Załącznik Nr 1 do Zarządzenia nr 23/2019
Dyrektora ZSCH we Włocławku

POLITYKA BEZPIECZEŃSTWA W ZAKRESIE ZARZĄDZANIA PRZETWARZANIEM DANYCH OSOBOWYCH W ZESPOLE SZKÓŁ CHEMICZNYCH WE WŁOCŁAWKU

§ 1
Postanowienia ogólne

1. „Polityka bezpieczeństwa w zakresie zarządzania przetwarzaniem danych osobowych, służącym do przetwarzania danych osobowych w Zespole Szkół Chemicznych we Włocławku jest dokumentem zwanym dalej polityką bezpieczeństwa, który określa zasady i procedury przetwarzania danych osobowych ich zabezpieczenia przed nieuprawnionym ujawnieniem.
2. Niniejsza polityka bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, aktach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.
3. Polityka bezpieczeństwa w zakresie zarządzania przetwarzaniem danych osobowych, zawiera:
    1. Zasady przetwarzania danych osobowych,
    2. Opis pomieszczeń tworzących obszar, w którym są przetwarzane dane osobowe,
    3. Środki techniczne i organizacyjne, służące zapewnieniu poufności, integralności i rozliczalności przetwarzanych danych,
    4. Rejestr czynności przetwarzania danych,
    5. Procedura postępowania z incydentami,
    6. Zabezpieczenie sprzętu,
    7. Analiza ryzyka,
    8. Odpowiedzialność osób upoważnionych do przetwarzania danych,
    9. Monitorowanie dostępu do systemu i jego użycia
    10. Umowa powierzenia przetwarzania danych osobowych,
    11. Przegląd polityki bezpieczeństwa i audyt systemu,
    12. Postanowienia końcowe.
4. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zatrudnionych w Zespole Szkół Chemicznych we Włocławku.
   W skład obszaru przetwarzania danych osobowych w ZSCH wchodzi budynek przy ulicy Bulwary 4 we Włocławku.

§ 2
Określenia:

Określenia użyte w Polityce bezpieczeństwa oznaczają:

1. Administrator danych osobowych (ADO) – rozumie się przez to osobę, decydującą o celach i środkach przetwarzania danych. W Zespole Szkół Chemicznych we Włocławku funkcję administratora danych pełni Dyrektor.
2. Inspektor ochrony danych (IOD) – rozumie się przez to osobę, której Administrator danych powierzył pełnienie obowiązków Inspektora Ochrony Danych.
3. Informatyk – rozumie się przez to osobę nadzorującą pracę systemu informatycznego oraz wykonującą w nim czynności wymagane specjalnych uprawnień.
4. Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
5. Zbiór danych – zestaw danych osobowych posiadający określoną strukturę, prowadzony wg określonych kryteriów oraz celów.
6. Przetwarzanie danych – wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywania, udostępnianie, zmienianie, usuwanie.
7. Hasło – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

8. Identyfikator użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
9. Odbiorca danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą; osobę upoważnioną do przetwarzania danych; osobę, której powierzono przetwarzanie danych; organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
10. Osoba upoważniona do przetwarzania danych osobowych – rozumie się przez to pracownika ZSCH, która upoważniona została do przetwarzania danych osobowych przez Dyrektora na piśmie.
11. Poufność danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
12. Integralność – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
13. Rozliczalność – rozumie się przez to właściwość zapewniającą działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
14. Uwierzytelnianie – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
15. Raport – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych.
16. Sieć publiczna – rozumie się przez to sieć telekomunikacyjną, wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych.
17. System informatyczny – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
18. ZSCH – rozumie się przez to Zespół Szkół Chemicznych we Włocławku.
19. RODO – rozumie się przez to rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46WE (Dz. Urz. UE L 119, s. 1).
20. Użytkownik – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.
21. Ustawa o ochronie danych osobowych – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000).

§ 3

Zasady przetwarzania danych osobowych

Administrator danych przetwarza dane osobowe:

1. Zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność, przejrzystość"),
2. Zbiera je w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarza ich dalej w sposób niezgodny z tymi celami („ograniczenie celu"),
3. Adekwatnie, stosownie oraz w sposób ograniczony do tego, co niezbędne do celów, w których są przetwarzana („minimalizacja danych"),
4. Prawidłowo i w razie potrzeby uaktualnia zebrane dane („prawidłowość"),
5. Przechowuje je w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane („ograniczenie przechowywania"),
6. W sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzenie, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność"),

§ 4

Cel

W celu realizacji tych zasad Administrator danych przetwarza dane legalnie, na podstawie przesłanek opisanych w art. 6 RODO. Pobiera dane osobowe adekwatnie do celów przetwarzania i przetwarza je przez określony czas. Wobec osób, których dane przetwarza wypełnia obowiązki informacyjne określone w art. 13 RODO lub w art. 14 RODO (gdy informacje pobierane są w sposób inny niż od osoby, której dane dotyczą) oraz wskazuje posługujące im uprawnienia takie jak prawo do:

- dostępu do danych,
- sprostowania danych,
- usunięcia danych (prawo do bycia zapomnianym),
- przenoszenia
- sprzeciwu wobec przetwarzania,
- ograniczenia przetwarzania
- wniesienia skargi do organu nadzorczego
- sprzeciwu wobec bycia profilowanym.

§ 5

Administrator Danych Osobowych

1. Funkcję Administratora danych osobowych sprawuje Dyrektor Zespołu Szkół Chemicznych we Włocławku. Administrator danych osobowych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:
   - podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji Administratora danych oraz technik zabezpieczenia danych osobowych,
   - upoważnia (załącznik nr 1) poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków, oraz odwołuje te upoważnienia lub wyrejestrowuje użytkownika z systemu informatycznego,
   - wyznacza, inspektora danych osobowych oraz określa zakres jego zadań i czynności,
   - prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych oraz pozostałą dokumentację z zakresu ochrony danych, o ile do jej prowadzenia nie powierzy innej osobie,
   - zapewnia użytkownikom odpowiednie stanowiska i warunki pracy, umożliwiające bezpieczne przetwarzanie danych,
   - podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur,

§ 6

Powołanie Inspektora Ochrony Danych

Administrator Danych Osobowych jest zobowiązany powołać inspektora ochrony danych.
W przypadku powołania inspektora ochrony danych do jego zadań należą:

1. Informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów RODO oraz ustawy o ochronie danych osobowych,
2. Monitorowanie przestrzegania przepisów RODO oraz ustawy o ochronie danych osobowych oraz Polityki bezpieczeństwa obowiązującej w ZSCH, 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 osobowych oraz monitorowania jej wykonania zgodnie z art. 35 RODO,
4. Współpraca z organem nadzorczym, tj. Prezesem Urzędu Ochrony Danych Osobowych,
5. Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

W przypadku wyznaczenia inspektora ochrony danych należy zgłosić jego powołanie Prezesowi Urzędu Ochrony Danych w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko, adres poczty elektronicznej lub numer telefonu inspektora.

§ 7

Informatyk

Informatyk realizuje zadania w zakresie bieżącego nadzoru nad systemem informatycznym Administratora danych, w tym zwłaszcza:

1. Projektuje i wykonuje bazy danych i ich oprogramowanie aplikacyjne. Administruje bazami danych i systemami przetwarzania informacji, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji Administratora.
2. Obsługuje komputery, posługując się gotowymi pakietami oprogramowania użytkowego i narzędziowego.
3. Dobiera konfigurację sprzętu i oprogramowania komputerowego. Obsługuje lokalne sieci komputerowe i nadzoruje ich pracę.
4. Przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe.
5. Na wniosek Dyrektora ZSCH przydziela każdemu użytkownikowi hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych.
6. Usuwa uszkodzenia powstające w urządzeniach systemu komputerowego oraz testuje jakość ich pracy
7. Nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych.
8. Wyrejestrowuje użytkowników na polecenie Administratora danych.
9. Zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz w razie potrzeby, Administratorowi danych osobowych.
10. W sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje Administratora danych o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia.
11. Prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym.
12. Sprawuje nadzór nad wykonaniem kopii zapasowych na których zapisane są dane osobowe, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadki awarii systemu informatycznego.
13. Podejmuje działania, służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

§ 8

Osoba upoważniona do przetwarzania danych osobowych.

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

1. Może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez Administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych.
2. Musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u Administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji.
3. Zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej polityki bezpieczeństwa, służącymi do przetwarzania danych osobowych.
4. Stosuje określone przez Administratora danych procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne przetwarzanie danych.
5. Korzysta z systemu informatycznego Administratora danych w sposób zgodny ze wskazówkami zawartymi w instrukcji obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników.
6. Zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

§9

Opis pomieszczeń tworzących obszar, w którym są przetwarzane dane osobowe

1. Zespół Szkół Chemicznych we Włocławku mieści się w budynku przy ulicy Bulwary im. Józefa marsz. Piłsudskiego 4 we Włocławku.
2. Sekretariat i pokój Dyrektora znajduje się na parterze budynku szkoły. Każde z tych pomieszczeń przystosowane jest do pracy dla jednej osoby. W pokojach tych przetwarzane są dane osobowe ręcznie oraz poprzez system informatyczny. Dokumentację papierową oraz komputerowe nośniki informacji tj. pendrive, płyty CD przechowuje się w szafach zamykanych na klucze, które są w posiadaniu Dyrektora. W komputerze znajduje się program SIO – system informacji oświatowej. Program może uruchomić tylko pracownik upoważniony do jego otwarcia przy użyciu odpowiednich haseł.
3. Pokoje rachuby i płac znajdują się na II i III piętrze budynku Centrum. W pokojach tych przetwarzane są dane osobowe pracowników Centrum oraz pracowników jednostek obsługiwanych przez Centrum. Dokumentację papierową oraz komputerowe nośniki informacji tj. pendrive, płyty CD przechowuje się w szafach zamykanych na klucze, które są w posiadaniu danego pracownika Centrum odpowiedzialnego za te dokumenty.
4. Pokoje Zastępców Dyrektora znajdują się na parterze budynku szkoły. Jeden znajduje się w budynku A szkoły a drugi w budynku B szkoły. Pokoje są przystosowane do pracy dla jednej osoby. W pokojach tych przetwarzane są dane osobowe ręcznie oraz poprzez system informatyczny. Dokumentację papierową oraz komputerowe nośniki informacji tj. płyty CD i pendrive przechowuje się w szafach zamykanych na klucze, które są w posiadaniu Z–cy. Dyrektora. Komputer może uruchomić tylko pracownik upoważniony do jego otwarcia przy użyciu odpowiednich haseł.
5. Pokój Głównego Księgowego znajduje się na drugim piętrze p. 214 budynku Centrum i jest przystosowany do pracy dla jednej osoby. W pokoju tym przetwarzane są dane osobowe ręcznie oraz poprzez system informatyczny. Dokumentację papierową oraz komputerowe nośniki informacji tj. płyty CD i pendrive przechowuje się w szafach zamykanych na klucze, które są w posiadaniu głównego księgowego. Komputer może uruchomić tylko pracownik upoważniony do jego otwarcia przy użyciu odpowiednich haseł.
6. Pieczęcie z nazwą i siedzibą ZSCH oraz imienne są przechowywane w szafkach zamykanych na klucz, które otwierają i zamykają użytkownicy tych pieczątek zgodnie z ich rejestrem.
7. Przesyłki zawierające dane osobowe przesyła się jako polecone z ewentualnym zwrotnym potwierdzeniem odbioru oraz zabezpieczone w sposób uniemożliwiający zapoznanie się z ich treścią przez osoby nieupoważnione.
8. Dokumenty zawierające dane osobowe przekazuje się do archiwum mieszczącego się w ZSCH, po okresie przydatności dokumenty zawierające dane osobowe niszczy się na podstawie decyzji Dyrektora komisyjnie, w warunkach gwarantujących zabezpieczenie danych osobowych w sposób gwarantujący uniemożliwienie ich odtworzenia, wykazy i spisy zdawczo - odbiorcze dokumentów zawierające dane osobowe przekazywanych do archiwum oraz protokoły zniszczenia dokumentów przechowuje Administrator danych. Dostęp do archiwum posiada Sekretariat oraz Dyrektor ZSCH.
9. Dokumenty zawierające dane osobowe niezbędne do pracy w terenie należy przechowywać w warunkach gwarantujących ich należytą ochronę.

§10

Wykaz programów stosowanych w ZSCH :

- Windows,
- Office,
- SIO- System Informacji Oświatowej,
- Płatnik- program obsługujący przekazywanie danych do ZUS,
- Płace – Optivum,
- PFRON,
- iPKO Biznes,
- GUS,

- JPK (zbiory informacji o operacjach gospodarczych sporządzane w specjalnym schemacie XML określonym przez Ministerstwo Finansów),
- VULCAN- księgowość
-

§ 11

Środki techniczne i organizacyjne, służące zapewnieniu poufności, integralności i rozliczalności przetwarzanych danych

Bezpieczeństwo osobowe.

1. Dyrektor ZSCH przeprowadza nabór na wolne stanowiska w drodze konkursu. Kandydaci na pracowników są dobierani z uwzględnieniem ich kompetencji merytorycznych, a także odpowiedniego wykształcenia. Zwraca się uwagę na takie cechy kandydata, jak uczciwość, odpowiedzialność, przewidywalność zachowania.
2. Dostęp do danych wprowadzonych przez użytkowników systemów informatycznych mają jedynie Administrator danych osobowych, oraz upoważnieni pracownicy zapewniając jego prawidłową eksploatację.

Zasady zabezpieczania danych:

- zbiory kartotekowe winny znajdować się w zamkniętych pomieszczeniach zabezpieczonych przed dostępem osób nieupoważnionych
- zbiory w systemach informatycznych winny być zabezpieczone hasłem dostępu znanym użytkownikowi zbioru,
- ochronie podlegają dane osobowe gromadzone i przetwarzane w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych oraz w urządzeniach i systemie informatycznym,
- pomieszczenia, w których przetwarza się dane osobowe powinny być fizycznie zabezpieczone przed dostępem osób nieuprawnionych, to znaczy posiadać odpowiednie zamki do drzwi, zabezpieczenia w oknach (w szczególności na parterze) oraz być wyposażone w środki ochrony ppoż. (gaśnice);
- dokumenty i nośniki informacji, zawierające dane osobowe powinny być zabezpieczone przed dostępem osób nieupoważnionych do przetwarzania danych. Jeśli nie są aktualnie używane powinny być przechowywane w szafach lub w innych przeznaczonych do tego celu urządzeniach biurowych, posiadających odpowiednie zabezpieczenia

Zachowanie poufności.

1. Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych (np. osoby sprzątające pomieszczenia ZSCH), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy.
2. Ryzyko ze strony osób, które dokonują bieżących napraw komputera, minimalizowane jest obecnością użytkownika systemu.

§12

Analiza Ryzyka

Administrator danych prowadzi analizę ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń. Analiza prowadzona jest dla zbioru danych. W przypadku konieczności przeprowadza się ocenę skutków dla oceny ryzyka na mocy art.35 RODO

§13

Wykaz zabezpieczeń

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

§14
Rejestr czynności przetwarzania

Administrator danych prowadzi rejestr czynności przetwarzania. W rejestrze tym zamieszcza się:

- imię i nazwisko oraz dane kontaktowe Administratora,
- cele przetwarzania,
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
- kategorie odbiorców, których dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych,
- gdy ma to zastosowanie, informacje na temat przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwę tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust 1akapit drugi RODO, dokumentację odpowiednich zabezpieczeń,
- jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
- jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust 1 RODO.

§15
Szkolenia w zakresie ochrony danych osobowych.

1. Administrator danych osobowych uwzględnia następujący plan szkoleń:
   - szkoli się każdą osobę, która ma zostać upoważniona do przetwarzania danych osobowych,
   - szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w przypadku każdej zmiany zasad lub procedur ochrony danych osobowych,
   - przeprowadza się szkolenia dla osób innych niż upoważnione do przetwarzania danych, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem danych osobowych.
2. Tematyka szkoleń obejmuje:
   - przepisy i procedury, dotyczące ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i zapisów na nośnikach,
   - sposoby ochrony danych przed osobami postronnymi i procedury udostępniania danych osobom, których one dotyczą,
   - obowiązki osób upoważnionych do przetwarzania danych osobowych i innych,
   - odpowiedzialność za naruszenie obowiązków z zakresu ochrony danych osobowych,
   - zasady i procedury określone w polityce bezpieczeństwa.

§16
Strefy bezpieczeństwa.

1. W ZSCH wydzielono dwie strefy bezpieczeństwa.
   - Do strefy I wchodzą: gabinet Dyrektora p. 201, Z- ca Dyrektora p. 307 oraz gabinet Głównego Księgowego p. 214, Zastępcy Głównego księgowego, w którym może przebywać: Dyrektor, Z- ca Dyrektora, Główny Księgowy, Z-ca Głównego Księgowego inspektorzy, specjaliści i inni użytkownicy danych, tylko w towarzystwie Dyrektora, Z- cy Dyrektora, Głównego Księgowego, Z-cy Głównego Księgowego, natomiast osoby postronne nie mają dostępu.
   - W strefie II do danych osobowych mają dostęp wszystkie osoby upoważnione do ich przetwarzania, a osoby postronne tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych. Strefa ta obejmuje pokoje pracowników Centrum w tym sekretariat i kasę.

§17
Procedura postępowania z incydentami

Administrator danych wprowadza do stosowania procedurę postępowania z incydentami naruszenia ochrony danych osobowych. Celem tej procedury jest wypełnienie obowiązku wynikającego z art. 33 RODO. Procedura określa sposób definiowania incydentów zagrażających bezpieczeństwu danych osobowych oraz sposób reagowania na nie, a także procedurę wprowadzenia działań naprawczych. Każda osoba upoważniona do przetwarzania danych osobowych ma obowiązek poinformowania o możliwości wystąpienia incydentu lub o jego wystąpieniu. Taka informacja powinna być przekazana Dyrektorowi ZSCH oraz inspektorowi ochrony danych.
Powiadomienia wymagają:

- niewłaściwe zabezpieczenie sprzętu elektronicznego, oprogramowania przed wyciekiem, kradzieżą i utrata danych osobowych, udostępnienie haseł osobom postronnym,
- niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
- nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek, przyklejanie kartek z hasłami w szufladach),
- ślady na drzwiach, oknach i szafkach wskazujące na próbę włamania,
- dokumentacja zawierająca dane osobowe niszczona bez użycia niszczarki,
- otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
- obecność osób postronnych w ZSCH,
- złe ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
- wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz ZSCH bez upoważnienia Administratora danych,
- awarie serwera, komputerów, twardych dysków, oprogramowania,
- udostępnienie danych osobowych osobom nieupoważnionym,
- telefoniczne próby wyłudzenia danych osobowych,
- kradzież, zagubienie komputerów lub CD, twardych dysków, pen- drive z danymi osobowymi,
- maile nakłaniające do ujawnienia identyfikatora lub hasła,
- zainfekowanie komputerów wirusem lub inne błędne zachowanie komputerów,
- zdarzenia losowe (pożar, zalanie wodą, utrata zasilania, utrata łączności),
- włamanie do systemu informatycznego lub pomieszczeń,
- kradzież danych/sprzętu,
- świadome zniszczenie dokumentów.

Ponadto należy udokumentować wystąpienie incydentu, jego skutki oraz podjęte działania naprawcze i zaradcze. W przypadku gdy incydent skutkuje naruszeniem praw lub wolności osób fizycznych, Administrator danych zgłasza je w ciągu 72 godzin Prezesowi Urzędu Ochrony Danych Osobowych oraz gdy istnieje taki wymóg, powiadamia o tym fakcie osoby, których incydent dotyczył.

§18

Zabezpieczenie sprzętu.

1. Komputery w ZSCH są zasilane za pośrednictwem całkowitych zasilaczy (UPS).
2. W celu zapewnienia większego bezpieczeństwa i ochrony danych powinno wykorzystać się system operacyjny Microsoft Windows, posiadający rozbudowane mechanizmy nadawania uprawnień i praw dostępu. Dla pełnego wykorzystania mechanizmów należy stosować system plików NTFS, który zapewnia wsparcie mechanizmu ochrony plików i katalogów oraz mechanizmów odzyskiwania na wypadek uszkodzenia dysku lub awarii komputerów.
3. Informatyk jest jedyną osoba uprawnioną do instalowania i usuwania oprogramowania systemowego i narzędziowego. Dopuszcza się instalowanie tylko legalnie pozyskanych programów, niezbędnych do wykonywania ustalonych i statutowych zadań ZSCH i posiadających ważną licencję użytkownika.
4. Bieżąca konserwacja sprzętu wykorzystywanego w ZSCH do przetwarzania danych prowadzona jest przez Informatyka.
5. Poważne naprawy wykonywane przez pracowników firm zewnętrznych realizowane są w budynku ZSCH po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych, określającej kary umowne za naruszanie bezpieczeństwa danych.
6. Dopuszcza się konserwowanie i naprawę sprzętu poza ZSCH jedynie po trwałym usunięciu danych osobowych. Zużyty sprzęt służący do przetwarzania danych osobowych, można zbyć dopiero po usunięciu danych osobowych, a urządzenia uszkodzone mogą być przekazywane do utylizacji (jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony ZSCH) właściwym podmiotom, z którymi także zawiera się umowy powierzania przetwarzanych danych.
7. Wszystkie awarie, działania konserwacyjne i naprawy systemu informatycznego są opisywane w stosownych protokołach, które podpisują osoby uczestniczące w naprawie lub konserwacji.

§19

Zabezpieczenia we własnym zakresie.

W celu podniesienia bezpieczeństwa danych każda osoba upoważniona do przetwarzania danych lub użytkownik systemu informatycznego zobowiązani są do:

1. Ustawiania ekranów komputerowych tak, aby osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia.
2. Niepozostawienia bez kontroli dokumentów i nośników danych w pokojach biurowych i innych miejscach publicznych oraz w samochodach.
1. Dbania o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie).
2. Niepodłączania do listew, podtrzymujących napięcie, przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory).
3. Pilnego strzeżenia akt i nośników komputerowych.
4. Kasowania po wykorzystaniu danych na dyskach przenośnych.
5. Niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku.
6. Powstrzymywania się przez osoby upoważnione do przetwarzania danych osobowych od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu, nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych.
7. Przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła.
8. Obowiązku utrzymania czystego biurka i ekranu – załącznik nr 2.
9. Opuszczania stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób.
10. Kopiowania tylko jednostkowych danych (pojedynczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane.
11. Udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej.
12. Niewynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej.
13. Wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie.
14. Kończenia pracy stacji roboczej po wprowadzeniu danych przetwarzanych tego dnia w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w ups i listwie.
15. Niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończonym dniu pracy.
16. Niepozostawianie osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych.
17. Zachowania tajemnicy danych, w tym także wobec najbliższych.
18. Chowania do zamykanych na klucz szaf wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy.
19. Umieszczanie kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy.
20. Zamykanie okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych.
21. Zamykanie okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy.
22. Zamykania drzwi na klucz po zakończeniu pracy w danym dniu i złożenia klucza w sekretariacie. Jeśli niemożliwe jest umieszczenie wszystkich dokumentów, zawierających dane osobowe w zamykanych szafach, należy powiadomić o tym Dyrektora ZSCH, który zgłasza osobie sprzątającej jednorazową rezygnację z wykonywania swej pracy. W takim przypadku także należy zostawić klucz w sekretariacie.

Postępowanie z nośnikami danych i ich bezpieczeństwo.

Osoby upoważnione do przetwarzania danych osobowych powinny pamiętać zwłaszcza, że:

1. Dane z nośników przenośnych niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego Administratora danych powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD-ROM) lub usunięcie danych programem trwale usuwającym pliki. Jeśli istnieje uzasadniona konieczność, dane pojedynczych osób (a nie całe zbiory czy szerokie wypisy ze zbiorów) mogą być przechowywane na specjalnie oznaczonych nośnikach. Nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nieudostępnianych osobom postronnym. Po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone,
2. Uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie w niszczarce służącej do niszczenia nośników,
3. Zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych kart, jeśli zawierają one dane chronione. Zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów,
4. Po wykorzystaniu wydruki, zawierające dane osobowe, należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę Administratora danych.

§21

Wymiana danych i ich bezpieczeństwo.

1. Sporządzanie kopii zapasowych następuje w trybie opisanym w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
2. Inne wymogi bezpieczeństwa systemowego są określane w instrukcjach obsługi producentów sprzętu i używanych programów, wskazówkach Administratora danych oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".
3. Pocztą elektroniczną można przesyłać tylko jednostkowe dane, a nie całe bazy lub szerokie z nich wypisy i tylko w postaci zaszyfrowanej. Chroni to przesyłane dane przed „przesłuchami" na liniach teletransmisyjnych oraz przed przypadkowym rozproszeniem ich w Internecie.
4. Przed atakami z sieci zewnętrznej wszystkie komputery Administratora danych (w tym także przenośne) chronione są środkami dobranymi przez Administratora danych osobowych. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy informować Administratora danych osobowych oraz umożliwić mu monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa.
5. Informatyk dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń (nowe wirusy, robaki, trojany, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu informatycznego Administratora danych i powiększania bazy danych. Jednocześnie należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie wywołuje nowych zagrożeń.
6. Należy stosować następujące sposoby kryptograficznej ochrony danych:

– przy przesyłaniu danych za pomocą poczty elektronicznej stosuje się POP – tunelowanie, szyfrowanie połączenia,
– przy przesyłaniu danych pracowników, niezbędnych do wykonania przelewów wynagrodzeń, używa się bezpiecznych stron https://.

§22

Kontrola dostępu do systemu.

1. Administrator danych osobowych przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem. System wymusza zmianę hasła przy pierwszym logowaniu.
2. Pierwsze hasło wymagane do uwierzytelnienia się w systemie przydzielane jest przez Informatyka po odebraniu upoważnienia do przetwarzania danych.

3. Do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń Administratora danych osobowych.

§23
Kontrola dostępu do sieci.

1. System informatyczny posiada szerokopasmowe połączenie z Internetem.
2. Operacje za pośrednictwem rachunku bankowego Administratora danych i rachunku bankowego jednostek obsługiwanych, może wykonywać wyłącznie Dyrektor, Z-ca Dyrektora, Główny Księgowy, Zastępca Głównego księgowego, upoważniony przez Dyrektora ZSCH, pracownik po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek.

§24
Komputery przenośne i praca na odległość.

W ZSCH używa się komputerów przenośnych do przetwarzania danych osobowych, które uruchamia się po wprowadzeniu hasła. Użytkowanie komputerów przenośnych określa regulamin użytkowania komputerów przenośnych stanowiący załącznik nr 3 do niniejszej Polityki.

§25
Monitorowanie dostępu do systemu i jego użycia.

1. Odpowiedzialnym za monitorowanie dostępu do systemu i jego użycia jest Administrator danych osobowych lub upoważniona przez niego osoba. Administrator danych osobowych kontroluje przebieg monitorowania i jego rezultaty.
2. System informatyczny, działający w ZSCH, powinien zapewnić odnotowanie:
   - daty pierwszego wprowadzenia danych do systemu,
   - identyfikatora użytkownika wprowadzającego dane osobowe do systemu,
   - źródła danych - w przypadku zbierania danych nie od osoby, której one dotyczą,
   - informacji o odbiorcach w rozumieniu art. 7 pkt 6 Ustawy, którym dane osobowe zostały udostępnione, o dacie i zakresie tego udostępnienia,
   - sprzeciwu wobec przetwarzania danych osobowych, o którym mowa w art. 32 ust. 1 pkt. 8 Ustawy.
3. Odnotowanie informacji, o których mowa w pkt. 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
4. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w pkt. 1-5.
5. System informatyczny Administratora danych umożliwia zapisywanie zdarzeń wyjątkowych na potrzeby audytu i przechowywanie informacji o nich przez określony czas. Zapisy takie obejmują:
   - identyfikator użytkownika,
   - datę i czas zalogowania i wylogowania się z systemu,
   - tożsamość stacji roboczej,
   - zapisy udanych i nieudanych prób dostępu do systemu,
   - zapisy udanych i nieudanych prób dostępu do danych osobowych i innych zasobów systemowych.

Udostępnianie danych osobowych.

1. Udostępnianie danych osobowych policji i sądom może nastąpić w związku z prowadzonym przez nie postępowaniem.
2. Udostępnianie informacji policji odbywa się według następującej procedury:
    1) Udostępnianie danych osobowych funkcjonariuszom policji może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną i zawierać:
        - oznaczenie wnioskodawcy,
        - wskazanie przepisów uprawniających do dostępu do informacji,
        - określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia,
        - wskazanie imienia, nazwiska i stopnia służbowego policjanta upoważnionego do pobrania informacji lub zapoznania się z ich treścią.
    2) Udostępnianie danych osobowych na podstawie ustnego wniosku, zawierającego wszystkie powyższe cztery elementy wniosku pisemnego może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania, np. w trakcie pościgu za osobą podejrzaną o popełnienie czynu zabronionego albo podczas wykonywania czynności mających na celu ratowanie życia i zdrowia ludzkiego lub mienia.
    3) Osoba udostępniająca dane osobowe, jest obowiązana zażądać od policjanta pokwitowania pobrania dokumentów zawierających informacje przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść informacji. Policjant jest obowiązany do pokwitowania lub potwierdzenia.
    4) Jeśli informacje są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności zwrócić się z prośbą o pokwitowanie albo potwierdzenie. Jeśli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie są możliwe, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.
    5) Jeśli policjant pouczył osobę udostępniającą informacje o konieczności zachowania tajemnicy faktu i okoliczności przekazania informacji, to okoliczność ta jest odnotowywana w rejestrze udostępnień niezależnie od odnotowania faktu udostępniania informacji.
3. Innym podmiotom dane osobowe, dotyczące pracowników nie mogą być udostępniane.

§27

Umowa powierzenia przetwarzania danych osobowych

W przypadku zlecania przetwarzania danych osobowych podmiotom zewnętrznym Administrator danych zobowiązany jest zawrzeć umowę powierzenia. W ZSCH prowadzony jest rejestr umów powierzenia przetwarzania danych osobowych.
Umowa określa kategorie osób, których dane dotyczą, obowiązki i prawa Administratora. Ponadto zobowiązuje podmiot przetwarzający do:

- przetwarzania danych osobowych wyłącznie na udokumentowane polecenie Administratora, którymi w szczególności są dokumenty dotyczące płac: umowa o pracę umowa cywilno- prawna, porozumienia stron zmieniające warunki pracy i płacy, świadectwa pracy.
- zapewniania, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób,
- podejmowania wszelkich środków wymaganych na mocy art. 32 RODO,
- przestrzegania warunków umowy do przetwarzania danych osobowych
- pomagania Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO,
- pomagania Administratorowi wywiązać się z obowiązków określonych w art. 32 – 36 RODO,
- usuwania lub zwracania Administratorowi danych osobowych oraz usuwania wszelkich istniejących kopii, chyba że prawo Unii lub prawo Państwa członkowskiego nakazują przechowywanie danych osobowych,
- udostępniania Administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w przepisach RODO

§28

Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych.

1. Niezastosowanie się do prowadzonej przez Administratora danych polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.
2. Niezależnie od rozwiązania stosunku pracy osoby, popełniające przestępstwo, będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 51 i 52 ustawy oraz art. 266. Kodeksu karnego.

§29

Przegląd polityki bezpieczeństwa i audyt systemu

1. Polityka bezpieczeństwa powinna być poddawana przeglądowi raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych Administrator danych osobowych może zarządzić przegląd polityki bezpieczeństwa stosownie do potrzeb.
2. Administrator danych osobowych analizuje, czy polityka bezpieczeństwa o pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:
   - zmian w budowie systemu informatycznego,
   - zmian organizacyjnych Administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
   - zmian w obowiązującym prawie.
3. Administrator ZSCH może stosownie do potrzeb przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Zakres, przebieg i rezultaty audytu dokumentowane są na piśmie w protokole podpisanym przez Administratora danych osobowych.

§30

Postanowienia końcowe

1. Każda osoba, upoważniona do przetwarzania danych osobowych, zobowiązana jest do zapoznania się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz instrukcja zarządzania, regulaminem ochrony danych, procedurą alarmową i złożyć stosowne oświadczenie (załącznik nr 4) potwierdzające znajomość ich treści.
2. Nie zastosowanie się do postanowień niniejszego dokumentu i naruszenie procedur ochrony danych jest traktowane jako ciężkie naruszenie obowiązków służbowych, skutkujące poważnymi konsekwencjami prawnymi włącznie z rozwiązaniem stosunku pracy na podstawie art. 52. Kodeksu pracy.

§31

Polityka bezpieczeństwa, wchodzi w życie z dniem podpisania.