienia komputera stacjonarnego lub przenośnego.
3. W celu rozpoczęcia pracy w systemie informatycznym użytkownik wykonuje logowanie do systemu używając nadanego, indywidualnego loginu i hasła.
4. Podczas nieobecności przy stanowisku komputerowym należy wylogować się z systemu bądź uruchomić wygaszasz ekranu chroniony hasłem.
5. Po zakończeniu pracy w systemie należy wylogować się z systemu i wyłączyć stację roboczą.

Nadawanie uprawnień

§ 5.

1. Dane osobowe w systemach informatycznych może przetwarzać wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych, którego wzór stanowi załącznik nr 1 do „Polityki bezpieczeństwa w Centrum Kształcenia Zawodowego w Toruniu".
2. Administrator danych określa zakres danych, cel przetwarzania, czas dostępu oraz obowiązki wynikające z przetwarzania danych, do których dostęp uzyskuje upoważniony pracownik.
3. Upoważnienie do przetwarzania danych osobowych w systemie informatycznym nadaje Administrator danych.
4. Uprawnienia do logowania w zewnętrznym systemie informatycznym nadaje dostawca oprogramowania lub nadrzędny administrator systemu, na podstawie upoważnienia nadanego przez Administratora danych.
5. Zabrania się udostępniania loginu i hasła innym użytkownikom systemu informatycznego oraz osobom nieupoważnionym.
6. W celu zapewnienia ciągłości przetwarzania danych dostęp do danej kategorii danych posiada dwóch pracowników Centrum.

Zabezpieczenia

§ 6.

1. Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej stacji roboczych, na których przetwarzane są dane osobowe zapewniają zasilacze UPS.
2. Gwarancję ochrony danych osobowych na zewnętrznych platformach informatycznych zapewnia dostawca usług.
3. Stosuje się aktywną ochronę antywirusową na każdym komputerze, na którym przetwarzane są dane osobowe. Za dokonywanie skanowania systemu w poszukiwaniu złośliwego oprogramowania i aktualizację bazy wirusów odpowiada użytkownik stacji roboczej.
4. Przekazywanie wiadomości drogą mailową, zawierających dane osobowe odbywa się poprzez pliki zabezpieczone hasłem.
5. Wszyscy pracownicy posiadają imienne konta mailowe założone na służbowej domenie pocztowej.

Odpowiedzialnym za wykonanie kopii danych i kopii awaryjnych jest pracownik obsługujący program przetwarzający dane.
2. Kopie awaryjne są wykonywane raz na 6 miesięcy, natomiast kopie zapasowe po każdej zmianie treści, nie rzadziej niż raz na 6 miesięcy.
3. Kopie awaryjne są przechowywane w kasetce pancernej, natomiast kopie zapasowe w pokojach służbowych w szafkach zabezpieczonych zamkiem. Kopie awaryjne i zapasowe są przechowywane na dwóch różnych nośnikach pamięci.
4. Kopie awaryjne i zapasowe są zabezpieczone hasłem.
5. Usunięcie danych z nośników zewnętrznych, na których były zapisywane kopie bezpieczeństwa, dokonuje się poprzez trwałe wymazanie pamięci lub mechaniczne zniszczenie (np. formatowanie dysku typu flash).

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

§ 8.

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane wyłącznie przez pracowników Centrum lub przez upoważnionych przedstawicieli wykonawców.
2. Prace wymienione w ust.1 powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
3. Przed rozpoczęciem prac wymienionych w ust.1 przez osobę nie będącą pracownikiem Centrum należy dokonać potwierdzenia tożsamości tej osoby.
4. Nośniki magnetyczne przekazywane na zewnątrz są pozbawione zapisów zawierających dane osobowe. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
5. Uszkodzone nośniki magnetyczne przed ich utylizacją należy fizycznie zniszczyć (przeciąć, przełamać itp.)
6. Po wykorzystaniu wydruki papierowe zawierające dane osobowe są trwale utylizowane w niszczarce.