Załącznik nr 4
do Uchwały Zarządu
Fundacji 2xKochaj 25 maja 2018r. 2018r

Instrukcje
Polityki Bezpieczeństwa Informacji
w Fundacji 2xKochaj

Mysłowice, 2018 rok

SPIS TREŚCI

PREAMBUŁA

Zarząd Fundacji 2xKochaj, świadomy wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych powierzających Fundacji swoje dane osobowe do właściwej i skutecznej ochrony tych danych deklaruje zamiar: podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych, stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Fundacji w zakresie problematyki bezpieczeństwa tych danych, w tym propagowania świadomości wartości powierzonych Fundacji danych osobowych jako czynnika wpływającego na jakość i ciągłość działalności oraz wiarygodność jednostki, traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby, doskonalenia i rozwijania nowoczesnych metod zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem, szczególnie w zakresie dotyczącym dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych

CZĘŚĆ I
IINSTRUKCJA OCHRONY DANYCH OSOBOWYCH

ROZDZIAŁ I
Przepisy ogólne, definicje i objaśnienia

§ 1

1. Polityka Bezpieczeństwa Informacji Fundacji 2xKochaj jest zbiorem zasad i procedur obowiązujących przy zbieraniu, przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich danych osobowych administrowanych przez Fundacje.
2. Przetwarzanie danych osobowych w Fundacji 2xKochaj jest dopuszczalne tylko pod warunkiem przestrzegania Ustawy i wydanych na jej podstawie przepisów wykonawczych, a także przepisów wdrożonych w instrukcjach.

§ 2

Ilekroć w Instrukcji jest mowa o :

1. Administratorze Danych Osobowych – rozumie się przez to Fundacje 2xKochaj, reprezentowaną przez Zarząd Fundacji, zwany dalej ADO.
2. Administratorze Bezpieczeństwa Informacji – rozumie się przez to osobę wyznaczoną przez Zarząd Fundacji 2xKochaj, odpowiedzialną za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, zwaną dalej ABI.
3. Administratorze Systemów Informatycznych – rozumie się przez to osobę wyznaczoną przez Zarząd Fundacji 2xKochaj, odpowiedzialną za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych przetwarzających zbiory danych osobowych, zwaną dalej ASI.
4. Użytkowniku systemu – rozumie się przez to osobę posiadającą upoważnienie wydane przez Administratora Bezpieczeństwa Informacji lub uprawnioną przez niego osobę i dopuszczoną jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu, zwaną dalej Użytkownikiem.
5. Zbiorze danych osobowych – rozumie się przez to każdy posiadający strukturę zestaw danych, o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie

od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

6. Danych osobowych – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
7. Przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
8. Systemie informatycznym – jest to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.
9. Usuwaniu danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

§ 3

Do realizacji wytycznych Instrukcji powołujemy i czynimy odpowiedzialnym:

1. Administratora Bezpieczeństwa Informacji (ABI), do którego zadań w szczególności należy:

a) Występowania do Administratora Danych Osobowych o powołanie oraz odwołanie osób dopuszczonych do pracy w systemie oraz określanie zakresu ich szkolenia w obrębie niniejszej Instrukcji.

b) Weryfikowania opracowań stworzonych i przedłożonych przez Administratora Systemu Informatycznego w wypadku konieczności weryfikacji i modyfikacji Instrukcji Zarządzania Systemem Informatycznym.

c) Kontroli działań prowadzonych przez Administratora Systemu Informatycznego oraz pozostałych upoważnionych do przetwarzania danych osobowych pracowników.

d) W porozumieniu z Administratorem Danych Osobowych formalnego inicjowania kontroli systemu informatycznego.

e) Prowadzenie ewidencji wydanych upoważnień i oświadczeń.

f) Szkolenie pracowników z zakresu ochrony danych oraz informowanie użytkowników o zmianach w systemie ochrony danych osobowych.

2. Administratora Danych Osobowych (ADO), który:

a) określa zakres przetwarzanych danych osobowych w wydawanych regulaminach.

b) prowadzi dokumentację opisująca sposób przetwarzania danych osobowych.

c) zobowiązany jest stosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednia do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostepnieniem osobom nieupoważniony, utrata, uszkodzeniem lub zniszczeniem.

d) zobowiązany jest zapewnić ochronę przetwarzanych danych osobowych, określa cel, środki i sposoby przetwarzania danych

§ 4

Administratorem Bezpieczeństwa Informacji jest osoba powołana przez Zarząd Fundacji 2xKochaj.

§ 5

1. Dostęp do zbioru danych osobowych oraz ich przetwarzania mają tylko osoby wpisane do rejestru prowadzonego przez Administratora Bezpieczeństwa Informacji **(załącznik nr 1).**
2. Użytkownicy systemu zaangażowani w proces przetwarzania danych osobowych są zobowiązani do przechowywania danych osobowych we właściwych zbiorach, nie dłużej niż jest to niezbędne dla osiągnięcia celu ich przetwarzania.
3. Użytkownicy systemu zaangażowani w proces przetwarzania danych osobowych w systemach informatycznych są zobowiązani do postepowania zgodnie z „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”
4. Osoby przetwarzające dane są zobowiązane powiadomić Administratora Bezpieczeństwa Informacji o ewentualnych incydentach/naruszeniach bezpieczeństwa systemu ochrony danych osobowych we wszystkich zbiorach.
5. Tryb postępowania określa „Instrukcja postępowania w sytuacji uszkodzenia systemu lub naruszenia bezpieczeństwa danych osobowych w Fundacji 2xKochaj”. **(załącznik nr 2).**

§ 6

Zabrania się przetwarzania danych ujawniających:

- pochodzenie rasowe lub etniczne;

- poglądy polityczne;

- przekonania religijne lub filozoficzne;

- przynależność wyznaniową;
- przynależność partyjną lub związkową;
- stan zdrowia, nałogi;
- orientację seksualną

chyba, że pozwalają na to obowiązujące przepisy prawa lub osoba, której powyższe dane dotyczą wyraziła pisemną zgodę.

§ 7

Pracownik/współpracownik/wolontariusz, który:
1) Przetwarza w zbiorze danych:
   a) dane osobowe, do których przetwarzania nie jest upoważniony;
   b) dane osobowe, których przetwarzanie jest zabronione;
   c) dane osobowe niezgodne z celem stworzenia zbioru danych;
2) Udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym
3) Nie zgłasza Administratorowi Bezpieczeństwa Informacji zbiorów danych podlegających rejestracji.
4) Nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach.
5) Uniemożliwia osobie której dane dotyczą, korzystanie z przysługujących jej praw
- podlega odpowiedzialności karnej zgodnie z Ustawą z dnia 29 sierpnia 1997 r o ochronie danych osobowych oraz przepisami Kodeksu Pracy.

ROZDZIAŁ II

Gromadzenie danych osobowych

§ 1

Dane osobowe przetwarzane w Fundacji 2xKochaj mogą być uzyskiwane:
1) bezpośrednio od osób, których te dane dotyczą;
2) z innych źródeł, w granicach dozwolonych przepisami prawa.

§ 2

Zbierane dane osobowe muszą być wykorzystane tylko do celów, w jakich są lub będą przetwarzane. Po wykorzystaniu danych osobowych, powinny być one przechowywane w

sposób i przez okres wskazany w Instrukcji kancelaryjnej oraz w Instrukcji archiwizacyjnej.

§ 3

1. Pracownicy/współpracownicy/wolontariusze Fundacji 2xKochaj zbierający i przetwarzający dane osobowe są odpowiedzialni za poinformowanie osób, których dane przetwarzają o adresie siedziby, gdzie są zbierane i przetwarzane, celu zbierania danych, dobrowolności lub obowiązku podania danych, a jeżeli obowiązek istnieje, o jego podstawie prawnej, prawie dostępu do treści swoich danych oraz ich kontrolowania.
2. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, osobę której dotyczą należy poinformować ponadto o :
    1) źródle danych;
    2) uprawnieniach wynikających z art. 32 ust. 1 pkt. 7 i 8 Ustawy o ochronie danych osobowych.

ROZDZIAŁ III
Udzielanie informacji o przetwarzaniu danych osobowych

§ 1

1. Osobom, których dane przetwarza się w zbiorze danych, przysługuje prawo kontroli ich danych osobowych, a w szczególności prawo uzyskania wyczerpujących informacji na temat tych danych.
2. Każda osoba, która wystąpi z wnioskiem o otrzymanie informacji musi otrzymać odpowiedź na piśmie w terminie nie przekraczającym 30 dni od daty wpłynięcia wniosku **(załącznik nr 3).**

§ 2

W przypadku gdy dane osoby są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy, albo są zbędne do realizacji celu, dla którego zostały zebrane, pracownicy i współpracownicy zobowiązani są do ich uzupełnienia, uaktualnienia lub sprostowania.

ROZDZIAŁ IV
Rejestracja zbioru danych osobowych
oraz ochrona przetwarzania danych osobowych

§ 1

1. Pracownicy/współpracownicy/wolontariusze, którzy przetwarzają dane osobowe, zobowiązani są do zgłoszenia Administratorowi Bezpieczeństwa Informacji:

1) Planowanego rejestrowania nowych zbiorów danych osobowych

2) Wnoszenia zmian do zbiorów już zarejestrowanych.

§ 2

Administrator Danych Osobowych zobowiązany jest do stosowania środków organizacyjnych i technicznych, zapewniających ochronę przetwarzania danych, w szczególności przed ich udostepnieniem, kradzieżą, uszkodzeniem lub zniszczeniem przez osoby nieupoważnione.

§ 3

1. Administrator Bezpieczeństwa Informacji wydaje i przechowuje indywidualnie upoważnienia **(załącznik nr 4)** osobom przetwarzającym dane osobowe.
2. ABI zobowiązany jest do prowadzenia rejestru osób zatrudnionych przy przetwarzaniu danych **(załącznik nr 1)**, prowadzenia ewidencji oświadczeń o zachowaniu tajemnicy osób obecnie zatrudnionych na podstawie umowy zlecenia, o dzieło i innej umowy cywilnej oraz żądania ich przy nowo zawieranych umowach **(załącznik nr 5).**
3. Administrator Bezpieczeństwa Informacji zapewnia przeszkolenie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami dotyczącymi ochrony danych osobowych w Fundacji 2xKochaj (**załącznik nr 6).**

§ 4

1. W celu realizacji powierzonych zadań Administrator Bezpieczeństwa Informacji ma prawo:

1) kontrolować siedzibę Fundacji w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe.

2) informować Zarząd Fundacji 2xKochaj o przypadkach naruszenia bezpieczeństwa danych osobowych.

3) żądania od wszystkich pracowników/współpracowników/wolontariuszy wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych.

ROZDZIAŁ V
Zasady udostępniania danych osobowych

§ 1

Fundacja 2xKochaj udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

§ 2

1. Zbiory danych udostępnia się na pisemny, umotywowany wniosek, chyba, że odrębne przepisy prawa stanowią inaczej.
2. Wniosek powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.
3. Wniosek jest rozpatrywany przez wyznaczonego przez Zarząd Fundacji pracownika, którzy jednocześnie prowadzi ich ewidencję.
4. Decyzje w sprawie udostępnienia podejmuje Zarząd Fundacji.

§ 3

Fundacja 2xKochaj może odmówić udostępniania danych osobowych, jeżeli spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą lub innych osób.

CZĘŚĆ II

INSTRUKCJA

ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

SŁUŻĄCYM DO PRZETWARANIA DANYCH OSOBOWYCH

ROZDZIAŁ I

Podstawowe definicje, przedmiot

§ 1

Ilekroć w Instrukcji jest mowa o:

systemie informatycznym – należy przez to rozumieć zespół środków technicznych tzn. urządzenia komputerowe wraz z okablowaniem i oprogramowaniem, którego funkcją jest przetwarzanie danych.

systemie operacyjnym – należy przez to rozumieć szczególny rodzaj programu, którego zadaniem jest koordynowanie pracy wszystkich urządzeń wchodzących w skład komputera i zainstalowanych na komputerze programów. To właśnie system operacyjny uruchamia się jako pierwszy program po włączeniu komputera.

danych – należy przez to rozumieć każdą informację (tekst, cyfry, wykres, rysunek, dźwięk, animacja itp.), która może być przetworzona;

przetwarzaniu danych – należy przez to rozumieć jakiekolwiek operacje wykonywane na danych osobowych;

użytkowniku – należy przez to rozumieć każdą osobę, której przydzielono uprawnienia pozwalające na korzystanie z systemu informatycznego i przetwarzanie danych w nim zawartych w określonym przez te uprawnienia zakresie oraz zapewniono fizyczny dostęp do systemu;

Administratorze Systemu Informatycznego (ASI) – rozumie się przez to osobę wyznaczoną przez Zarząd Fundacji 2xKochaj, odpowiedzialną za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych przetwarzających zbiory danych osobowych, zwaną dalej ASI.

Nośniki danych – rozumie się przez to przedmiot umożliwiający fizyczne zapisanie danego rodzaju informacji, z którego możliwe jest późniejsze odczytanie tej informacji (np. płyta CD,

płyta DVD, dysk przenośny).

§ 2

Niniejsza Instrukcja:
1) reguluje zasady zarządzania zabezpieczeniem systemów informatycznych, wykorzystywanych do zbierania, ochrony, przetwarzania i archiwizowania danych osobowych w Fundacji 2xKochaj;
2) określa zasady pracy w każdym systemie informatycznym służącym do przetwarzania danych osobowych.
3) reguluje zagadnienia:
a) zasad eksploatacji systemów informatycznych,
b) bezpieczeństwa systemów informatycznych,
c) zasad dostępu do systemu informatycznego,
d) procedury rozpoczęcia i zakończenia pracy w systemie informatycznym,
e) zasad tworzenia i przechowywania kopii awaryjnych,
f) zabezpieczenia antywirusowego systemu informatycznego,
g) zasad postępowania z nośnikami informacji,
h) zasad komunikowania w sieciach komputerowych,
i) zasad monitorowania, przeglądu i konserwacji systemów informatycznych,
j) zasad dokonywania zmian w systemach informatycznych,
k) odpowiedzialności i obowiązków użytkowników systemu informatycznego.

§ 3

Niniejsza Instrukcja ma status dokumentu przeznaczonego do użytku wewnętrznego i może być udostępniona osobom upoważnionym (lub określonym) przez Zarząd Fundacji.

§ 4

Administrator Danych Osobowych powołuje na Administratora Systemu Informatycznego (ASI) pracownika/współpracownika/wolontariusza Fundacji 2xKochaj

§ 5

Do podstawowych obowiązków ASI należy:

1) Wykonywanie czynności wynikających z niniejszej Instrukcji w zakresie zabezpieczenia prawidłowego i bezpiecznego funkcjonowania bazy technicznej i oprogramowania systemu.
2) Wykonywanie czynności wynikających z niniejszej instrukcji, związanych z zapewnieniem bezpieczeństwa systemu, w tym:

a) Wprowadzanie lub usuwanie prawa dostępu do systemu informatycznego dla poszczególnych pracowników/współpracowników/wolontariuszy na wniosek ADO.

b) Opracowanie systemu haseł do poszczególnych obszarów systemu.

c) Zapewnienie konfiguracji systemu uniemożliwiającej wprowadzanie lub uzyskiwanie danych z systemu przez niepowołane osoby.

d) Przeprowadzanie kontroli systemu informatycznego na wniosek ABI.

e) Opracowywanie harmonogramu szkoleń z zakresu systemu oraz urządzeń dla Użytkowników systemu – ze szczególną dbałością o wiedzę z zakresu bezpieczeństwa systemów

f) Prowadzenie rzetelnej dokumentacji systemu i czuwanie nad prawidłowością sporządzania tej dokumentacji przez inne osoby.

g) Prowadzenie oraz uaktualnianie wykazu programów zastosowanych do przetwarzania danych osobowych w Fundacji wraz ze wskazaniem zakresu zbiorów danych osobowych w nich przetwarzanych **(załącznik nr 2).**

§ 6

Wszystkie osoby zatrudnione przy przetwarzaniu danych osobowych w systemie informatycznym w Fundacji 2xKochaj bez względu na zajmowane stanowisko i miejsce pracy oraz charakter stosunku pacy są zobowiązane do postepowania zgodnie z zasadami określonymi w niniejszej instrukcji.

§ 7

Za tworzenie, wdrażanie, administrację i interpretację polityki bezpieczeństwa informacji, standardów, zaleceń i procedur w całym systemie informatycznym w Fundacji 2xKochaj odpowiedzialny jest Administrator Danych Osobowych.

§ 8

Polecenia osób wyznaczonych przez Zarząd Fundacji 2xKochaj do realizacji zadań w zakresie ochrony informacji i bezpieczeństwa systemu informatycznego (ASI oraz ABI) muszą być bezwzględnie wykonywane przez wszystkich użytkowników systemu.

ROZDZIAŁ II

Ogólne zasady eksploatacji systemów informatycznych

§ 1

System informatyczny w Fundacji 2xKochaj może być używany tylko na potrzeby działania Fundacji 2xKochaj.

§ 2

Systemy sieciowe stosowane w systemie informatycznym w Fundacji 2xKochaj muszą wykorzystywać oprogramowanie ograniczające dostęp do plików dla każdego użytkownika osobno, rejestrujące aktywność każdego użytkownika i przyznające Administratorowi Systemu Informatycznego specjalne uprawnienia.

§ 3

Wszystkie stacje robocze pracujące w systemie informatycznym w Fundacji Rozwoju 2xKochaj muszą być zgodne ze sprzętową oraz programową konfiguracją zalecaną przez ASI.

§ 4

Systemy sieciowe stosowane w systemie informatycznym w Fundacji 2xKochaj muszą wykorzystywać oprogramowanie ograniczające dostęp do plików dla każdego użytkownika osobno, rejestrujące aktywność każdego użytkownika i przyznające Administratorowi Systemu Informatycznego specjalne uprawnienia.

§ 5

1. Stacje robocze działające w systemie informatycznym muszą mieć możliwość blokowania dostępu do tego systemu oraz możliwość zastosowania zabezpieczonego hasłem wygaszacza ekranu automatycznie uruchamianego po określonym czasie braku aktywności użytkownika.
2. Powyższe zasady odnoszą się również do komputerów przenośnych zawierających dane z systemu informatycznego w Fundacji 2xKochaj, jak również do wykorzystywanych w tym systemie urządzeń.

§ 6

Zasady określone w niniejszej instrukcji odnoszą się również do przetwarzania danych osobowych w komputerach przenośnych, w których za bezpieczeństwo danych w całości odpowiada użytkownik urządzenia.

ROZDZIAŁ III

Zabezpieczenia systemów informatycznych

Postanowienia ogólne

§ 1

1. Zabrania się testowania i podejmowania prób poznania metod zabezpieczenia systemu

informatycznego w Fundacji 2xKochaj przez pracowników/współpracowników/ wolontariuszy, dopóki nie otrzymają specjalnego upoważnienia na piśmie podpisanego przez Administratora Bezpieczeństwa Informacji.

2. Próby obejścia zabezpieczeń, które w dowolny sposób dotyczą bezpieczeństwa systemów są całkowicie zabronione.

Ochrona pomieszczeń

§ 2

1. Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe w Fundacji 2xKochaj stanowi **załącznik nr 1** do niniejszej Instrukcji.

§ 3

1. W pomieszczeniach, gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych z systemu informatycznego w Fundacji 2xKochaj powinny być ustawione w sposób uniemożliwiający tym osobom wgląd w dane.
2. Przebywanie w pomieszczeniach, o których mowa w ust. 1 osób nieuprawnionych do dostępu do danego systemu informatycznego jest możliwe tylko w obecności użytkownika uprawnionego do korzystania ze sprzętu informatycznego znajdującego się w danym pomieszczeniu.

§ 4

Przez naruszenie pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe w Fundacji 2xKochaj systemu rozumie się:

1) Włamanie do tych pomieszczeń,

2) Stwierdzenie braku urządzeń systemu.

§ 5

W wypadku stwierdzenia przez kogokolwiek naruszenia pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe należy:

1) powiadomić ABI

2) powiadomić ASI.

§ 6

Zasady i sposób przechowywania kluczy do pomieszczeń, w których znajduje się sprzęt komputerowy określa Zarząd Fundacji 2xKochaj .

ROZDZIAŁ IV

Ochrona i znaczenie sprzętu komputerowego

§ 1

1. Sprzęt komputerowy używany w systemie informatycznym w 2xKochaj powinien być fizycznie chroniony przed kradzieżą, zniszczeniem lub niewłaściwym używaniem.
2. Użytkownicy nie mogą sami demontować komputerów oraz dokonywać jakiejkolwiek zmiany komponentów sprzętu komputerowego. Wykonują to tylko uprawnione osoby.

§ 2

Sprzęt komputerowy używany w systemie informatycznym w Fundacji 2xKochaj nie może być przenoszony bez zgody ABI.

§ 3

1. Każde urządzenie w systemie informatycznym Fundacji 2xKochaj musi być oznaczone w celu jego identyfikacji.
2. Oznaczenia sprzętu dokonuje ABI.
3. Inwentaryzacji sprzętu dokonuje Komisja Inwentaryzacyjna, powołana przez Zarząd Fundacji 2xKochaj.

ROZDZIAŁ V

Zabezpieczenie oprogramowania

§ 1

1. Oprogramowanie używane w systemie informatycznym w Fundacji 2xKochaj musi być chronione przed jakąkolwiek niekontrolowaną modyfikacją, nieautoryzowanym usunięciem oraz kopiowaniem.
2. Przed jakimkolwiek zainstalowaniem nowego oprogramowania należy sprawdzić jego działanie pod kątem bezpieczeństwa całego systemu.

§ 2

1. W systemie informatycznym w Fundacji 2xKochajmoże być używane wyłącznie oprogramowanie licencjonowane przez posiadacza praw autorskich.
2. Oprogramowanie może być używane tylko zgodnie z prawami licencji.

Dostęp Użytkowników do systemu informatycznego

§ 3

1. Każdy Użytkownik systemu musi posiadać indywidualne hasło dostępu do systemu.
2. Nowy Użytkownik w systemie informatycznym jest wprowadzany do systemu po:

a) upoważnieniu przez ABI,
b) po podpisaniu oświadczenia o znajomości przepisów dot. niniejszej instrukcji oraz przepisów dot. ochrony danych osobowych.
3. Przy wprowadzaniu nowego użytkownika do system informatycznego, ASI konfiguruje jego konto, nadając mu uprawnienia do pracy w systemie operacyjnym.

§ 4

1. Natychmiast po utracie praw dostępu, będącej wynikiem zmiany stanowiska pracy lub zwolnienia z pracy, Członek Zarządu wnioskuje do ABI o zmianę uprawnień użytkownika lub zlikwidowanie dostępu**.**
2. Członek Zarządu powinien poinformować ABI, w przypadku złożenia przez osobę dopuszczoną do przetwarzania danych osobowych w systemie informatycznym, deklaracji o zamiarze zmiany stanowiska pracy.

Identyfikatory użytkowników i hasła dostępu

§ 5

1**.** Dostęp do systemu chroniony jest przez identyfikator i hasło użytkownika.

2. Identyfikator nadawany jest przez ASI.

3. Hasło dostępu do systemu komputerowego tworzone jest przez użytkownika i stanowi tajemnicę znana wyłącznie temu użytkownikowi.

4. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego przechowywanie.

5. Rejestr identyfikatorów prowadzi ABI.

§ 6

1. Hasła nie mogą być przechowywane w formie jawnej ani w postaci elektronicznej, ani w postaci tradycyjnej, w miejscach gdzie osoby trzecie mogą je odczytać.
2. Hasła muszą zostać zmienione, jeśli istnieje przypuszczenie, że znajdują się w posiadaniu osób trzecich.

§ 7

1. Hasła dostępu do systemów informatycznych powinny być zmienianie zgodnie z ustaleniami ABI.

2. Zmiana powinna być wymuszona w sposób automatyczny przez odpowiednie

oprogramowanie nie rzadziej niż co 30 dni.

§ 8

1. Użytkownicy nie mogą mieć możliwości logowania się do systemu informatycznego lub sieci komputerowej w sposób anonimowy.
2. Proces logowania się do systemu informatycznego w musi przebiegać za pomocą wyświetlanego przez system okna logowania.

Zabezpieczenie antywirusowe

§ 9

1. System informatyczny należy kontrolować pod kątem obecności wirusów

§ 10

Program antywirusowy i konfiguracja systemu musi zapewniać kontrolę całego systemu:

a) na bieżąco
b) przynajmniej raz dziennie, jeżeli z przyczyn technicznych nie można wykonywać jej na bieżąco.
c) każdorazowo, przy korzystaniu z nośników wymienianych.

§ 11

1.Po zasygnalizowaniu przez program antywirusowy wystąpienia wirusa, użytkownik systemu powinien natychmiast powiadomić ASI, który podejmuje odpowiednie kroki:

a) identyfikuje wirus i określa obszar jego działania;
b) odseparowuje część systemu objętą wirusem od całości sieci;
c) w razie konieczności przerywa pracę systemu, przystąpić do usuwania wirusa, zgodnie z wymogami stosowanego programu antywirusowego;
d) w razie konieczności, należy ponownie wgrać system i dane systemu z ostatnich aktualnych kopii systemu, przetestować sprawność systemu i ponownie wykonać wszystkie operacje z bieżącego dnia.

§ 12

Ponowne uruchomienie systemu do pracy może nastąpić jedynie na polecenie ABI lub ASI.

Rozpoczęcie i zakończenie pracy w systemach informatycznych

§ 13

Przed przystąpieniem do pracy w systemie informatycznym w Fundacji 2xKochaj, każdy użytkownik powinien upewnić się, że spełnione są podstawowe warunki bezpieczeństwa wymagane przy przetwarzaniu danych w systemie informatycznym w Fundacji, a w szczególności:

1) jeśli w pomieszczeniu przebywają osoby postronne, monitor stanowiska dostępu do danych z systemu informatycznego ustawiony jest w sposób uniemożliwiający tym osobom wgląd w dane.

§ 14

Na pracę użytkowników systemu, poza godzinami pracy Fundacji, musi wyrazić zgodę Zarząd Fundacji 2xKochaj.

§ 15

Po zakończeniu pracy w systemie informatycznym, użytkownik obowiązany jest wylogować się z tego systemu.

Kopie zapasowe

§ 16

1. Ze względu na bezpieczeństwo wprowadza się obowiązek sporządzana kopii awaryjnych oprogramowania systemowego oraz danych.
2. Kopie awaryjne mogą być użyte jedynie dla odbudowy systemu uszkodzonego wskutek ataku wirusa, awarii twardego dysku lub innych problemów.
3. Kopie awaryjne oprogramowania systemowego powinny być sporządzane zgodnie z zaleceniami ASI oraz po każdej modyfikacji.
4. Za systematyczne przygotowywanie kopii bezpieczeństwa odpowiada ASI.

ROZDZIAŁ VI

Nośniki danych i komputery przenośne

§ 1

1. Użytkownicy nie mogą kopiować oprogramowania, informacji o wysokim stopniu ważności, należących do Fundacji 2xKochaj na jakiekolwiek nośniki danych, przenosić tego oprogramowania na inne komputery lub udostępniać je osobom trzecim.
2. Uprawnionym do powyższych czynności jest jedynie ABI.

§ 2

1. Rejestr wydanych komputerowych nośników danych i komputerów przenośnych prowadzony jest przez ABI **(załącznik nr 4).**
2. Za pobrany nośnik danych i komputer przenośny oraz bezpieczeństwo zapisanych na nich danych odpowiada użytkownik, który pobrał dany nośnik i posiada go na swoim stanie.

§ 3

Nośniki danych i komputery przenośne w Fundacji powinny być po zakończeniu pracy przechowywane w sposób zapewniający bezpieczeństwo zapisanych na nich danych.

§ 4

1. Sprzęt nie może być wykorzystywany poza siedzibą Fundacji, chyba że za zgodą ABI.
2. Korzystając ze sprzętu poza siedzibą Fundacji należy zachować szczególną dbałość o jego bezpieczeństwo.

§ 5

1. Nośniki przenośne mogą być podłączane do systemu jedynie na komputerach zapewniających ochronę przed złośliwym oprogramowaniem.

Sposoby i czas przechowywania wydruków

§ 6

1. Nie należy magazynować zbędnych wydruków.
2. Po upływie okresu przechowywania muszą one być fizycznie zniszczone w sposób uniemożliwiający odtworzenie informacji.

3. Za zniszczenie zbędnych wydruków i innych dokumentów zawierających dane osobowe odpowiedzialni są pracownicy komórek organizacyjnych.
4. Wydruki muszą być przechowywane w pomieszczeniach, uniemożliwiających dostęp do nich przez osoby niepowołane.

Monitorowanie, przegląd i konserwacja systemów informatycznych

§ 7

Zabronione jest dokonywanie napraw sprzętu komputerowego samodzielnie przez pracowników bez zgody ASI.

§ 8

1. Poszczególne systemy informatyczne muszą w sposób bezpieczny prowadzić zapis wszystkich znaczących zdarzeń systemowych, mających wpływ na bezpieczeństwo przetwarzanych w nich danych osobowych a w szczególności:

1) Prób odgadywania haseł;
2) Prób wykorzystania uprawnień, do których użytkownik nie uzyskał autoryzacji
3) Modyfikacji oprogramowania;
4) Zmian uprawnień użytkowników;
5) Prób ingerencji w systemowe rejestry zdarzeń.

2. Rejestry zdarzeń systemowych związanych z bezpieczeństwem systemów informatycznych muszą być przechowywane przez okres co najmniej 1 roku.
3. Podczas tego okresu muszą być zabezpieczone w taki sposób aby nie była możliwa ich modyfikacja oraz aby były one dostępne jedynie dla autoryzowanych użytkowników.

§ 9

1. Ze względu na bezpieczeństwo wprowadza się następujące dokumenty:

1) Inwentaryzacji zbiorów danych, które stanowi załącznik numer 1 do uchwały zarządu z dnia 25 maja 2018r.
2) Analizy ryzyka, które stanowi załącznik nr 2 do uchwały zarządu z dnia 25 maja 2018r.
3) Rejestr czynności przetwarzania danych, który stanowi załącznik nr 3 do uchwały zarządu z dnia 25 maja 2018r.

Zmiany w systemach informatycznych

§ 9

1. Wszystkie zmiany dotyczące sieci komputerowych w Fundacji 2xKochaj powinny być udokumentowane w takim porządku w jakim zostały przeprowadzone, zaakceptowane przez ASI.
2. Zmiany w systemie informatycznym mogą być dokonywane wyłącznie przez ASI.
3. Nie wolno zestawiać nowych połączeń między komputerami w systemie informatycznym w Fundacji, chyba że zostanie udzielone pozwolenie przez ASI.

ROZDZIAŁ VII

Odpowiedzialność użytkowników systemu informatycznego.

§ 1

1. Użytkownicy odpowiedzialni są za wypełnianie wszystkich postanowień dot. bezpieczeństwa informacji w systemie informatycznym w Fundacji 2xKochaj .
2. Zarząd Fundacji odpowiedzialny jest za bieżące przestrzeganie zasad ustalonych w instrukcjach ochrony danych osobowych oraz zasad użytkowania urządzeń i systemów informatycznych w Fundacji.

Sankcje

§ 2

1. Nieprzestrzeganie postanowień niniejszej instrukcji oraz brak nadzoru nad bezpieczeństwem informacji stanowi naruszenie obowiązków pracowniczych i może być przyczyna odpowiedzialności dyscyplinarnej określonej przepisami Kodeksu Pracy.
2. Jeżeli skutkiem działania użytkownika jest ujawnienie informacji osobie nieupoważnionej, osoba ta może być pociągnięta do odpowiedzialności karnej określonej przepisami Kodeksu Karnego.