Polityka Bezpieczeństwa
Instytutu Chemii Fizycznej
Polskiej Akademii Nauk

Zatwierdził:

Prof. dr hab. Marcin Opałło

Warszawa 2015

Spis treści

1. CEL POLITYKI BEZPIECZEŃSTWA

Niniejszy dokument określa zasady bezpieczeństwa przetwarzania danych osobowych jakie powinny być przestrzegane i stosowane w Instytucie Chemii Fizycznej Polskiej Akademii Nauk zwany dalej ICHF PAN, przez pracowników i współpracowników, którzy przetwarzają dane osobowe.

Stosowanie zasad określonych w niniejszym dokumencie ma na celu zapewnienie prawidłowej ochrony danych osobowych przetwarzanych przez Instytut Chemii Fizycznej rozumianej jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.

2. ŹRÓDŁA WYMAGAŃ

Polityka Bezpieczeństwa Instytutu Chemii Fizycznej Polskiej Akademii Nauk, dalej zwana POLITYKĄ została utworzona na podstawie rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. 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. Nr 100, poz. 1024) oraz zgodnie z :

- Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 1997 r. Nr 133 poz. 883 z późn. zm.) dalej zwana USTAWĄ
- Wytycznymi w zakresie opracowania i wdrożenia polityki bezpieczeństwa- Generalny Inspektor Ochrony Danych Osobowych dalej zwany GiODO

3. ZAKRES STOSOWANIA

Politykę stosuje w celu zabezpieczenia danych osobowych przetwarzanych tradycyjnie w wersji papierowej, na stacjonarnych i przenośnych elektronicznych nośnikach informacji (pendrive, dyski zewnętrzne, płyty CD itp.) oraz w systemie informatycznym.

W zakresie podmiotowym, POLITYKA obowiązuje wszystkich pracowników[1] Instytutu Chemii Fizycznej Polskiej Akademii Nauk.

4. BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH

Przez bezpieczeństwo przetwarzania danych osobowych rozumie się zapewnienie:

- poufności- właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;
- integralności- właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- rozliczalności- właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

5. DEFINICJE

Dane osobowe (DO) - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, jeżeli jej tożsamość można określić bezpośrednio lub pośrednio (w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne).
Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań
Przetwarzanie danych osobowych – wszelkie operacje wykonane na danych osobowych takie jak:

- zbieranie;
- utrwalanie;
- przechowywanie;
- opracowywanie;
- zmienianie;
- udostępnianie;
- usuwanie

[1] Pracownik – osoba fizyczna zatrudniona na podstawie umowy o pracę/zlecenie/o dzieło, praktykanci, stażyści, wolontariusze, pracownicy firm zewnętrznych wykonujący pracę na rzecz ICHF.

Zbiór danych osobowych – każdy posiadający strukturę zestaw danych osobowych, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.

Administrator Danych (AD) – organ decydujący o celach i środkach przetwarzania danych osobowych, w przypadku niniejszej Polityki funkcję AD pełni ICHF PAN reprezentowany przez Dyrektora Instytutu.

Administrator Bezpieczeństwa Informacji (ABI) – osoba wyznaczona przez AD do realizacji zadań wynikających z art. 36a USTAWY.

Administrator Systemów Informatycznych (ASI) – osoba pełniąca obowiązki w zakresie konfiguracji stacji roboczych i serwerów w systemie informatycznym.

6. ODPOWIEDZIALNOŚĆ

Administrator Danych Osobowych

Do obowiązków Kierownictwa należy:

- podejmowanie odpowiednich i niezbędnych kroków mających na celu zapewnienie prawidłowej ochrony danych osobowych
- podział zadań i obowiązków związanych z organizacją ochrony danych osobowych, w szczególności wyznaczenie ABI
- wprowadzenie procedur zapewniających prawidłowe przetwarzanie danych osobowych;
- zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych przetwarzanych w określonym przez nich celu.
- zapewnienie niezbędnych środków potrzebnych do bezpiecznego przetwarzania danych osobowych.
- Upoważnianie i prowadzenie ewidencji pracowników upoważnionych do przetwarzania danych osobowych.
- Kontrola nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Administrator Bezpieczeństwa Informacji

Do obowiązków ABI należy nadzorowanie przestrzegania zasad ochrony danych osobowych oraz:

- określenie wymagań bezpieczeństwa przetwarzania danych osobowych;
- nadzór nad wdrożeniem stosowanych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzania danych osobowych;
- nadzorowanie dokumentacji opisującej zastosowaną politykę bezpieczeństwa przetwarzania danych osobowych (niniejsza Polityka oraz wynikające z niej instrukcje i procedury);
- dokonywanie okresowo, nie rzadziej niż raz na rok, sprawdzenia przetwarzania danych osobowych.
- Prowadzenie jawnego rejestru zbiorów danych przetwarzanych przez AD

Administrator Systemów Informatycznych

Administrator Danych może powołać Administratora Systemów Informatycznych. ASI odpowiedzialny jest za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych. Do obowiązków ASI w szczególności należy:

- nadawanie uprawnień dostępu do systemów informatycznych osobom upoważnionym do przetwarzania danych osobowych;
- prowadzenie ewidencji nadanych uprawnień;
- nadzór nad przestrzeganiem przepisów Instrukcji Zarządzania Systemami Informatycznymi.

Osoby upoważnione do przetwarzania danych osobowych

Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy znajomość i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do swojej stacji roboczej. Do obowiązków należy również:

- zapoznanie się z regulacjami wewnętrznymi dotyczącymi ochrony danych osobowych w ICHF PAN, w szczególności z Polityką oraz z Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
- przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami;
- przetwarzanie danych osobowych wyłącznie za pomocą autoryzowanych urządzeń służbowych.
- udzielanie wyczerpujących wyjaśnień ABI w toku prowadzonego przez niego sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

- zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczania, do których uzyskały dostęp w trakcie zatrudnienia, również po ustaniu zatrudnienia.
- Informowania o wszelkich podejrzenia naruszania lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe do ABI.

7. ZARZĄDZANIE BEZPIECZEŃSTWEM DANYCH OSOBOWYCH

Podstawowe zasady

- Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z obowiązkami służbowymi oraz rolą sprawowaną w procesie przetwarzania danych.
- Każda z osób mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich w granicach udzielonego jej upoważnienia;
- należy zapewnić poufność, integralność i rozliczalność przetwarzanych danych osobowych.
- Należy stosować adekwatny do zmieniających się warunków i technologii poziom bezpieczeństwa przetwarzania danych osobowych.

Procedury postępowania z danymi osobowymi

- dostęp do danych osobowych powinien być przyznawany zgodnie z zasadą wiedzy koniecznej;
- dane osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją;

Upoważnienie do przetwarzania danych osobowych

- Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez AD.
- Upoważnienia są wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych.
- Do przetwarzania danych osobowych może zostać dopuszczona wyłącznie osoba, która została przeszkolona przez ABI z przepisów dotyczących ochrony danych osobowych i podpisała oświadczenie stanowiące załącznik nr 1 do Polityki.
- Na podstawie podpisanego oświadczenia ABI wnioskuje od AD o nadanie Upoważnienia do przetwarzania danych osobowych, stanowiącego załącznik nr 2 do Polityki

- Upoważnienia, o których mowa powyżej przechowywane są w aktach osobowych pracownika i obowiązują do czasu ustania stosunku pracy lub cofnięcia upoważnienia do przetwarzania danych osobowych

Ewidencja osób upoważnionych

Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona przez ABI i zawiera w szczególności:

- imię i nazwisko osoby upoważnionej do przetwarzania danych osobowych;
- zakres upoważnienia do przetwarzania danych osobowych;
- identyfikator, jeżeli osoba upoważniona została zarejestrowana w systemie informatycznym, służącym do przetwarzania danych osobowych;
- datę nadania i ustania uprawnień.
- Zajmowane stanowisko

Przełożeni osób upoważnionych odpowiadają za natychmiastowe zgłoszenie do ABI osób, które utraciły uprawnienia dostępu do danych osobowych.

Zgodność

- Niniejsza Polityka powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi dotyczącymi ochronny danych osobowych oraz zmianami faktycznymi w ramach Instytutu Chemii Fizycznej Polskiej Akademii Nauk, które mogą powodować iż zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.
- Zmiany niniejszej Polityki wymagają przeglądu innych dokumentów dotyczących ochrony danych osobowych obowiązujących w Instytucie Chemii Fizycznej Polskiej Akademii Nauk.

8. ZARZĄDZANIE USŁUGAMI ZEWNĘTRZNYMI

Bezpieczeństwo usług zewnętrznych

- Należy zapewnić, aby usługi zewnętrzne były prowadzone wyłącznie zgodnie z wymaganiami bezpieczeństwa przetwarzania danych osobowych obowiązującymi w Instytucie Chemii Fizycznej Polskiej Akademii Nauk, wymaganiami umowy oraz wymaganiami prawa.

- Wymagania bezpieczeństwa przetwarzania danych osobowych, zakres usług oraz poziom ich dostarczania należy określić w umowie świadczenia usług.
- Należy zapewnić aby użytkownicy nie będący pracownikami Instytutu Chemii Fizycznej Polskiej Akademii Nauk posiadali Upoważnienie do przetwarzania danych osobowych nadanych przez AD i stosowali te same zasady bezpieczeństwa przetwarzania danych osobowych co użytkownicy będący pracownikami.

Powierzanie przetwarzania danych osobowych

- Powierzenie przetwarzania danych osobowych może mieć miejsce wyłącznie na podstawie pisemnej umowy określającej w szczególności zakres i cel przetwarzania danych. Umowa musi określać również zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie przetwarzanie danych z tytułu niewykonania lub nienależytego wykonania umowy.
- Powierzenie przetwarzania danych osobowych musi uwzględniać wymogi określone w art. 31 i nast. Ustawy. W szczególności podmiot zewnętrzny, któremu ma zostać powierzone przetwarzanie danych osobowych, jest obowiązany przed rozpoczęciem przetwarzania danych do podjęcia środków zabezpieczających zbiór danych, o których mowa w art. 36-39a Ustawy.
- W umowach stanowiących podstawę powierzenia przetwarzania danych, eksploatacji systemu informatycznego lub części infrastruktury należy umieścić zobowiązanie podmiotu zewnętrznego do przestrzegania niniejszej Polityki oraz zastosowania odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo i odpowiedni poziom ochrony danych.
- Powierzenie przetwarzania danych nie oznacza zwolnienia z odpowiedzialności Instytutu Chemii Fizycznej Polskiej Akademii Nauk za zgodne z prawem przetwarzanie powierzonych danych, co wymaga w umowach stanowiących podstawę powierzenia przetwarzania danych umieszczenia prawa Instytutu Chemii Fizycznej Polskiej Akademii Nauk do kontroli wykonania przedmiotu umowy w siedzibie pomiotu zewnętrznego m. in. w zakresie przestrzegania Polityki obowiązujących regulacji wewnętrznych, umów i właściwych przepisów prawa.

Udostępnianie danych osobowych

- Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dotyczą.
- Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą AD
- Informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru listem poleconym za pokwitowaniem odbioru lub innym bezpiecznym sposobem, określonym wymogiem prawnym lub umową.
- Udostępniając dane osobowe innym podmiotom należy odnotować informacje o udostępnieniu bezpośrednio w systemie informatycznym, z którego udostępniono dane lub w inny zatwierdzony sposób. Odnotować należy: informacje o odbiorcy danych, dacie i zakresie udostępnionych danych osobowych.
- Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

9. BEZPIECZEŃSTWO FIZYCZNE OBSZARÓW PRZETWARZANIA

Obszar przetwarzania

Dane osobowe mogą być przetwarzane wyłącznie w obszarach przetwarzania danych osobowych, na które składają się pomieszczenia biurowe oraz części pomieszczeń, gdzie Instytut Chemii Fizycznej Polskiej Akademii Nauk prowadzi działalność. Do takich pomieszczeń, zalicza się w szczególności:

- pomieszczenia biurowe, w których zlokalizowane są stacje robocze lub serwery służące do przetwarzania danych osobowych;
- pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego zawierające dane osobowe;
- pomieszczenia, w których przechowywane są sprawne i uszkodzone urządzenia, elektroniczne, wszelkie inne nośniki informacji oraz kopie zapasowe zawierające dane osobowe.
- Dopuszczalne jest przetwarzania danych osobowych poza pomieszczeniami biurowymi oraz częścią pomieszczeń, gdzie Instytut Chemii Fizycznej Polskiej Akademii Nauk prowadzi działalność, jeśli jest to uzasadnione charakterem czynności oraz każdorazowo zostało potwierdzone pisemnie przez Administratora Danych, bądź postanowieniami umowy o pracę oraz pod warunkiem właściwego zabezpieczenia przetwarzanych danych osobowych.

Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.

Osoby upoważnione zobowiązane są do zamykania na klucz wszelkich pomieszczeń wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu jak i po jej zakończeniu.
Zabronione jest pozostawianie kluczy w zamkach drzwi pomieszczeń w których przetwarzane są dane osobowe.
Wydruki i nośniki elektroniczne zawierające dane osobowe należy zabezpieczyć przed dostępem do nich osób nieupoważnionych.

Niepotrzebne wydruki lub inne dokumenty należy niszczyć za pomocą niszczarek.

Przebywanie wewnątrz obszarów przetwarzania danych osobowych osób nieuprawnionych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych.

Szczegółowy wykaz obszarów przetwarzania danych osobowych stanowi załącznik nr 4 do Polityki.

10. ZBIORY DANYCH OSOBOWYCH

Wykaz zbiorów danych osobowych i ich struktura zamieszczone są w załączniku nr 6:

Dane osobowe gromadzone we wskazanych zbiorach są przetwarzane w systemach informatycznych oraz w kartotekach ewidencyjnych, które są zlokalizowane w pomieszczeniach lub części pomieszczeń należących do obszaru przetwarzania danych osobowych.

Wskazane w załączniku nr 6 zakresy danych osobowych przetwarzanych w poszczególnych zbiorach danych osobowych są ustalone w oparciu o strukturę zbiorów danych osobowych prowadzonych w systemach informatycznych oraz powiązania pól informacyjnych utworzonych w tych systemach.

Zawartość pól informacyjnych, występujących w systemach zastosowanych w celu przetwarzania danych osobowych, musi być zgodna z przepisami prawa, które uprawniają Administratora danych do przetwarzania danych osobowych.

Sposób przepływu danych pomiędzy systemami:
- obieg dokumentów zawierających dane osobowe, pomiędzy komórkami organizacyjnymi Jednostki, winien odbywać się w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji)
- przekazywanie informacji (danych) w systemie informatycznym poza sieć lokalną Jednostki, w miarę możliwości, powinno odbywać się w sposób szyfrowany.

11. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANIA DANYCH

1. Ochrona pomieszczeń wykorzystanych do przetwarzania danych osobowych:
   1) budynki i wszystkie pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone są przed dostępem osób nieuprawnionych,
   2) dokumentacja papierowa po godzinach pracy jest przechowywana w zamkniętych pomieszczeniach.
   3) przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych jest dopuszczalne w obecności osoby upoważnionej do przetwarzania danych osobowych.
2. Przedsięwzięcia w zakresie zabezpieczenia sprzętu komputerowego:
   1) dla zapewnienia ciągłości działania systemów informatycznych służących do przetwarzania danych osobowych stosuje się w nich sprzęt oraz oprogramowanie wyprodukowane przez renomowanych producentów oraz zabezpiecza się sprzęt przed awarią zasilania lub zakłóceniami w sieci zasilającej,
   2) zbiory danych osobowych oraz programy służące do przetwarzania danych osobowych są zabezpieczane przed przypadkową utratą oraz celowym zniszczeniem poprzez wykonywanie kopii zapasowych**,**
   3) kopie zapasowe są usuwane niezwłocznie po ustaniu ich użyteczności.

3. Przedsięwzięcia w zakresie teletransmisji danych:

1) w celu ochrony systemów informatycznych służących do przetwarzania danych osobowych przed zagrożeniami pochodzącymi z Internetu stosuje się zabezpieczenia chroniące przed nieuprawnionym dostępem,

4. Przedsięwzięcia w zakresie środków ochrony w ramach oprogramowania systemów:

1) w celu zapewnienia rozliczalności operacji dokonywanych przez użytkowników systemu informatycznego, w systemie tym dla każdego użytkownika rejestrowany jest odrębny identyfikator i hasło,
2) w przypadku, gdy do uwierzytelnienia użytkowników używa się identyfikatora i hasła, składa się ono z co najmniej 8 znaków, w szczególności zawiera małe i duże litery, cyfry oraz znaki specjalne,
3) hasła służące do uwierzytelnienia w systemach informatycznych służących do przetwarzania danych osobowych są zmieniane co najmniej raz na 30 dni,
4) system informatyczny powinien wymuszać zmianę haseł, informując o upływie ich ważności,

5. Przedsięwzięcia w zakresie środków ochrony w ramach narzędzi baz danych i innych narzędzi programowych:

1) w celu ochrony zbiorów danych osobowych prowadzonych w systemach informatycznych przed nieuprawnionym dostępem stosuje się mechanizmy kontroli dostępu do tych danych,
2) system zapewnia automatyczne odnotowywanie w systemie informacji o identyfikatorze użytkownika, które wprowadził dane osobowe oraz dacie pierwszego wprowadzenia danych do systemu,
3) stosuje się oprogramowanie umożliwiające trwałe usunięcie danych osobowych z urządzeń, dysków, lub innych elektronicznych nośników informacji, które przeznaczone są do naprawy, przekazania lub likwidacji przez osobę nieuprawnioną.

6. Przedsięwzięcia w zakresie środków ochrony w ramach systemu użytkowego:

1) w celu ochrony danych osobowych przetwarzanych na stacjach roboczych na czas krótkotrwałego puszczenia stanowiska pracy przez użytkownika systemu, stosuje się mechanizm blokady stacji roboczej zabezpieczony hasłem,
2) stosuje się mechanizmy kontroli dostępu użytkowników do systemów- ogranicza się dostęp do katalogów, ogranicza się wykonywanie poleceń,

3) na stacjach roboczych użytkownicy nie posiadają uprawnień do instalowania nieautoryzowanego oprogramowania,
4) stosuje się oprogramowania antywirusowe z automatyczną aktualizacją w celu ochrony systemu przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
5) kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie jak i do celów instalacyjnych.

7. Przedsięwzięcia w zakresie środków organizacyjnych.
1) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,
2) dostęp do danych osobowych możliwy jest po uzyskaniu formalnego upoważnienia do przetwarzania danych osobowych wydanego przez upoważnione osoby,
3) wprowadzono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
4) monitoruje się wdrożone zabezpieczenia systemu informatycznego.

12. POSTANOWIENIA KOŃCOWE

W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (t.j. Dz. U. nr 133 poz. 883 z późn. zm.) oraz przepisy wykonawcze do tej Ustawy.

Pracownicy Instytutu Chemii Fizycznej Polskiej Akademii Nauk zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce, w wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących w Instytucie Chemii Fizycznej Polskiej Akademii Nauk, użytkownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.

13. ZAŁĄCZNIKI

Nr 1 Oświadczenie
Nr 2 Upoważnienie do przetwarzania danych osobowych
Nr 3 Odwołanie upoważnienia do przetwarzania danych osobowych
Nr 4 Ewidencja osób upoważnionych do przetwarzania danych osobowych
Nr 5 Lista oprogramowani służących do przetwarzania danych osobowych

Instrukcja Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych

§1

Postanowienia ogólne

1. Instrukcja reguluje zasady zarządzania systemem informatycznym do przetwarzania danych osobowych w Instytucie Chemii Fizycznej PAN.
2. Definicje i skróty:
   1) Definicje:
   a) przetwarzanie danych, system informatyczny, administrator danych użyto w rozumieniu nadanym art. 7 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych,
   b) zalogowanie się- oznacza- uwierzytelnienie- w rozumieniu §2 pkt. 11 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych

i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,

c) sieć publiczna- rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt. 22 Ustawy z dnia 21 lipca 2000r.- Prawo telekomunikacyjne.

2) Skróty:

a) ASI- administrator sieci informatycznej (osoba pełniąca obowiązki w zakresie konfiguracji stacji roboczych i serwerów w systemie informatycznym).

§2

Procedury nadawania i zmiany uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

1. Nadawanie uprawnień dostępu do systemu informatycznego przetwarzającego dane osobowe.
   1) Pracownik po uzyskaniu zgody przełożonego przekazuje wniosek o nadanie uprawnień dostępu do systemu informatycznego do ABI, który zajmuje się dalszą procedurą nadania uprawnień. Po uzyskaniu zgody od AD przekazuje decyzje pracownikowi.

2. Odebranie uprawnień dostępu do systemu informatycznego przetwarzającego dane osobowe. Odebranie uprawnień może nastąpić na wniosek przełożonego pracownika, kierownika kadr, ABI lub ASI.
   1) Przełożony pracownika lub kierownik działu spraw pracowniczych przekazuje wniosek o odebraniu uprawnień dostępu do systemu informatycznego do ABI.
   2) ABI odnotowuje datę odebrania uprawnień dostępu do systemu informatycznego w ewidencji osób dopuszczonych do przetwarzania danych osobowych.
   3) ASI na wniosek ABI w ciągu 2 godzin blokuje konto dostępu do systemu informatycznego i stacji roboczej.

§3

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. W systemie informatycznym w celu utrzymywania kontroli dostępu do danych stosuje się identyfikatory użytkowników i hasła na poziomie dostępu do stacji roboczej i aplikacji.

1) ASI jest odpowiedzialny za zarejestrowanie identyfikatora i wygenerowanie hasła tymczasowego do stacji roboczej. Identyfikator i hasło przekazuje pracownikowi osobiście, w sposób uniemożliwiający zapoznanie się z nim przez inne osoby.

2. Hasło służące do uwierzytelnienia pracowników składa się z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.

3. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.

4. Użytkownik ma obowiązek zmiany hasła nie rzadziej niż raz na 30 dni.

5. W przeciągu 6 miesięcy użytkownik nie może ponownie logować się do stacji roboczej, czy aplikacji za pomocą tego samego hasła.

6. Hasła nie mogą być zapisane i pozostawiane w miejscach gdzie osoby nieuprawnione mogą je odczytać.

7. Hasło nie może być ujawnione nawet po utracie przez nie ważności.

8. Wszystkie hasła muszą być natychmiast zmienione, jeśli istnieje podejrzenie, że zostały odkryte, lub wiadomo, że znajdują się w posiadaniu osoby innej niż autoryzowani użytkownicy.

§4

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1. Rozpoczynając pracę w systemie informatycznym użytkownik wprowadza identyfikator użytkownika i hasło (załogowanie się) do stacji roboczej, a następnie do aplikacji. Czynności te dokonuje w warunkach, które uniemożliwiają osobom trzecim zapoznanie się z hasłem.

2. Po zalogowaniu się do aplikacji użytkownik sprawdza ogólną poprawność działania systemu, zwracając w szczególności uwagę na:

1) wygląd aplikacji;
2) dostępność opcji, do korzystania z których użytkownik został upoważniony;
3) sposób działania aplikacji;
4) zakres danych i sposób ich przedstawienia.

3. Użytkownik powiadamia ASI o:

1) niemożliwości zalogowania się do aplikacji;
2) zmianie wyglądu aplikacji odmiennym od normalnego;
3) niedostępności opcji, do korzystania z których użytkownik został upoważniony;
4) dostępności opcji, do korzystania z których użytkownik nie został upoważniony;
5) zmianach sposobu działania aplikacji;

6) zmianach zakresu danych lub sposobu ich przedstawienia odbiegających od stanu normalnego;
7) innych zmianach działania aplikacji uzasadniających podejrzenie naruszenia danych osobowych.

4. Użytkownik powiadamia ASI o niemożliwości zalogowania się do stacji roboczej.

5. Oprogramowanie służące do przetwarzania danych osobowych użytkownik wykorzystuje zgodnie z jego przeznaczeniem oraz zachowuje szczególną ostrożność przy wprowadzaniu danych, aby były one poprawne i kompletne.

6. Przy każdorazowym opuszczeniu stanowiska komputerowego użytkownik ma obowiązek dopilnować, aby na ekranie nie były wyświetlane dane osobowe.

7. Przed opuszczeniem miejsca pracy na dłuższy czas blokuje system (wciskając klawisze Windows + L)

8. Kończąc pracę w systemie informatycznym użytkownik każdorazowo dokonuje wylogowania z aplikacji i stacji roboczej.

§5

Procedury tworzenia kopii zapasowych

1. Za tworzenie kopii zapasowych danych osobowych i programów służących do przetwarzania danych osobowych odpowiadają osoby wyznaczone przez kierownika jednostki organizacyjnej w której to przetwarzanie występuje.

2. Pełna kopia zapasowa danych osobowych sporządzana jest raz na dwa miesiące, natomiast kopia przyrostowa lub różnicowa (odpowiednio do charakteru zmian danych) sporządzana jest codziennie. Kopie wykonywane są w jednym egzemplarzu na nośniku optycznym, magnetycznym lub pamięci typu Flash w zależności od urządzeń archiwizujących dane znajdujących się w jednostce organizacyjnej.

3. Kopie różnicowe lub przyrostowe przechowywane są do czasu sporządzenia pełnej kopii zapasowej.

4. Pełna kopia zapasowa przechowywana jest przez okres minimum trzech miesięcy.

5. Kopia programu służącego do przetwarzania danych przechowywana jest do czasu sporządzania drugiej w kolejności pełnej kopii.

§6

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji oraz wydruków zawierających dane osobowe

1. Dane osobowe zapisane na urządzeniach, dyskach lub innych nośnikach elektronicznych nie mogą być wynoszone poza teren Instytutu.
2. Po zakończeniu pracy przenośne nośniki elektroniczne oraz wydruki z danymi osobowymi przechowywane są w zamkniętych pomieszczeniach.
3. W pomieszczeniach przeznaczonych do przechowywania kopii zapasowych może przebywać wyłącznie Administrator Bezpieczeństwa Informacji oraz osoby przez niego upoważnione.

§7

Sposób zabezpieczania systemu informatycznego przed wirusami komputerowymi oraz działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. Za zainstalowanie oprogramowania antywirusowego, jego aktualizację oraz uaktualnianie bazy definicji wirusów odpowiedzialny jest ASI lub inna osoba wyznaczona przez ASI.
2. Podczas uruchamiania komputera oprogramowanie antywirusowe skanuje sektor rozruchowy komputera i pamięć operacyjną. W trybie ciągłym monitoruje działania podczas otwierania oraz modyfikowania plików, skanuje pliki przychodzące w sieci zewnętrznej oraz pliki załączane do wiadomości e- mail.
3. Program antywirusowy chroni komputery przed wirusami i zagrożeniami bezpieczeństwa bez względu na ich źródło pochodzenia. Ochrona dotyczy wirusów i zagrożeń bezpieczeństwa rozprzestrzeniających się z dysków twardych, nośników zewnętrznych oraz sieci.
4. Użytkownik systemu natychmiast po umieszczeniu nośnika elektronicznego w systemie informatycznym odpowiedzialny jest za jego sprawdzenie pod kątem możliwości występowania wirusów.
5. Gdy podczas skanowania zostanie wykryty wirus, oprogramowanie antywirusowe domyślnie usiłuje usunąć go z zainfekowanego pliku i naprawić skutki działania wirusa. Pomyślne oczyszczenie pliku oznacza, że wirus został całkowicie usunięty. Jeśli z jakichś powodów oprogramowanie antywirusowe nie może oczyścić pliku, wówczas przenosi zainfekowany plik do obszaru kwarantanny. Zapobiega to rozprzestrzenianiu się wirusa. Po zaktualizowaniu bazy definicji wirusów oprogramowanie antywirusowe automatycznie sprawdza, czy w obszarze kwarantanny znajdują się jakieś pliki, a następnie skanuje je przy użyciu nowych danych systemu ochrony.
6. W przypadku wystąpienia infekcji i braku możliwości usunięcia wirusów przez system antywirusowy użytkownicy zobowiązani są do natychmiastowego powiadomienia ASI.

1) ASI sprawdza, czy nie zostały naruszone dane osobowe w systemie informatycznym.
2) W przypadku naruszenia danych ASI sporządza z zaistniałych okoliczności raport na postawie którego zabezpiecza system przed wystąpieniem ponownego zagrożenia.
3) ASI przywraca system informatyczny do poprawnej pracy.
4) Jeśli ASI stwierdzi, że użytkownik przyczynił się do zawirusowania systemu informatycznego z powodu nie zastosowania się do określonych procedur i regulaminów obowiązujących w Instytucie i doprowadził tym działaniem do naruszenia danych osobowych, wówczas powiadomieni o tym zostaje AD i ABI.

7. System informatyczny służący do przetwarzania danych osobowych chroniony jest przed zagrożeniami pochodzącymi z sieci publicznej przez zaporę sieciową- firewall. Firewall chroni sieć administratora danych przed nieuprawnionym dostępem z sieci zewnętrznej oraz kontroluje przepływ informacji pomiędzy tymi sieciami.

8. W sytuacji wykrycia włamania do systemu informatycznego użytkownicy zobowiązani są do natychmiastowego powiadomienia o tym ASI.

1) ASI sprawdza, czy nie zostały naruszone dane osobowe w systemie.
2) W przypadku naruszenia danych ASI sporządza z zaistniałych okoliczności raport na podstawie którego zabezpiecza system przed wystąpieniem ponownego zagrożenia.
3) ASI przywraca system informatyczny do poprawnej pracy.
4) Jeśli ASI stwierdzi, że użytkownik przyczynił się do włamania do systemu informatycznego z powodu nie stosowania się do określonych procedur i regulaminów obowiązujących w Instytucie i doprowadził tym działaniem do naruszenia danych osobowych, wówczas powiadomiony o tym zostaje AD i ABI.

9. W systemie informatycznym w Instytucie może być używane wyłącznie oprogramowanie licencjonowane przez posiadacza praw autorskich oraz może być używane tylko zgodnie z prawem licencji.

§8

Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych.

1. Dla każdej osoby, której dane przetwarzane są w systemie- z wyjątkiem elementów systemu służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie oraz elementów systemu używanych do przetwarzania danych zawartych w zbiorach jawnych- system ten zapewnia odnotowywanie informacji o:

1) odbiorcach danych, których dane zostały udostępnione;
2) dacie udostępnienia;

3) zakresie udostępnienia.

2. Odbiorca danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
   1) osoby, której dane dotyczą;
   2) osoby użytkownika systemu lub innej osoby upoważnionej do przetwarzania danych osobowych w Instytucie;
   3) przedstawiciela, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
   4) podmiotowi, któremu powierzono przetwarzanie danych;
   5) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

3. Obowiązek odnotowania w/w informacji spoczywa na użytkowniku systemu.

4. Udostępnienie danych osobowych w jakiejkolwiek formie może nastąpić wyłącznie na pisemna prośbę odbiorcy danych.

5. Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.

§9

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

1. Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego wykonywane są w terminach określonych przez producenta sprzętu, a jeśli nie są one podane, to w terminach ustalonych przez ASI.

2. Nieprawidłowości ujawnione w trakcie tych działań niezwłocznie są usuwane, a ich przyczyny przeanalizowane przez ASI przekazane Dyrektorowi ICHF PAN.

3. Za terminowość przeprowadzenia przeglądów i konserwacji oraz za ich prawidłowy przebieg odpowiada ASI.

4. W przypadku naprawy lub konserwacji urządzeń zawierających nośniki z danymi osobowymi, wszelkie prace prowadzone są w warunkach zapewniających ochronę przed udostępnieniem danych osobom niedopuszczonym do ich przetwarzania.

5. Naprawa lub konserwacja urządzeń zawierających nośniki z danymi osobowymi przez osoby niedopuszczone do przetwarzania tych danych odbywa się po usunięciu danych w sposób uniemożliwiający ich odczytanie. W przypadku, gdy usunięcie danych jest niemożliwe, przed dokonaniem naprawy albo, gdy usunięcie danych spowodowałoby utratę danych nie skopiowanych, naprawa odbywa się pod nadzorem ASI.

BEZPIECZEŃSTWO SIECI LAN/WLAN

1.1. Normy

System okablowania strukturalnego spełnia wymagania aktualnie obowiązującej normy: ISO/IEC 11801:2002.

1.2. Okablowanie

Całość budynku posiada okablowanie strukturalne, kategorii 6**,** z podziałem na okablowanie pionowe i poziome integrujące wszystkie systemy teletechniczne instalowane w budynku.

Wydajność okablowania jest zgodna z najnowszymi wytycznymi komitetów normalizacyjnych.

Trasy prowadzenia przewodów transmisyjnych okablowania poziomego oraz kabli okablowania pionowego są skoordynowane z istniejącymi i wykonywanymi instalacjami w budynku m.in. instalacją elektryczną ogólną, instalacją centralnego ogrzewania, wody, gazu, itp.

1.2.1. Poziome

Ze względu na bezpieczeństwo transmisji oraz w celu zminimalizowania oddziaływania zakłóceń, szczególnie w miejscach o dużej ilości kabli transmisyjnych, okablowanie poziome występuje w wersji ekranowanej bądź światłowodowej.

1.2.2. Pionowe

Kanały na instalację pionową są odpowiedniej przepustowości.

1.2.3. Międzywęzłowe

W połączeniach międzywęzłowych są stosowane światłowody.

1.3. Zasilanie energetyczne

Sieć zasilająca infrastrukturę techniczną systemu informatycznego ma możliwość podtrzymywania napięcia w sytuacjach awaryjnych pozwalających na bezpieczne wyłączenie urządzeń. Każdy węzeł sieci posiada UPS. Fragmenty instalacji elektrycznej, do których podłączone są komputery, monitory i urządzenia sieciowe, są wyposażone w listwy przeciwprzepięciowe, do których nie są podłączone inne urządzenia elektryczne.

1.3.1. UPS

Czas podtrzymania zasilania pracy urządzeń aktywnych jest obliczony w taki sposób, by było możliwe bezpieczne wyłączenie zasilanych urządzeń aktywnych w przypadku zaniku zasilania sieci.

1.4. PEL

W każdym pomieszczeniu użytkowników systemów specjalizowanych jak również w pomieszczeniach biurowych są zainstalowane punkty elektryczno-logiczne składające się z 2 gniazd logicznych i 4 gniazd elektrycznych według zapotrzebowania.

Wyjątek stanowią pomieszczenia techniczne serwerowni, pomieszczenie obsługi technicznej, pomieszczenie administratorów sieci lokalnej LAN i WLAN oraz same uruchomień i testów sprzętu, gdzie ilość PEL jest o ok. 20% większa niż zakładają to obecne potrzeby.

1.5. Wymagania budowlane

W przypadku budowy sieci LAN w nowych budynkach wymagane są jedynie prace dostosowawcze konfiguracyjne zależnie od potrzeb. Okablowanie jest prowadzone w rynnach PCV lub podwieszkach sufitowych wraz z pozostałym okablowaniem. Instalacje prowadzone w ścianach są wykonane w gładkich rurach PCV. Rury są prowadzone w liniach prostych, a tam, gdzie zmieniają kierunek, są zainstalowane drzwiczki rewizyjne.

1.6. Węzeł sieci

Węzły sieciowe znajdują się w wydzielonych pomieszczeniach, do których dostęp mają jedynie osoby uprawnione (administratorzy sieci LAN/WLAN).

Okablowanie węzła spełnia podstawowe wymagania:

- opis i numeracja gniazd w szafach krosowniczych i PEL'i jest wykonana w sposób jednoznaczny i nie nastręcza trudności w interpretacji zarówno w bieżącym użytkowaniu sieci jak i przy rozbudowie okablowania strukturalnego.

- dla każdego piętra lub segmentów sieci przewidziana jest wydzielona szafa krosownicza

- kable łączące serwery i urządzenia z szafą krosowniczą są w innym kolorze niż pozostałe.

- dedykowana dla okablowania instalacja elektryczna jest wykonana zgodnie z obowiązującymi normami i przepisami.

1.6.1. Szafa

Zainstalowane są szafy krosownicze wiszące. Do wszystkich zapewniony jest swobodny dostęp od frontu, a w większości ze wszystkich stron szafy.

1.6.2. Okablowanie

Okablowanie w węzłach jest rozmieszczone w sposób uporządkowany. Unika się splątania przewodów, a zapas kabla umieszczony jest poza szafą dystrybucyjną.

1.6.3. Urządzenia

Urządzenia aktywne sieci umożliwiają zdalne zarządzanie, które jest obsługiwane poprzez VLAN.

1.6.4. Wentylacja/klimatyzacja

Pomieszczenia są zabezpieczone przed dostępem osób nieupoważnionych i mają zapewniony odpowiedni poziom wentylacji umożliwiający poprawną eksploatację zamontowanego tam sprzętu.

Klimatyzacja węzła sieci jest dostosowana do warunków pomieszczenia i mocy cieplnej wydzielanej przez zainstalowane urządzenia.

Zapewniona jest odpowiednia wentylacja i klimatyzacja pomieszczeń, w których zainstalowano aktywne urządzenia sieciowe (serwery, routery, UPS i inne). W pomieszczeniach tych prowadzone są okresowe kontrole i monitoring temperatury.

Pomieszczenia techniczne, w tym serwerownia, są zabezpieczone przed dostępem osób trzecich.

1.6.5. Oświetlenie

Zastosowane jest oświetlenie zapewniające prawidłową widoczność szafy dystrybucyjnej ze wszystkich stron.

1.6.6. Pomieszczenie

Pomieszczenie przeznaczone na węzeł sieci zapewnia swobodną obsługę szafy dystrybucyjnej i urządzeń.

1.6.7. Dostęp do pomieszczenia

Dostęp do węzłów sieci jest ograniczony tylko do uprawnionego personelu technicznego oraz pracowników jednostek odpowiedzialnych za szkielet sieci.

1.7. Serwerownia

Pomieszczenie techniczne serwerowni to główny punkt dystrybucyjny okablowania strukturalnego, w którym zbiega się okablowanie poziome i pionowe obiektu, kable światłowodowe, jak również doprowadzenia traktów sieci rozległej.

1.7.1. Szafa

Wszystkie urządzenia aktywne, pasywne, modemy są umieszczone w szafach dystrybucyjnych typu „RACK”. Szafy krosownicze i teletechniczne są montowane w standardzie 19” i umożliwiają zainstalowanie odpowiedniej liczby urządzeń aktywnych.

1.7.2. Urządzenia

Liczba elementów aktywnych zależy od ilości punktów sieci. Na każde 48 punktów logicznych przewidziane jest miejsce w szafie o wysokości 2U. W szafach zarezerwowana jest przestrzeń umożliwiająca ewentualne ustawienie urządzeń teletransmisyjnych. Szafa uwzględnia miejsce na zamontowanie lokalnego UPS’a podtrzymującego działanie urządzeń aktywnych zamontowanych w szafie. W szafie zainstalowana jest listwa zasilająca umożliwiająca zasilanie zamontowanych tam urządzeń.

Montowane w szafach switche oraz urządzenia transmisji danych (routery i modemy) pochodzą od renomowanych producentów i są dobrane tak, by zabezpieczały ok. 10% wolnych gniazd dla łatwej rekonfiguracji połączeń w ramach sieci lokalnej.

1.7.3. UPS

Zastosowane są UPS-y o mocy sumarycznej pozwalającej na podtrzymanie wszystkich urządzeń aktywnych komputerowej sieci lokalnej.

1.7.4. Wentylacja/klimatyzacja

Klimatyzacja w pomieszczeniu serwerowni dostosowana jest do warunków pomieszczenia i mocy cieplnej wydzielanej przez zainstalowane urządzenia.

1.7.5. Oświetlenie

Zastosowane oświetlenie zapewnia prawidłową widoczność szaf dystrybucyjnych ze wszystkich stron.

1.7.6. Pomieszczenia

Systemy alarmowe spełniające wymagania trzeciego poziomu.

1.7.7. Dostęp do pomieszczenia

Serwerownia jest zabezpieczona przed dostępem osób trzecich. Pomieszczenie dla administratorów oraz operatorów jest oddzielone fizycznie od pomieszczenia technicznego serwerowni.

1.8. Przyłącza do budynku

Połączenia między budynkami są wykonywane przy użyciu łącz światłowodowych. Przyłącza światłowodowe znajdują się w miejscach, do których dostęp jest ograniczony.

Rozwojem i utrzymaniem sieci szkieletowej zajmuje się administrator systemu informatycznego.

1.9. Testowanie i szkolenie

Poprawność wykonania instalacji sieci sygnałowej jest potwierdzona pomiarami statycznymi i dynamicznymi właściwości poszczególnych torów. Testy zostały przeprowadzone dla wszystkich punktów przyłączeniowych. Dla łączy światłowodowych zostały przeprowadzone testy tłumienności sygnału zgodnie z wymaganiami odpowiednich standardów.

Szkolenia administratorów i użytkowników systemów w zakresie bezpieczeństwa - proces podnoszenia świadomości użytkowników oraz doskonalenie umiejętności bezpiecznej

eksploatacji systemu, w tym postępowania w przypadku wystąpienia incydentów bezpieczeństwa lub sytuacji kryzysowych.

Administrator organizuje systematyczne wewnętrzne szkolenia, testy i ćwiczenia dotyczące postępowania użytkowników systemu informatycznego z zasobami informacyjnymi oraz postępowania w przypadku wystąpienia incydentów bezpieczeństwa lub sytuacji kryzysowych.

1.10. Dokumentacja i certyfikaty

W posiadaniu znajduje się dokumentacja dotycząca serwerów, routerów, switchów i UPS-ów. Firma wykonująca zlecenia dotyczące infrastruktury sieciowej dostarcza dokumentację dotyczącą szaf dystrybucyjnych oraz certyfikaty kablowe.

Załącznik nr 1

....
Imię i nazwisko *data*

.....
Stanowisko/pełniona funkcja

OŚWIADCZENIE

Ja, niżej podpisany/a, **oświadczam, iż:**

- zostałem/am przeszkolony/a w zakresie ochrony danych osobowych i znana jest mi treść ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm.) oraz „Polityki Bezpieczeństwa danych Osobowych w Instytucie Chemii Fizycznej Polskiej Akademii Nauk" oraz **zobowiązuję się do:**
- zachowania w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem obowiązków pracowniczych na stanowisku ..... w ..... zadań służbowych*/ zadań zleconych** przez Instytut Chemii Fizycznej PAN; w szczególności nie będę wykorzystywał/a- w celach pozasłużbowych/ niezgodnych ze zleceniem/ powierzonym celem przetwarzania*- wykorzystywał/a danych osobowych, z którymi zapoznałem/am się w Instytucie, o ile nie są one powszechnie znane;
- zachowania w tajemnicy sposobów zabezpieczania danych osobowych stosowanych w Instytucie.

Jednocześnie oświadczam, że **przyjmuję do wiadomości, iż:**

- za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej osoby fizycznej, albo możliwej do zidentyfikowania- zgodnie z art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm.);
- sposoby zabezpieczania danych osobowych stosowane w IChF PAN stanowią tajemnicę pracodawcy oraz tajemnicę przedsiębiorstwa- w rozumieniu art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. nr 153, poz. 1503)**;
- postępowanie sprzeczne z powyższymi zobowiązaniami jest ciężkim naruszeniem obowiązków pracowniczych z wszystkimi wynikającymi stąd konsekwencjami, z rozwiązaniem stosunku pracy włącznie (za naruszenie przepisów karnych ustawy o ochronie danych osobowych/ przepisów prawa cywilnego**).

.....
własnoręczny podpis oświadczającego

** - podkreślić (lub wpisać) odpowiednie,, ponieważ oświadczenie składają poza pracownikami, również zleceniobiorcy i konsultanci przetwarzający dane osobowe.*
*** - w przypadku umowy cywilnoprawnej*

Oświadczenie sporządzane jest w dwóch jednobrzmiących egzemplarzach:
1 egz. - otrzymuje ABI,
1 egz. - otrzymują Kadry

Załącznik nr 2

....
(pieczęć pracodawcy) *(data)*

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Działając na podstawie art. 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)
- udziela się Panu/Pani*:

.....
(imię i nazwisko)

.....
(stanowisko służbowe)

.....
(nazwa komórki organizacyjnej)

do przetwarzania danych osobowych zawartych w następujących zbiorach:

.....

.....

Jest Pan/Pani* upoważniony/upoważniona* do przetwarzania danych osobowych wyłącznie w zakresie wynikającym z Pana/Pani* zadań służbowych oraz poleceń przełożonego.

Upoważnienie traci ważność w chwili ustania stosunku pracy lub cofnięcia upoważnienia do przetwarzania danych osobowych.

.....

(data i podpis Dyrektora Instytutu)

Załącznik nr 3

.....

(pieczęć pracodawcy) *(data)*

ODWOŁANIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Działając na podstawie art. 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (t.j. (Dz.Ust. nr 133 poz 883) z późniejszymi zmianami)
- odwołuję się Panu/Pani*:

.....

(imię i nazwisko)

.....

(stanowisko służbowe)

.....

(nazwa komórki organizacyjnej)

do przetwarzania danych osobowych zawartych w następujących zbiorach:

.....

.....

Jest Pan/Pani* upoważniony/upoważniona* do przetwarzania danych osobowych wyłącznie w zakresie wynikającym z Pana/Pani* zadań służbowych oraz poleceń przełożonego.

Upoważnienie traci ważność w chwili ustania stosunku pracy lub cofnięcia upoważnienia do przetwarzania danych osobowych.

.....

(data i podpis Dyrektora Instytutu)

Załącznik nr 4.

Ewidencja osób upoważnionych do przetwarzania danych osobowych w Instytucie Chemii Fizycznej Polskiej Akademii Nauk.

Imię i nazwisko	***pokój***	***Zbiór***	***Cel***
Małgorzata Pińkowska	Bud 9 p.40	Pracownicy/ Rodziny pracowników	Zatrudnienie (sprawy osobowe)
Jadwiga Skrzecz	Bud 9 p.40	Pracownicy/ Komisja socjalna/ Rodziny pracowników	Zatrudnienie (sprawy osobowe) Komisja socjalna (zasiłki, pożyczki)
Danuta Dudek	Bud 9 p.41	Doktoranci	Dokumentacja studiów doktoranckich, dokumentacja przewodów doktorskich, habilitacji, profesur, materiały które wpływają na stanowiska naukowe adiunkta, asystenta
Barbara Wilczek	Bud 9 p.41	Doktoranci	Dokumentacja studiów doktoranckich, dokumentacja przewodów doktorskich, habilitacji, profesur, materiały które wpływają na stanowiska naukowe adiunkta, asystenta
Ewa Pawełczyk	Bud 9 p.36	Przetargi/ zamówienia publiczne	Postępowanie o udzielenie zamówienia publicznego
Piotr Cwalina	Bud 9 p.42	Przetargi/ zamówienia publiczne	Postępowanie o udzielenie zamówienia publicznego
		Patenty	Regulowanie praw do własności, dokonywanie zgłoszeń patentowych
Aleksandra Kapuścińska-Bernatek	Bud 9 p.42	Potencjalni pracownicy	Praktyki studenckie w ICHF
		Przetargi/ zamówienia publiczne	Postępowanie o udzielenie zamówienia publicznego
		Pracownicy	Wynajem pokoi w akademiku, podpisywanie umów wynajmu
Anna Garwolińska	Bud 9 p.27	Księga korespondencyjna	Korespondencja
Małgorzata Kanoza	Bud 9 p.8	Pracownicy, Konkursy	Sporządzanie wniosków na projekty badawcze, stypendia, umowy o finansowanie projektu badawczego

Zofia Wolarek	Bud 9 p.8	Pracownicy, Konkursy	Sporządzanie wniosków na projekty badawcze, stypendia, umowy o finansowanie projektu badawczego
Olga Niemiec	Bud 9 p.8	Pracownicy, Konkursy	Sporządzanie wniosków na projekty badawcze, stypendia, umowy o finansowanie projektu badawczego
Małgorzata Krajewska	Bud 9 p.23	Pracownicy	Ocena dorobku pracowników naukowych, realizacja projektów np. badawczych
Patrycja Nitoń	Bud 9 p.19	Pracownicy, Konkursy	Przygotowywanie umów , realizacja projektów badawczych, zlecenia
Illonarda Raczko	Bud 9 p.34	Pracownicy Kontrahenci	Współpraca dyrekcji z innymi jednostkami, konkursy, umowy, bieżące sprawy
Izabela Ozóg	Bud 9 p. 24	Wszystkie zbiory	Główna Księgowa
Anna Wójcik	Bud 9 p.25	Pracownicy Kontrahenci	Płace, Faktury
Ewa Wronek	Bud 9 p.25	Pracownicy Kontrahenci	Płace
Aneta Gawęda- Fijołek	Bud 9 p.22	Pracownicy Kontrahenci	Sprawy księgowe
Izabela Beszczyńska	Bud 9 p.26	Pracownicy Kontrahenci	Sprawy księgowe
Bożena Łaskawiec	Bud 9 p.24	Pracownicy Kontrahenci	Sprawy księgowe
Henryka Skrzypczak	Bud 9 p.21	Pracownicy Kontrahenci	Sprawy księgowe
Wiesława Sobieraj	Bud 9 p.22	Pracownicy Kontrahenci	Sprawy księgowe
Magdalena Szustak	Bud 9 p.22	Pracownicy Kontrahenci	Sprawy księgowe
Katarzyna Polkowska	Bud 9 p.20	Pracownicy, Komisja socjalna	Karta szkolenia, badania profilaktyczne, zasiłki, pożyczki
Małgorzata Kowalewska-Jóźwik	Bud 9 p.44	Wszystkie zbiory	Archiwizacja
Danuta Szczecińska	Bud 9 p.44	Wszystkie zbiory	Archiwizacja
Agnieszka Duchnowska	Bud 9 hol	Księga wejść i wyjść	Ewidencja osób wchodzących na teren zakładu
Agnieszka Tadrzak	Bud 9 p.19	Konkursy, Pracownicy	Przygotowywanie umów , realizacja projektów badawczych, zlecenia
Rafał Chabrowski	Bud 3 p.37	Wszystkie zbiory	Informatyk – dostęp do wszystkich systemów informatycznych

Rafał Gąsiorowski	Bud 3 p.37	Wszystkie zbiory	Informatyk – dostęp do wszystkich systemów informatycznych
Tadeusz Pacholik	Bud 9 p.43	Wszystkie zbiory	Zarząd Instytutu ICHF
Jacek Gregorowicz	Bud 9 p.34	Wszystkie zbiory	Zarząd Instytutu ICHF
Robert Hołyst	Bud 7 p.133	Pracownicy/ Potencjalni Pracownicy	Zatrudnienie
Marcin Opałło	Bud 9 p.34	Wszystkie zbiory	Zarząd Instytutu ICHF
Marek Tkacz	Bud 7a p.204	Pracownicy/ Potencjalni Pracownicy	Zatrudnienie
Włodzimierz Kutner	Bud 6 p.156	Pracownicy/ Potencjalni Pracownicy	Zatrudnienie
Joanna Niedziółka Jönsson	Bud 3 p.32	Pracownicy/ Potencjalni Pracownicy	Zatrudnienie
Piotr Bernatowicz	Bud 3 p.54	Pracownicy/ Potencjalni Pracownicy	Zatrudnienie
Piotr Garstecki	Bud 7 p.147	Pracownicy/ Potencjalni Pracownicy	Zatrudnienie
Marcin Fiałkowski	NH p.212	Pracownicy/ Potencjalni Pracownicy	Zatrudnienie
Janusz Lewiński	NH p.108	Pracownicy/ Potencjalni Pracownicy	Zatrudnienie
Aleksander Jabłoński	Bud 7 p.123	Pracownicy/ Potencjalni Pracownicy	Zatrudnienie
Zbigniew Karpiński		Pracownicy/ Potencjalni Pracownicy	Zatrudnienie
Zbigniew Kaszkur	Bud 6 p. 250, 252	Pracownicy/ Potencjalni	Zatrudnienie
Rafał Szmigielski	Bud 7a p.112, 114	Pracownicy/ Potencjalni Pracownicy/ Komisja socjalna	Zatrudnienie , zasiłki, pożyczki
Tadeusz Zakroczymski	Bud 7a p.211	Pracownicy/ Potencjalni Pracownicy	Zatrudnienie
Robert Nowakowski	Bud 7a p.120	Pracownicy/ Potencjalni Pracownicy	Zatrudnienie
Jerzy Górecki	Bud 10 p.4	Pracownicy/ Potencjalni Pracownicy	Zatrudnienie
Robert Kołos	Bud 7a p.203	Pracownicy/ Potencjalni Pracownicy	Zatrudnienie

Marek Pietraszkiewicz	Bud 4a NH20	Pracownicy/ Potencjalni Pracownicy	Zatrudnienie
Sa Jacinto	Bud 7a p.104	Pracownicy/ Potencjalni Pracownicy	Zatrudnienie
Czesław Radzewicz	Bud 3 p.45	Pracownicy/ Potencjalni Pracownicy	Zatrudnienie
Jacek Waluk	Bud 7a p.78	Pracownicy/ Potencjalni Pracownicy	Zatrudnienie
Wojciech Góźdź	Bud 7a p.210	Pracownicy/Potencjalni Pracownicy	Zatrudnienie
Martin Jonsson-Niedziółka	Bud 3 p.35	Pracownicy/Potencjalni Pracownicy	Zatrudnienie
Piotr Zarzycki	Bud 7 p.247	Pracownicy/Potencjalni Pracownicy	Zatrudnienie
Patryk Ejgierd Zaleski	Bud 7 p.246	Pracownicy/Potencjalni Pracownicy	Zatrudnienie
Juan Colmenares	Bud 6 p.255	Pracownicy/Potencjalni Pracownicy	Zatrudnienie
Anna Ochab- Marcinek	Bud 7p.129	Pracownicy/Potencjalni Pracownicy	Zatrudnienie
Ryszard Sokołowski	Bud 9 p.20	Sprawy socjalne	Zasiłki, Pożyczki
Janusz Sobczak	Bud 6 p.153	Sprawy socjalne	Zasiłki, Pożyczki
Maciej Małecki	NH p.16	Pracownicy	
Alicja Rusinowska	Bud 3 p.13	Pracownicy	Usługi medyczne - recepty
Anna Wątróbska	Bud 3 p.14	Pracownicy	Usługi medyczne - recepty
Onisk Leontyna Halina	Bud 3 p.14	Pracownicy	Usługi medyczne - recepty
Joanna Bielecka- Mądry	Bud 9 p.11	Studenci Biblioteka	Wypożyczanie książek
Jolanta Szymańska	Bud 9 p.14	Studenci	Wypożyczanie książek
Jadwiga Wojnar	Bud 9 p.14	Pracownicy	
Tomasz Miśkiewicz		Pracownicy , Potencjalni Pracownicy	Dyrektor Chemipan

Załącznik 5

Oprogramowania

W Instytucie Chemii Fizycznej Polskiej Akademii Nauk do przetwarzania danych osobowych wykorzystuje się następujące oprogramowania:

1. MS OFFICE 2007/2010/ 2012
2. Xpertis (kadry i płace)
3. Titan (wejściówki)
4. Unicard (wejściówki)
5. Bank BPH
6. Archsys (archiwum)
7. Asystent BHP 4.0
8. POLON
9. Thunderbird poczta

Wykaz zbiorów danych osobowych i ich struktura

- **pracownicy** *(Imię, nazwisko, adres, PESEL, data i miejsce urodzenia, wykształcenie, przebieg dotychczasowego zatrudnienia, nr konta, wynagrodzenie)*
- **potencjalni pracownicy** (*(Imię, nazwisko, adres, PESEL, data i miejsce urodzenia, wykształcenie, przebieg dotychczasowego zatrudnienia)*
- **doktoranci** *(Imię, nazwisko, adres, PESEL, data i miejsce urodzenia, wykształcenie, przebieg dotychczasowego zatrudnienia, dorobek naukowy)*
- **studenci** *(Imię, nazwisko, adres, nr telefonu)*
- **przetargi/ zamówienia publiczne** *(Imię, nazwisko, zaświadczenie o niekaralności, miejsce pracy (firma))*
- **patenty** *(Imię, nazwisko, adres, PESEL)*
- **księga korespondencyjna** *(Imię, nazwisko, zakład pracy, dział, adres)*
- **konkursy** *(Imię, nazwisko, wykształcenie, doświadczenie zawodowe, adres, PESEL, data i miejsce urodzenia, seria, nr dowodu osobistego, e- mail, nr telefonu)*
- **kontrahenci** (Imię, nazwisko, PESEL, NIP, adres, urząd skarbowy)
- **księga wejść i wyjść** *(Imię, nazwisko, adres zamieszkania, nr dowodu osobistego)*
- **biblioteka** *(Imię, nazwisko, adres zamieszkania, nr dowodu osobistego)*
- **komisja socjalna** *(Imię, nazwisko, nr telefonu, informacje o chorobie, zarobki)*
- **usługi medyczne** *(Imię, nazwisko, PESEL, informacje o stanie zdrowia)*
- **rodziny pracowników** *(Imię, nazwisko, pesel, adres zamieszkania)*