Polityka bezpieczeństwa przetwarzania danych osobowych w Stowarzyszeniu Centrum Wspierania Aktywności Lokalnej CAL.

Celem *Polityki bezpieczeństwa przetwarzania danych osobowych* zwanej dalej *Polityką bezpieczeństwa* jest określenie kierunków działań oraz wsparcia dla zapewnienia bezpieczeństwa przetwarzania zbiorów danych osobowych zarządzanych przez Stowarzyszenie Centrum Wspierania Aktywności Lokalnej CAL (dalej CAL).

1. Podstawę prawną dla opracowania i wdrożenia niniejszej *Polityki bezpieczeństwa* stanowią:
   a. Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jedn. Dz. U. z 2002 r., nr 101, poz. 926 z późn. zm.);
   b. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., nr 100, poz. 1024).
2. CAL zarządza bezpieczeństwem informacji i danych osobowych w celu zapewnienia sprawnego i zgodnego z przepisami prawa wykonywania swoich zadań oraz zadań wykonywanych na podstawie umów lub powierzonych do wykonania na podstawie porozumień.
3. Przez bezpieczeństwo danych osobowych przetwarzanych przez CAL rozumie się zapewnienie ich poufności, integralności i dostępności oraz zapewnienie rozliczalności działań.
   a. **Poufność informacji** – rozumiana jest jako zapewnienie, że tylko uprawnieni pracownicy oraz inne uprawnione osoby mają dostęp do informacji,
   b. **Integralność informacji** – rozumiana jest jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,
   c. **Dostępność informacji** – rozumiana jest jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
   d. **Zarządzanie ryzykiem** – rozumiane jest jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych,
   c. **Rozliczalność działań** – rozumiana jest jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwe jest zidentyfikowanie użytkownika, który działania te wykonał.
4. Zakres przedmiotowy stosowania niniejszej *Polityki bezpieczeństwa* obejmuje wszystkie zbiory danych osobowych przetwarzane w CAL, zarówno w formie elektronicznej, jak i tradycyjnej.
5. W zakresie podmiotowym *Polityka bezpieczeństwa* obowiązuje wszystkich pracowników CAL oraz inne osoby mające dostęp do danych osobowych, w tym stażystów, praktykantów, osoby zatrudnione na umowę zlecenia lub umowę o dzieło itp.
6. *Polityka bezpieczeństwa* jest wewnętrznym dokumentem CAL, skierowanym do osób zatrudnionych czy zajmujących się z ramienia CAL przetwarzaniem danych osobowych.

Stosowana terminologia

Administrator Danych Osobowych (ADO) – osoba odpowiedzialna za całokształt zagadnień związanych z przetwarzaniem danych osobowych w administrowanych przez nią zbiorach danych.
Administrator Bezpieczeństwa Informacji (ABI) – pracownik CAL wyznaczony do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych.
Lokalny Administrator Bezpieczeństwa Informacji (LABI) – osoba odpowiedzialna za przestrzeganie zasad ochrony danych osobowych i nadzorująca bezpieczeństwo przetwarzanych danych osobowych.Każdy kierownik komórki organizacyjnej oraz osoba zatrudniona na samodzielnym stanowisku pracy (koordynator) wykonuje zadania Lokalnego Administratora Bezpieczeństwa Informacji.
Administrator Systemu Informatycznego (ASI) – pracownik zatrudniony w CAL (na podstawie umowy o pracę lub umowy cywilnoprawnej) , odpowiedzialny za funkcjonowanie systemów i urządzeń informatycznych w CAL, stosowanie technicznych i organizacyjnych środków ochrony oraz przestrzeganie zasad ochrony danych osobowych w systemie informatycznym i nadzorujący przetwarzanie danych osobowych w systemie informatycznym.
Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden z kilku specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
Zbiór danych osobowych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony (jego części znajdują się w różnych miejscach) lub podzielony funkcjonalnie (przetwarzany za pomocą programów realizujących różne funkcje).
Wykaz zbiorów danych osobowych – wykaz zarejestrowanych, oraz niepodlegających rejestracji zbiorów danych osobowych.
System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
Bezpieczeństwo systemu informatycznego – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych w celu zapewnienia ochrony przed nieuprawnionym dostępem i przetwarzaniem danych osobowych, a także ich utratą.
Sieć lokalna – połączenie systemów informatycznych w CAL wyłącznie dla własnych jego potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.
Przetwarzanie danych – wszystkie operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
Pracownik – osoba zatrudniona w CAL na podstawie umowy o pracę lub umowy cywilnoprawnej.
Użytkownik systemu informatycznego – użytkownikiem może być pracownik CAL, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż absolwencki lub praktykę studencką w CAL.
Identyfikator użytkownika (LOGIN) – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

Hasło – ciąg znaków literowych cyfrowych lub innych, stanowiący tajemnicę użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym; w połączeniu z identyfikatorem użytkownika umożliwiający uwierzytelnienie w systemie informatycznym.
Uwierzytelnienie (zalogowanie) – działanie, którego celem jest weryfikacja deklarowanej tożsamości użytkownika.
Odbiorca danych – każdy, komu udostępnia się dane osobowe, z wyłączeniem:

a. osoby, której dane dotyczą,
b. osoby upoważnionej do przetwarzania danych,
c. przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych,
d. podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,
e. organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

Osoba trzecia – każda osoba nieupoważniona i przez to nieuprawniona do dostępu do danych osobowych lub zbiorów tych danych.
Usuwanie danych – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

Polityka bezpieczeństwa przetwarzania danych osobowych określa:

I. Odpowiedzialność za bezpieczeństwo informacji i danych osobowych przetwarzanych w CAL.
II. Wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.
III. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.
IV. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.
V. Sposób przepływu danych pomiędzy poszczególnymi systemami.
VI. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
VII. Przeglądy i aktualizacje Polityki.
VIII. Postanowienia końcowe.

I. ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO INFORMACJI I DANYCH OSOBOWYCH PRZETWARZANYCH W CAL

1. CAL zabezpiecza dane osobowe przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. W imieniu Administratora Danych Osobowych nadzór nad przestrzeganiem zasad ochrony danych osobowych sprawuje Administrator Bezpieczeństwa Informacji.
3. Każdy pracownik przetwarzający dane osobowe zarządzane przez Administratora Danych Osobowych posiada pisemne upoważnienie do przetwarzania danych osobowych zawierające:
   a. imię i nazwisko,
   b. datę nadania i okres jego obowiązywania,
   c. zakres danych, które może przetwarzać (zbiory danych).
4. Każdy pracownik przetwarzający dane osobowe zobowiązany jest zapewnić ich należytą ochronę, a w szczególności przestrzegać zasad ochrony, o których mowa w części VI niniejszej *Polityki bezpieczeństwa*.
5. Bezpośredni nadzór nad przetwarzaniem danych osobowych w komórkach organizacyjnych CAL sprawują kierownicy komórek będący Lokalnymi Administratorami Bezpieczeństwa Informacji.
6. Obowiązek przestrzegania tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia, a także zasad funkcjonowania systemów i urządzeń służących do ich przetwarzania spoczywa na wszystkich pracownikach, którzy mają do nich dostęp, również po ustaniu stosunku pracy lub rozwiązaniu umowy cywilnoprawnej.
7. Przetwarzanie danych osobowych sprzeczne z przepisami ustawy o ochronie danych osobowych może stanowić ciężkie naruszenie obowiązków pracowniczych lub obowiązków umownych (umowa cywilnoprawna).

ADMINISTRATOR DANYCH OSOBOWYCH (ADO)

Administratorem Danych Osobowych (ADO) jest CAL, reprezentowany przez Zarząd.
Administrator Danych Osobowych odpowiedzialny jest za:

1. realizację ustawy o ochronie danych osobowych w zakresie dotyczącym administratora danych,
2. ustalanie wykazu informacji stanowiących tajemnicę CAL,
3. stosowanie niezbędnych środków technicznych i organizacyjnych w celu zapewnienia ochrony przetwarzanych w CAL danych osobowych,
4. wyznaczenie Administratora Bezpieczeństwa Informacji (ABI) odpowiedzialnego za bezpieczeństwo przetwarzanych danych osobowych zarówno w formie tradycyjnej – papierowej, jak i w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI (ABI)

Administratora Bezpieczeństwa Informacji (ABI) powołuje Administrator Danych Osobowych.
Administrator Bezpieczeństwa Informacji odpowiedzialny jest za:

1. realizację ustawy o ochronie danych osobowych w zakresie dotyczącym Administratora Bezpieczeństwa Informacji,
2. zapewnienie, że do danych osobowych i informacji chronionych mają dostęp wyłącznie osoby upoważnione,
3. rozpatrywanie wniosków Lokalnych Administratorów Bezpieczeństwa Informacji o udzielenie upoważnienia do przetwarzania danych osobowych (do dostępu do danych lub do przebywania w obszarze przetwarzania danych) i nadawanie uprawnień w systemie informatycznym,
4. przygotowywanie stosownych upoważnień dla pracowników i wydawanie ich pracownikom,
5. zlecenie modyfikacji uprawnień w systemie informatycznym w przypadku odebrania lub zmiany upoważnienia do przetwarzania danych osobowych,
6. prowadzenie rejestru osób upoważnionych do przetwarzania danych osobowych,
7. zgłoszenie konieczności uzupełnienia zakresu czynności osoby zatrudnionej przy przetwarzaniu danych osobowych o zakres odpowiedzialności tej osoby za ochronę tych danych do jej bezpośredniego przełożonego (Lokalnego Administratora Bezpieczeństwa Informacji),
8. bieżące informowanie użytkowników o obowiązujących w CAL zasadach polityki bezpieczeństwa przetwarzania danych osobowych,
9. określenie budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego,
10. kontrolowanie komórek organizacyjnych w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarza się dane osobowe,
11. wydawanie poleceń kierownikom komórek organizacyjnych w zakresie bezpieczeństwa danych osobowych,
12. przedstawianie Administratorowi Danych Osobowych – w miarę potrzeb - odpowiednich propozycji zmian do *Instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych*,
13. informowanie Administratora Danych Osobowych o przypadkach naruszenia bezpieczeństwa danych osobowych,
14. przygotowanie i aktualizację dokumentów polityki bezpieczeństwa informacji,

15. opracowanie instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji,
16. nadzorowanie przestrzegania zasad określonych w *Polityce bezpieczeństwa* i *Instrukcji* dotyczących ochrony bezpieczeństwa danych osobowych,

*L*OKALNY ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI (LABI)

Rolę Lokalnych Administratorów Bezpieczeństwa Informacji (LABI) pełnią, kierownicy komórek organizacyjnych oraz pracownicy zatrudnieni na samodzielnych stanowiskach pracy (koordynatorzy), w których przetwarzana jest dana grupa informacji.
Lokalny Administrator Bezpieczeństwa Informacji odpowiedzialny jest za:

1. współdziałanie z Administratorem Bezpieczeństwa Informacji w zakresie przestrzegania zasad ochrony danych osobowych w CAL,
2. poprawność merytoryczną danych gromadzonych w zbiorach danych osobowych,
3. określanie miejsca i czasu przetwarzania, przechowywania, tworzenia i niszczenia informacji należącej do danej grupy,
4. niezwłocznego zawiadomienia Administratora Bezpieczeństwa Informacji o konieczności utworzenia nowego zbioru danych osobowych, nie ujętego w niniejszej Polityce,
5. ewidencjonowanie udostępniania danych zgodnie z ustawą o ochronie danych osobowych,
6. wskazanie ASI dodatkowych nie ujętych w *Instrukcji zarządzania systemem informatycznym*, rodzaju aplikacji informatycznych, które są niezbędne do realizacji zadań i prowadzenia zbiorów danych w komórce organizacyjnej,
7. występowanie do Administratora Bezpieczeństwa Informacji z wnioskiem o nadanie, modyfikację lub odebranie uprawnień do przetwarzania danych osobowych dla podległych pracowników,
8. powiadomienie Administratora Systemu Informatycznego o konieczności utworzenia identyfikatora użytkownika w systemie,
9. wdrażanie zasad i procedur określonych w niniejszej *Polityce bezpieczeństwa* i *Instrukcji zarządzania systemem informatycznym* w podległej komórce organizacyjnej.

Praca Lokalnych Administratorów Bezpieczeństwa Informacji jest nadzorowana pod względem bezpieczeństwa przez Administratora Bezpieczeństwa Informacji.

ADMINISTRATOR SYSTEMU INFORMATYCZNEGO (ASI)

Rolę Administratora Systemu Informatycznego (ASI) pełni podmiot wskazany przez CAL.
Administrator Systemu Informatycznego odpowiedzialny jest za:

1. bieżący monitoring oraz zapewnianie ciągłości działania systemu informatycznego i systemów baz danych,
2. optymalizację wydajności systemu informatycznego i systemów baz danych,
3. instalację i konfigurację sprzętu sieciowego i serwerowego,
4. instalację, konfigurację i administrację oprogramowaniem systemowym, sieciowym i bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
5. konfigurację i administrację systemem pocztowym CAL,
6. przyznawanie na wniosek Lokalnego Administratora Bezpieczeństwa Informacji, za zgodą Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do informacji w danym systemie bazodanowym – definiowanie użytkowników i ich praw oraz haseł dostępu,

7. prowadzenie rejestru osób dopuszczonych do systemu informatycznego i systemu baz danych (rejestr powinien zawierać: imię i nazwisko osoby, pełnioną rolę, grupę informacji, czas trwania dostępu),
8. nadzorowanie funkcjonowania mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolę dostępu do danych osobowych,
9. przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe,
10. współpracę z dostawcami usług, aplikacji i sprzętu sieciowego, serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
11. nadzór nad wdrożonymi aplikacjami (przeglądanie, nadawanie i odbieranie uprawnień użytkownikom, definiowanie słowników itp.),
12. weryfikację możliwości integracji systemów informatycznych i aplikacji bazodanowych,
13. zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego i sieciowego,
14. zarządzanie kopiami awaryjnymi danych w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
15. wykonywanie i nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu,
16. nadzorowanie przeglądów, konserwacji oraz uaktualnień systemów służących do przetwarzania danych osobowych oraz wszystkich innych czynności wykonywanych na bazach danych osobowych,
17. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
18. aktualizowanie oprogramowania antywirusowego i innego, chyba że aktualizacje te wykonywane są automatycznie,
19. zapewnienie przeszkolenia użytkowników w zakresie prawidłowego korzystania z aplikacji bazodanowych zgodnie z powierzonymi im obowiązkami,
20. świadczenie pomocy technicznej w ramach aplikacji bazodanowych dla użytkowników,
21. wykorzystywanie narzędzi baz danych dla tworzenia zestawień,
22. prowadzenie – w porozumieniu z ABI – zakupów urządzeń sieciowych i serwerowych oraz oprogramowania sieciowego i serwerowego,
23. nadzór nad wykorzystywanym w CAL oprogramowaniem oraz jego legalnością,
24. wnioskowanie do Administratora Bezpieczeństwa Informacji w sprawie procedur bezpieczeństwa i standardów zabezpieczeń.
25. instalowanie nowych urządzeń i oprogramowania do przetwarzania danych osobowych niezbędnego dla prawidłowej realizacji zadań CAL,
26. nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe,
27. nadzór i kontrolę systemów informatycznych służących do przetwarzania danych osobowych,
28. ochronę i bezpieczeństwo danych osobowych zawartych w zbiorach systemów informatycznych CAL,
29. badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych,
30. podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych,
31. analizę sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło) i przygotowanie oraz przedstawienie

Administratorowi Danych Osobowych odpowiednich zmian do *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych*,
32. sporządzanie raportów z naruszenia bezpieczeństwa systemu informatycznego,
33. współdziałanie z Administratorem Bezpieczeństwa Informacji w zakresie przestrzegania instrukcji określającej sposób zarządzania systemem informatycznym.

UŻYTKOWNIK

Użytkownikiem jest każdy, kto posiada pisemne upoważnienie do przetwarzania danych osobowych wydane przez Administratora Danych Osobowych.
Użytkownik odpowiedzialny jest za:

1. zapoznanie się i przestrzeganie przepisów prawa w zakresie ochrony danych osobowych,
2. stosowanie określonych przez Administratora Danych Osobowych, procedur i środków mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,
3. zachowanie szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, których te dane dotyczą,
4. zachowanie szczególnej staranności przy gromadzeniu danych, aby dane te były:
   a. przetwarzane zgodnie z prawem,
   b. zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
   c. merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.
5. poprawne korzystanie z aplikacji zgodnie z powierzonymi obowiązkami służbowymi,
6. ustalenie hasła i okresowe jego zmiany,
7. utrzymywanie w ścisłej tajemnicy haseł, którymi się posługuje,
8. zmianę hasła w przypadku powzięcia przez użytkownika podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby trzecie i powiadomienie o tym fakcie Administratora Bezpieczeństwa Informacji,
9. informowanie Lokalnego Administratora Bezpieczeństwa Informacji, Administratora Bezpieczeństwa Informacji lub Administratora Systemu Informatycznego o wszelkich nieprawidłowościach działania systemu i zauważonych nieprawidłowościach danych gromadzonych w systemie,
10. zgłaszanie awarii urządzeń komputerowych, oprogramowania systemowego, sieci informatycznej Administratorowi Systemu Informatycznego,
11. dbałość o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania danych zgodnie z obowiązującą w CAL *Polityką bezpieczeństwa*, regulaminami i instrukcjami wewnętrznymi, w tym m. in.:
    a. Chronić dane przed dostępem osób nieupoważnionych,
    b. Chronić dane przed przypadkowym lub nieumyślnym zniszczeniem, utratą lub modyfikacją,
    c. Chronić nośniki magnetyczne i optyczne oraz wydruki komputerowe przed dostępem osób nieupoważnionych oraz przed przypadkowym zniszczeniem,
    d. Utrzymywać w tajemnicy powierzone identyfikatory, hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w CAL.

Zabrania się pod rygorem odpowiedzialności służbowej i karnej:
1. Ujawniać dane – w tym dane osobowe zawarte w obsługiwanych systemach,

2. Kopiować bazy danych lub ich części poza tworzonymi kopiami bezpieczeństwa przewidzianymi Instrukcją zarządzania systemem informatycznym,
3. Przetwarzania danych w sposób inny niż opisany Instrukcją zarządzania systemem informatycznym .

II. WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

1. Dane osobowe przetwarzane są w biurze CAL w Warszawie przy ul. Mazowieckiej 11/14, 00-052 Warszawa w lokalach nr 3 i 14.
2. Część informacji przetwarzana jest również na komputerach przenośnych.
3. W uzasadnionych przypadkach (np. awaria) administratorzy mogą uzyskać dostęp do systemu informatycznego CAL z dowolnego pomieszczenia, w którym jest sieć komputerowa. Uzyskiwanie takiego dostępu przez innych użytkowników jest zabronione.
4. Pomieszczenia zabezpiecza się przed dostępem osób trzecich na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych.
5. Przebywanie osób trzecich w obszarze przetwarzania danych osobowych, jest dopuszczalne za zgodą Administratora Danych Osobowych lub Administratora Bezpieczeństwa Informacji lub w obecności osoby upoważnionej do przetwarzania danych.

III. WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

1. Za zbiór danych osobowych przetwarzanych w CAL uważa się:
   a. dokumentację papierową (korespondencja, wnioski, deklaracje, umowy, itd.);
   b. systemy informatyczne przetwarzania danych oraz oprogramowanie komputerowe służące do przetwarzania informacji;
   c. wydruki komputerowe.
2. Poniżei przedstawiono wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania:
   a. Dokumentacja pracownicza – program SYMFONIA;–
   b. Dokumentacja księgowa – program SYMFONIA
   c. Dokumentacja związana z realizowanymi projektami – pakiet MS OFFICE
3. Wykaz, o którym mowa w pkt. 2 prowadzi Administrator Bezpieczeństwa Informacji.
4. O zmianach w wykazie zbiorów danych informują kierownicy poszczególnych komórek organizacyjnych Administratora Bezpieczeństwa Informacji.
5. W CAL nie są przetwarzane dane, o których mowa w art. 27 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
6. W CAL obowiązuje wysoki poziom bezpieczeństwa (system informatyczny połączony jest z siecią publiczną), z wyjątkiem zbiorów przetwarzanych w wersji papierowej (podstawowy poziom bezpieczeństwa).

IV. OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMATYCZNYCH I POWIĄZANIA MIĘDZY NIMI

1. Dane osobowe są przetwarzane przy zastosowaniu systemów informatycznych, w zbiorach ewidencyjnych oraz poza zbiorami.
2. Zbiory danych osobowych zlokalizowane są w przedmiotowych bazach danych umieszczonych na serwerach bazodanowych.
3. Dane osobowe w zbiorach są przetwarzane tylko w aplikacjach (programach) dostosowanych do merytorycznych potrzeb komórek organizacyjnych CAL.
4. Zawartość pól informacyjnych, występujących w aplikacjach (programach) systemów zastosowanych do przetwarzania danych, musi być zgodna z przepisami prawa, które uprawniają lub zobowiązują CAL do przetwarzania danych osobowych.
5. Na żądanie Administratora lub osoby przez niego upoważnionej osoby, LABI, zobowiązani są wskazać podstawy prawne określające zakres przetwarzanych danych.

V. SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

1. Przepływ danych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych może odbywać się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego.
2. Przesyłanie danych pomiędzy systemami może odbywać się w sposób manualny, przy wykorzystaniu nośników zewnętrznych (np. dyskietka, CD, DVD, taśma streamera, dysk wymienny, PenDrive itp.) lub w sposób półautomatyczny, przy wykorzystaniu funkcji eksportu (importu) danych za pomocą teletransmisji (np. poprzez wewnętrzną sieć teleinformatyczną).

VI. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

1. Ochrona zbiorów danych polega na zabezpieczeniu informacji wprowadzonej, przetwarzanej, przesyłanej w systemie informatycznym oraz na nośnikach informacji przed nielegalnym ujawnieniem, kradzieżą oraz nieuprawnioną modyfikacją lub usunięciem.
2. W celu ochrony danych przechowywanych w systemach informatycznych należy wykorzystywać wchodzące w ich skład mechanizmy zarówno sprzętowe jak i programowe oraz inne rozwiązania zwiększające bezpieczeństwo tych danych.

VI. 1. Środki ochrony fizycznej

1. Biuro CAL, w którym zlokalizowany jest obszar przetwarzania danych osobowych jest zamykany po zakończeniu pracy.
2. Dostęp do pomieszczeń, w których są przetwarzane dane osobowe mogą mieć tylko pracownicy CAL.
3. Dostęp do pomieszczeń, o których mowa w pkt. 3 możliwy jest tylko i wyłącznie w godzinach pracy CAL. Dostęp do tych pomieszczeń poza godzinami pracy możliwy jest tylko na podstawie zezwolenia bezpośredniego przełożonego.
4. Wszystkie pomieszczenia, w których przetwarza się dane osobowe są zamykane na klucz w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych – także w godzinach pracy.
5. Klucze do pomieszczeń służbowych znajdują się w biurze CAL. Dostęp do kluczy posiadają tylko pracownicy CAL.
6. Przebywanie w obszarze przetwarzania danych osobowych oraz w pomieszczeniach, w których przechowuje się dane osobowe w kartotekach, rejestrach, skorowidzach, wykazach i ewidencjach – osób nieuprawnionych, dopuszczalne jest tylko w obecności osób upoważnionych do przetwarzania danych.
7. W przypadku przebywania osób postronnych w pomieszczeniach, o których mowa w pkt. 7, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
8. Pracownicy przetwarzający dane osobowe obowiązani są do prawidłowego ich zabezpieczania na swoich stanowiskach pracy i zabezpieczenia przed dostępem do nich osób nieupoważnionych.
9. Ewidencje ręczne i inne dokumenty zawierające dane osobowe przechowywane są w zamykanych szafach.
10. Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych a następnie powinny być zamykane.
11. Dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych a następnie muszą być chowane do szaf.
12. Klucze do szaf, w których przechowywane są zbiory danych osobowych posiadają tylko upoważnieni pracownicy.
13. Dane osobowe w wersji papierowej, a także wydruki i kopie, należy niszczyć w niszczarkach. Zabronione jest usuwanie danych przez wyrzucenie ich do kosza na odpadki.

VI. 2. Środki sprzętowe, informatyczne i telekomunikacyjne

1. Urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej listwą filtrującą oraz urządzeniem UPS w serwerowni.
2. Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej serwera i stacji roboczych, na których przetwarzane są dane osobowe zapewniają zasilacze UPS.
3. Dostęp fizyczny do sieci lokalnej jest ograniczony.
4. Na serwerach oraz stacjach roboczych zainstalowano oprogramowanie antywirusowe. Poczta elektroniczna wpływająca do CAL skanowana jest programem antywirusowym przed przesłaniem jej do użytkownika.

5. Ekrany monitorów ustawiane są do wewnątrz pomieszczeń wydzielonych do przetwarzania danych osobowych, w taki sposób, by uniemożliwić wgląd lub spisanie zawartości aktualnie wyświetlanej na ekranie monitora.
6. Ekrany komputerów, na których przetwarzane są dane osobowe, są chronione wygaszaczami zabezpieczonymi hasłem.
7. W przypadku korzystania z komputerów przenośnych zawierających dane osobowe należy zachować szczególną ostrożność podczas ich używania, transportu lub przechowywania poza obszarem przetwarzania danych wyszczególnionym w niniejszej Polityce.
8. Po zakończeniu pracy komputery (notebook) powinny być zabezpieczone w zamykanych na klucz szafach.
9. W przypadku naprawy, przekazania, likwidacji nośnika (papier, dysk twardy, płyta kompaktowa, dyskietka, taśma magnetyczna), który zawiera dane osobowe podmiotowi nieupoważnionemu do przetwarzania danych, należy zapewnić trwałe wymazanie informacji stanowiących dane osobowe.
10. Pomieszczenia, w których przetwarzane są dane osobowe wyposażone są w mechaniczne niszczarki dokumentów.

VI. 3. Środki ochrony w ramach oprogramowania urządzeń informatycznych

1. Zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (unikalny identyfikator i hasło). Dla każdego użytkownika systemu jest ustalony odrębny identyfikator i hasło.
2. Zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika.
3. Dostęp fizyczny do baz danych osobowych zastrzeżony jest wyłącznie dla Administratora Systemu Informatycznego.
4. Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji.
5. Tworzy się kopie zapasowe.

VI. 4. Środki organizacyjne

1. Administrator Danych Osobowych powołuje Administratora Bezpieczeństwa Informacji (ABI), który nadzoruje przestrzeganie zasad ochrony danych osobowych określonych w instrukcji zarządzania systemem informatycznym z uwzględnieniem spraw dotyczących ochrony danych osobowych przetwarzanych w tradycyjnych rejestrach papierowych (kartotekach).
2. Administrator Danych Osobowych wyznacza Administratora Systemu Informatycznego (ASI) odpowiedzialnego za funkcjonowanie systemu informatycznego CAL.
3. Dostęp do komputerów, na których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy CAL.
4. Do przetwarzania danych osobowych dopuszcza się wyłącznie osoby posiadające pisemne upoważnienie nadane przez administratora danych.
5. Przed dopuszczeniem do przetwarzania danych osobowych – osoby upoważnione do ich przetwarzania, są informowane o ich obowiązkach w zakresie bezpieczeństwa danych. Są one obowiązane do przestrzegania tych przepisów i zachowania w tajemnicy wszelkich informacji z zakresu przetwarzanych danych osobowych i sposobów ich zabezpieczenia.
6. Prowadzona jest ewidencja osób mających dostęp do danych osobowych i upoważnionych do przetwarzania danych osobowych, która zawiera:

a. imię i nazwisko osoby upoważnionej,
b. datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
c. identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

7. Przeglądu oraz konserwacji sprzętu informatycznego, na którym są przetwarzane informacje zawierające dane osobowe – dokonuje Administrator Systemu Informatycznego w obecności osoby zatrudnionej przy przetwarzaniu danych.
8. Określono sposób postępowania z nośnikami informacji.
9. Wprowadzono *Instrukcję zarządzania systemem informatycznym*, stanowiącą integralną cześć niniejszej *Polityki bezpieczeństwa*.

VII. PRZEGLĄDY I AKTUALIZACJE POLITYKI

1. Polityka bezpieczeństwa podlega przeglądowi pod kątem aktualności i stosowalności przez Administratora Bezpieczeństwa Informacji.
2. Aktualizacji Polityki dokonuje Administrator Bezpieczeństwa Informacji. Zatwierdzenia zaktualizowanej Polityki dokonuje Zarząd CAL.

VIII. POSTANOWIENIA KOŃCOWE

Do zapoznania się z niniejszym dokumentem oraz stosowania zawartych w nim zasad zobowiązani są wszyscy pracownicy CAL upoważnieni do przetwarzania danych osobowych.

IX. ZAŁĄCZNIKI

Integralną część niniejszej Polityki stanowią następujące załączniki:

1. Załącznik nr 1 - Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Załącznik nr 1 do Polityki bezpieczeństwa przetwarzania danych osobowych w Stowarzyszeniu Centrum Wspierania Aktywności Lokalnej CAL.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Stowarzyszeniu Centrum Wspierania Aktywności Lokalnej CAL.

I.

Celem *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych* zwanej dalej *Instrukcją* jest określenie sposobu posługiwania się oraz zarządzania systemem informatycznym w CAL.

ZAGADNIENIA OGÓLNE

II.

7. *Instrukcja* jest wewnętrznym dokumentem CAL, skierowanym do użytkowników systemu informatycznego przetwarzających dane osobowe w systemie informatycznym.
8. *Instrukcja* ma zastosowanie do wszelkich danych osobowych znajdujących się lub mogących znajdować się w systemie informatycznym CAL. Opisuje sposoby nadawania uprawnień użytkownikom, określa sposób pracy w systemie informatycznym, procedury zarządzania oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego.
9. Systemy informatyczne działające w CAL mogą być używane tylko na potrzeby realizacji zadań dotyczących CAL
10. Wszystkie osoby zatrudnione przy przetwarzaniu danych osobowych w systemach informatycznych bez względu na zajmowane stanowisko i miejsce pracy oraz charakter stosunku pracy są zobowiązane do postępowania zgodnie z zasadami określonymi w niniejszej *Instrukcji*.

III.

1. Uprawnienia do przetwarzania danych osobowych nadaje Administrator Danych Osobowych.
2. Z wnioskiem o udzielenie upoważnienia do dostępu lub przetwarzania danych osobowych oraz przydzielenie uprawnień w systemie informatycznym dla podległego pracownika występuje Lokalny Administrator Bezpieczeństwa Informacji do Administratora Bezpieczeństwa Informacji.
3. Osoby, które zostały upoważnione do przetwarzania danych osobowych, są obowiązane zachować je i sposoby ich zabezpieczenia w tajemnicy. Zachowanie tajemnicy obowiązuje również po ustaniu zatrudnienia.

IV.

1. Użytkownikom nadawane są uprawnienia do pracy tylko w wymaganych dla realizacji powierzonych zadań modułach i funkcjach programów. Uprawnienia dotyczą zarówno danych gromadzonych w systemie informatycznym, jak również w tradycyjnych rejestrach papierowych.
2. Użytkownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
3. Zmiana zakresu uprawnień następuje na pisemny wniosek przełożonego użytkownika złożony Administratorowi Bezpieczeństwa Informacji i jest realizowana przez Administratora Systemu Informatycznego.

4. Odebranie uprawnień pracownikowi następuje na pisemny wniosek przełożonego, któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień.
5. Odebranie uprawnień skutkuje pozbawieniem tego użytkownika dostępu do danych osobowych przetwarzanych zarówno w formie tradycyjnej jak i w systemie informatycznym oraz wyrejestrowaniem go z wszystkich systemów informatycznych, do których miał uprawnienia.

V.

1. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
2. Pracownik ds. kadr informuje Administratora Bezpieczeństwa Informacji o każdym nowym pracowniku, a także o ustaniu zatrudnienia lub zaprzestaniu świadczenia usług na podstawie umów cywilnoprawnych.

VI.

1. Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia ewidencji osób upoważnionych do dostępu lub przetwarzania danych osobowych oraz obsługi systemu informatycznego służącego do przetwarzania danych osobowych.
2. Ewidencja, o której mowa w pkt. 1 zawiera: imię, nazwisko, datę nadania uprawnień, datę ustania uprawnień, zakres dostępu oraz identyfikator i program komputerowy wykorzystywany do przetwarzania danych.

STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

VII.

1. Każdy użytkownik systemu informatycznego posiada swój odrębny, unikalny identyfikator.
2. Użytkownicy systemu informatycznego zobowiązani są do zachowania w tajemnicy przed osobami trzecimi ustalonych dla nich identyfikatorów. Niedopuszczalna jest wymiana przyznanych identyfikatorów.
3. Identyfikator jednoznacznie identyfikuje, weryfikuje i autoryzuje tożsamość użytkownika, a w szczególności jest podstawą do monitorowania czynności użytkownika w systemie oraz dochodzenia konsekwencji tych czynności.
4. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.

VIII.

1. Każdy użytkownik zarządza swoim hasłem. Zabronione jest przekazywania hasła innym osobom.
2. Hasło użytkownika nie może być takie samo jak identyfikator użytkownika.

IX.

1. Hasło użytkownika powinno być okresowo zmieniane. Zmiany hasła nie wolno zlecać innym osobom.

2. Użytkownik jest w pełnym zakresie odpowiedzialny za swoje hasło, w tym za jego okresowe zmienianie i utrzymywanie w tajemnicy. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
3. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
4. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
5. Niedopuszczalne jest podglądanie haseł wprowadzanych do systemu przez innych użytkowników. Jeżeli użytkownik w pobliżu zaczyna wprowadzać hasło należy odwrócić wzrok. Hasło użytkownika nie jest pokazywane na ekranie lub wydrukach w postaci otwartego tekstu.
6. Hasło użytkownika nie może być przesyłane przez sieć otwartym tekstem.
7. W systemach, które umożliwiają opcję zapamiętywania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.

X.

1. Użytkownik systemu ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
2. W przypadku powzięcia przez użytkownika systemu informatycznego podejrzenia lub stwierdzenia, że z identyfikatorem lub hasłem użytkownika mogły zapoznać się osoby trzecie, obowiązany jest on niezwłocznie zmienić hasło i powiadomić o tym Administratora Bezpieczeństwa Informacji, który zwróci się z wnioskiem do Administratora Systemu Informatycznego o nadanie nowego identyfikatora dla tego użytkownika.

XI.

1. Żaden z użytkowników, łącznie z Administratorem Systemu Informatycznego, nie może mieć możliwości uzyskania z systemu informatycznego aktualnego lub nieważnego hasła innego użytkownika.
2. Administrator Systemu Informatycznego ma możliwość zmiany hasła użytkownika bez znajomości aktualnego lub nieważnego hasła użytkownika.
3. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.
4. Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemu Informatycznego.

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU

XII.

1. Korzystanie z systemu informatycznego możliwe jest w dni pracy CAL w godzinach 8.00 – 16.00.
2. Praca poza okresem wymienionym w pkt. 1 wymaga zgody na piśmie bezpośredniego przełożonego.

XIII.

1. Użytkownik rozpoczyna pracę w systemie informatycznym od uruchomienia systemu i uwierzytelnienia się w systemie operacyjnym przy użyciu indywidualnego identyfikatora oraz hasła.
2. Przed uwierzytelnieniem w systemie użytkownik powinien upewnić się czy inna osoba nie ma możliwości obserwowania wprowadzania haseł.

XIV.
1. W przypadku opuszczenia stanowiska pracy na krótki czas należy zawiesić pracę w systemie i zablokować system przez naciśnięcie klawiszy CTRL+ALT+DEL i wciśnięcie przycisku „Zablokuj Komputer".
2. Zawieszenie pracy w systemie informatycznym może odbywać się poprzez aktywację wygaszacza ekranu z hasłem po 15 minutach od momentu bezczynności stacji roboczej.
3. Po powrocie do swojego stanowiska pracy należy odblokować komputer podając hasło.

XV.
1. Zakończenie pracy w systemie odbywa się przez wylogowanie z systemu oraz wyłączenie komputera.
2. Przed wylogowaniem z systemu należy upewnić się, że wszystkie używane aplikacje zostały wyłączone a wyniki pracy są zachowane. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.
3. Przed odejściem od stanowiska pracy należy upewnić się, że proces wylogowania zakończył się pomyślnie.

XVI.
1. Użytkownik jest zobowiązany do zadbania, aby niemożliwe było odczytanie informacji z monitora przez osoby nieuprawnione poprzez jego odpowiednie ustawienie.
2. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wylogowania z systemu.
3. Zabrania się użytkownikom systemu informatycznego pracującym w systemie:
   a. udostępniania stacji roboczej osobom nie zarejestrowanym w systemie zgodnie z niniejszą Instrukcją;
   b. udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z Administratorem Bezpieczeństwa Informacji;
   c. używania nielicencjonowanego oprogramowania;
   d. instalowania dodatkowego oprogramowania;
   e. używania nośników (CD, DVD, FDD, PEN DRIVE, HDD przenośne i inne) do wymiany informacji bez uprzedniego sprawdzenia programem antywirusowym.

XVII.
1. W sytuacji naruszenia lub podejrzenia naruszenia bezpieczeństwa systemu, użytkownicy zobowiązani są do bezzwłocznego powiadomienia o tym fakcie Lokalnego Administratora Bezpieczeństwa Informacji, Administratora Bezpieczeństwa Informacji lub Administratora Systemu Informatycznego.

PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

XVIII.

1. Za systematyczne wykonywanie i archiwizowanie kopii zapasowych (bezpieczeństwa) odpowiada Administrator Systemu Informatycznego.
2. Kopią zapasową objęte są dane znajdujące się na serwerach sieci informatycznej.
3. Każdą kopię tworzy się na oddzielnym nośniku informatycznym: magnetycznym lub optycznym.
4. Kopie zapasowe tworzone są po zakończeniu pracy wszystkich użytkowników systemu informatycznego.
5. W czasie wykonywania kopii zapasowej dostęp do kopiowanych danych dla wszystkich użytkowników jest zablokowany.

SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ORAZ KOPII ZAPASOWYCH

XIX.

1. Dane osobowe w postaci elektronicznej - za wyjątkiem kopii bezpieczeństwa - zapisane na dyskietkach, dyskach magnetooptycznych czy dyskach twardych nie są wynoszone poza pomieszczenia biura CAL.
2. Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych.
3. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób trwale uniemożliwiający ich odczytanie. Z nośników podlegających zniszczeniu nie wolno sporządzać wydruków.
4. Za bezpieczeństwo danych zapisanych w komputerach przenośnych oraz w innych urządzeniach przenośnych w całości odpowiada użytkownik komputera lub urządzenia przenośnego.

XX.

Kopie bezpieczeństwa.

1. Taśmy, płyty CD, DVD i dyski z kopiami zapasowymi przechowywane są w wyznaczonym miejscu.
2. Dostęp do ww. miejsca mają tylko Administrator Systemu Informatycznego oraz osoby upoważnione przez Administratora Bezpieczeństwa Informacji.
3. Administrator Systemu Informatycznego dokonuje okresowych przeglądów kopii zapasowych i ocenia ich przydatność do odtworzenia zasobów systemu informatycznego w przypadku jego awarii.
4. Stwierdzenie utraty przez kopię zapasową waloru przydatności do celu, o którym mowa powyżej, upoważnia Administratora Systemu Informatycznego do ich zniszczenia i odnotowania tego faktu.

5. Kopie zapasowe usuwa się niezwłocznie w wypadku ich uszkodzenia lub po utracie terminu przechowywania, w sposób trwale uniemożliwiający ich odczytanie.

Wydruki.

1. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom nieupoważnionym.
2. Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.
3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie przy użyciu niszczarki do dokumentów.
4. Trwałego zniszczenia zbędnych wydruków komputerowych dokonuje się na bieżąco w czasie pracy, nie później jednak niż przed opuszczeniem stanowiska pracy.
5. Za zniszczenie zbędnych wydruków i innych zbędnych dokumentów zawierających dane osobowe odpowiedzialny jest każdy pracownik CAL.

SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ SZKODLIWEGO OPROGRAMOWANIA

XXI.

Administrator Systemu Informatycznego zobowiązany jest do poinformowania każdego użytkownika systemu informatycznego o obowiązujących w CAL zasadach bezpieczeństwa danych, a w szczególności o zasadach:

1. bezpiecznej pracy pozwalających unikać szkodliwego oprogramowania,
2. postępowania w przypadku wykrycia, lub podejrzenia działania złośliwego oprogramowania.

XXII.

1. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wirusa wykryto oraz wszystkie posiadane przez użytkownika elektroniczne nośniki informacji.
2. W razie niemożności usunięcia wirusa Administrator Systemu Informatycznego ma obowiązek niezwłocznego przedstawienia Administratorowi Bezpieczeństwa Informacji lub wyznaczonej przez niego osobie, propozycji działań zaradczych. Po usunięciu wirusa Administrator Systemów Informatycznych sprawdza system informatyczny oraz przywraca go do pełnej funkcjonalności.

XXIII.

1. Bezwzględnie zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.
2. Bezwzględnie zakazuje się użytkownikom samowolnego instalowania na stacjach roboczych jakiegokolwiek oprogramowania z jakiegokolwiek źródła, za wyjątkiem aktualizowanych automatycznie komponentów systemu operacyjnego. Jedyną osobą uprawnioną do zainstalowania dodatkowego oprogramowania jest Administrator Systemu Informatycznego.
3. Bezwzględnie zabrania się użytkownikom łamania lub obchodzenia zabezpieczeń systemów informatycznych. O każdym przypadku znalezienia luki w zabezpieczeniach

użytkownik ma obowiązek powiadomić Administratora Bezpieczeństwa Informacji oraz Administratora Systemu Informatycznego.

4. Bezwzględnie zakazuje się użytkownikom wykorzystywania powierzonego im sprzętu informatycznego, oprogramowania i dostępu do zasobów informatycznych do jakichkolwiek celów innych niż wykonywanie powierzonych im obowiązków służbowych lub związanych z własną edukacją i dokształcaniem.
5. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia oraz plików objętych licencją komercyjną. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
6. Użytkownicy są bezpośrednio odpowiedzialni za zainstalowane na powierzonych im stacjach roboczych oprogramowanie oraz mają obowiązek zgłaszać wszelkie wątpliwości w tym zakresie Administratorowi Bezpieczeństwa Informacji lub Administratorowi Systemu Informatycznego.

PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

XXIV.

Przeglądu i konserwacji sprzętu w sieci informatycznej, systemów informatycznych i nośników informacji dokonuje stosownie do potrzeb Administrator Systemu Informatycznego w porozumieniu z Administratorem Bezpieczeństwa Informacji. Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić Administratora Bezpieczeństwa Informacji.

XXV.

1. W przypadku przekazywania stacji roboczej z dyskiem albo innych nośników informacji podmiotowi nieupoważnionemu do przetwarzania danych osobowych do naprawy lub likwidacji, dysk lub nośnik jest demontowany i pozbawiany wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie.
2. Jeżeli nie jest możliwe pozbawienie urządzenia zapisu danych osobowych, naprawa urządzenia dokonywana jest w obecności Administratora Systemu Informatycznego lub innej osoby upoważnionej przez Administratora Bezpieczeństwa Informacji.

XXVI.

1. Użytkownik ma obowiązek niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji lub Administratora Systemu Informatycznego o wszelkich nieprawidłowościach i awariach sprzętu informatycznego, mogących prowadzić do próby naruszenia lub naruszenia bezpieczeństwa danych osobowych.
2. Bezwzględnie zabronione jest samodzielne dokonywanie przez użytkowników napraw sprzętu informatycznego, wymiana jego podzespołów oraz wykonywanie innych czynności niezwiązanych bezpośrednio z jego eksploatacją lub niedopuszczonych do wykonywania przez producenta sprzętu w instrukcji obsługi.

POSTANOWIENIA KOŃCOWE

XXVII.

1. Administrator Bezpieczeństwa Informacji nadzoruje przestrzeganie zasad określonych w *Polityce bezpieczeństwa przetwarzania danych osobowych* oraz niniejszej *Instrukcji*.
2. Lokalny Administrator Bezpieczeństwa Informacji odpowiedzialny jest za przestrzeganie zasad ochrony danych osobowych zgromadzonych w systemie informatycznym oraz w tradycyjnych rejestrach papierowych prowadzonych w podległej komórce.

XXVIII.

Do zapoznania się z niniejszym dokumentem oraz stosowania zawartych w nim zasad zobowiązani są wszyscy pracownicy CAL upoważnieni do przetwarzania danych osobowych.