Zarządzenie **Nr 31/2013**
Dyrektora Centrum Materiałów Polimerowych i Węglowych PAN w Zabrzu
z dnia 13 listopada 2013

§ 1.

Niniejszym zarządzeniem wprowadzam do stosowania w Centrum:

a) Politykę bezpieczeństwa w zakresie ochrony danych osobowych obowiązującą w Centrum Materiałów Polimerowych i Węglowych PAN w Zabrzu (stanowiącą zał. nr 1 do niniejszego zarządzenia)
b) Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Centrum Materiałów Polimerowych i Węglowych PAN w Zabrzu (stanowiącą zał. Nr 2 do niniejszego zarządzenia),
c) Ewidencję osób upoważnionych do przetwarzania danych osobowych w Centrum Materiałów Polimerowych i Węglowych PAN w Zabrzu (stanowiącą zał. Nr 3 do niniejszego zarządzenia),

§ 2.

Wyznacza się administratora bezpieczeństwa informacji w osobie: dr hab. Jan Weszka, prof. nzw. PAN

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.

Dyrektor Instytutu
prof. dr hab. Andrzej Dworak

Załącznik nr 1
do Zarządzenia Nr 31/2013
Dyrektora Centrum Materiałów Polimerowych i Węglowych PAN w Zabrzu, z dnia 13.11.2013 roku

Polityka bezpieczeństwa obowiązująca w Centrum Materiałów Polimerowych i Węglowych PAN w Zabrzu

§ 1
Zagadnienia wstępne i definicje

1. Polityka niniejsza została opracowana i wdrożona ze względu na fakt, iż Centrum Materiałów Polimerowych i Węglowych PAN w Zabrzu, zwane dalej "Centrum", jest administratorem danych osobowych, w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.) Niniejsza polityka dotyczy wszystkich osób biorących udział w sposób bezpośredni lub pośredni w przetwarzaniu danych osobowych w Centrum.

2. Poprzez bezpieczeństwo należy rozumieć stan faktyczny uniemożliwiający wykorzystanie, przepływ, modyfikację lub zniszczenie informacji w zakresie danych osobowych w Centrum przez osoby postronne lub nieupoważnione.

3. Polityka oraz związane z nią dokumenty zostały opracowane zgodnie z wymaganiami obowiązujących przepisów prawnych, w szczególności zaś:
   - Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych wraz z późniejszymi zmianami (zwanej dalej Ustawą)
   - Rozporządzenia ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, wraz z późniejszymi zmianami (zwanego dalej Rozporządzeniem)

4. Dyrektor Centrum wyznacza administratora bezpieczeństwa informacji w celu sprawowania nadzoru nad przestrzeganiem obowiązujących zasad bezpieczeństwa danych osobowych oraz reprezentowania administratora danych osobowych. Administratorem bezpieczeństwa może być pracownik Centrum.

5. Wszystkie osoby biorące bezpośredni lub pośredni udział w procesie przetwarzania danych osobowych w systemie informatycznym są odpowiedzialne za właściwe zabezpieczanie tych danych.

§ 2
Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

1. Dane osobowe przetwarzane są w siedzibie Centrum Materiałów Polimerowych i Węglowych PAN:
   - w budynku w Zabrzu przy ul. M. Curie-Skłodowskiej 34 w pomieszczeniach: 124, 125, 126, 128, 129, 143, 221, 35
2. Pomieszczenia zabezpieczone są przed dostępem osób trzecich.
3. Nośniki informacji będą przechowywane w pomieszczeniach nr 124, 129 w Zabrzu, w zamkniętej szafie.

§ 3
Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

1. Centrum posiada następujące zbiory danych osobowych:
   a. zbiór danych osobowych pracowników Centrum i członków ich rodzin
   b. wykaz placówek współpracujących
   c. ewidencję osób upoważnionych do przetwarzania danych osobowych

2. Dane osobowe przetwarzane są z użyciem następujących programów:
   a. zbiór danych osobowych przy użyciu programów MADAR, PŁATNIK.
   b. ewidencję osób upoważnionych do przetwarzania danych osobowych przy użyciu edytora tekstu Microsoft WORD oraz arkusza kalkulacyjnego Microsoft Excel.
   c. dedykowany system informatyczny do obsługi zamówień, kart pracy oraz informacji o umowach zlecenia i o dzieło.
   d. system informatyczny do wspomagania rozliczeń projektów oraz grantów.

§ 4
Opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi

1. Dane osobowe są przetwarzane według następujących pozycji:

   a. zbiór danych osobowych pracowników Centrum
      I. imię
      II. nazwisko
      III. data urodzenia
      IV. miejsce zamieszkania
      V. adres korespondencyjny
      VI. stanowisko
      VII. numery NIP i Pesel
      VIII. numer rachunku bankowego
      IX. członkowie rodziny podlegający zgłoszeniu do ubezpieczenia społecznego

X. stopień pokrewieństwa

b. wykaz placówek współpracujących
   I. imię
   II. nazwisko
   III. firma
   IV. adres
   V. numer NIP

c. ewidencję osób upoważnionych do przetwarzania danych osobowych
   I. imię i nazwisko

2. Nie istnieje przepływ danych pomiędzy zbiorami określonymi w § 3.

§ 5

Określenie środków technicznych organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Zbiory danych osobowych podlegają ochronie i zabezpieczeniu w ten sposób, że:
   a) Budynek Centrum Materiałów Polimerowych i Węglowych poza godzinami pracy chroniony jest są systemem alarmowym oraz monitoringiem, którego naruszenie powoduje uruchomienie alarmu i powiadomienie pracownika firmy ochroniarskiej. Ponadto budynek strzeżony jest przez pracowników firmy ochroniarskiej 24 godz./dobę, a pracownicy ci sprawują również kontrolę nad osobami przebywającymi na terenie Centrum.
   b) W przypadku nieobecności osób zatrudnionych i upoważnionych do przetwarzania danych, pomieszczenia w których przetwarzane są dane osobowe zamykane są na klucz, a klucz zdeponowany u pracownika ochrony.
   c) Pojedyncze komputery zawierające dane osobowe zostają zabezpieczone hasłem. Pracownicy zatrudnieni przy ich obsłudze nie mogą zezwalać na użytkowanie komputera osobom nieupoważnionym. Hasło umożliwiające dostęp do komputera definiuje administrator bezpieczeństwa.
   d) Po zakończeniu pracy użytkownik zobowiązany jest do wylogowania z systemu, wyłączenia komputera i – raz na tydzień - umieszczenia kopii danych osobowych w szafach zamykanych na klucz w pomieszczeniach znajdujących się pokojach wymienionych w § 2 Polityki bezpieczeństwa, w sposób uniemożliwiający zapoznanie się z ich treścią osobom trzecim.
   e) Przebywanie w pomieszczeniach osób nieupoważnionych jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych.
   f) Monitory komputerów należy ustawić tak, aby uniemożliwić osobom postronnym wgląd do danych osobowych.
   g) Serwery zabezpieczone są hasłami, dostęp sieciowy poprzez firewall, oprogramowanie serwerowe poprzez zastosowanie haseł i algorytmu szyfrowania danych w sieci.

2. Do przetwarzania danych osobowych w Centrum uprawnione są tylko osoby upoważnione i wpisane do ewidencji.

3. Zakresy czynności osób zatrudnionych przy przetwarzaniu danych osobowych zawierają obowiązki z zakresu odpowiedzialności za bezpieczeństwo danych osobowych.

§ 6
Zmiany i udostępnienie tekstu polityki bezpieczeństwa

1. Dopuszcza się dokonywania zmian w niniejszym dokumencie.

2. Tekst Polityki bezpieczeństwa zostanie udostępniony użytkownikom w taki sposób, aby mogli się z nim zapoznać i wdrożyć w życie jej postanowienia.

Załącznik nr 2
do Zarządzenia Nr31/2013
Dyrektora Centrum Materiałów Polimerowych i Węglowych PAN w Zabrzu, z dnia 13.11.2013 roku

Instrukcja
zarządzania systemem informatycznym do przetwarzania danych osobowych w Centrum Materiałów Polimerowych i Węglowych PAN w Zabrzu

§ 1
Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień.

1. Każdy użytkownik komputera, na którym są przetwarzane dane osobowe otrzyma identyfikator oraz hasło pozwalające na zalogowanie się do systemu operacyjnego.
2. O przyznaniu hasła decydować będzie Administrator bezpieczeństwa.
3. Każdy z użytkowników przed dopuszczeniem do używania komputera, na którym przetwarzane są dane osobowe zapozna się z niniejszą Instrukcją i Polityką bezpieczeństwa i wpisany zostanie do ewidencji osób upoważnionych.
4. Po zakończeniu pracy na komputerze użytkownik obowiązany jest wylogować się z systemu.
5. W przypadku awarii, zagubienia hasła lub innych nieprzewidzianych sytuacji zagrażających bezpieczeństwu danych każdy z użytkowników obowiązany jest niezwłocznie powiadomić Administratora bezpieczeństwa informacji.

§ 2
Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Użytkownicy zostaną powiadomieni o haśle ze stosownym pouczeniem o poufnym charakterze hasła oraz obowiązku zachowania go w tajemnicy i zakazie ujawnienia go osobom trzecim, w tym innym użytkownikom.
2. Użytkownik obowiązany jest zapamiętać hasło, o którym mowa powyżej.
3. Hasło składać się będzie z ciągu co najmniej 8 znaków, zawierającego co najmniej jedną cyfrę i jeden znak specjalny.
4. Hasła będą różne dla każdego z użytkowników.

§ 3
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników

1. Rozpoczęcie pracy to moment zalogowania się do systemu

2. Zawieszenie pracy w systemie to każda przerwa w pracy związana chociażby z chwilowym odejściem od komputera.
3. Zakończeniem pracy w systemie jest chwila wylogowania się zeń użytkownika.
4. W celu uruchomiania komputera użytkownik powinien:
   a) włączyć komputer
   b) zalogować się do systemu poprzez wskazanie identyfikatora i wpisanie hasła.
5. Użytkownik podczas logowania do systemu nie może ujawniać hasła osobom trzecim, w tym innym użytkownikom.
6. Użytkownik zobligowany jest do skutecznego wylogowania się z systemu za każdym razem, gdy zamierza opuścić stanowisko pracy, niezależnie od tego, na jak długo ma zamiar odejść od komputera.
7. Wylogowanie następuje poprzez wybranie w systemie opcji "wyloguj" lub zablokowanie ekranu w sposób, który uniemożliwia odblokowanie go bez znajomości hasła.
8. Po zakończeniu pracy użytkownik zobowiązany jest do wyłączenia komputera.
9. O każdym podejrzeniu ingerencji w dane osobowe osób nieuprawnionych pracownik obowiązany jest powiadomić Administratora bezpieczeństwa

§ 4
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

- Użytkownicy zobowiązani są to tworzenia kopii zapasowych baz danych osobowych z częstotliwością raz na tydzień. Osoba odpowiedzialna za zasoby informatyczne zobowiązana jest do tworzenia kopii baz danych przechowywanych na serwerach Centrum w pomieszczeniach 143, 221 w Zabrzu oraz 212b w Gliwicach.
- Kopie zapisuje się na dyskach CD/DVD
- Kopie oznaczone imieniem, nazwiskiem oraz datą przechowuje się w budynku Centrum w Zabrzu, w pomieszczeniu nr 124, 129, w szafie zamykanej na klucz.
- Dodatkowo na zasadzie synchronizacji plików między stacjami roboczymi a serwerem wykonywana jest jedna kopia danych wybranych katalogów kluczowych stacji roboczych: Dyrektora, Sekretariatu, Działu kadr, Działu Obsługi Badań, biblioteki, Głównego księgowego, Biura Koordynacji Projektów, Zastępcy Dyrektora ds. administracyjno-ekonom, Sekretariatu Naukowego.
- Obiekt jest strzeżony przez profesjonalną firmę ochraniarską.

§ 5
Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

1. Elektroniczne nośniki informacji zawierające dane osobowe są przechowywane w zamkniętych szafkach z zabezpieczeniem przed dostępem osób trzecich.
2. Kopie zapasowe będą niezwłocznie zniszczone po ustaniu użyteczności danych osobowych tam zawartych.
3. Ze zniszczonych kopii zapasowych spisuje się stosowny protokół opatrzony podpisem Administratora bezpieczeństwa i osoby sporządzającej protokół.
4. Kopie przechowuje się przez okres 2 lat, o ile przepisy nie przewidują obowiązku dłuższego przechowywania. Jeśli użyteczność danych ustała przed okresem 2 lat, kopie mogą zostać zniszczone.

§ 6
Sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania

1. Komputery na których przetwarzane są dane osobowe chronione będą przed działaniem wirusów komputerowych oprogramowaniem antywirusowym aktualizowanym na bieżąco (oprogramowanie firmy. **ESET spol. s.r.a. Oddział w Polsce** z siedzibą w Krakowie przy ulicy Smoleńsk 21/5I5B, kod pocztowy: 31-108)
2. W celu przeciwdziałania atakom spowodowanym przez zainfekowane pliki użytkownik jest zobowiązany skanować system co najmniej dwa razy w tygodniu pod kątem obecności w systemie wirusów i innych zagrożeń.
3. W przypadku wykrycia jakiegokolwiek zagrożenia użytkownik niezwłocznie zawiadamia Administratora bezpieczeństwa informacji.

§ 7
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

1. W przypadku przekazania komputerów do serwisu lub naprawy innym podmiotom wszelkie dane osobowe zostaną z nich usunięte.
2. Dane należy zabezpieczyć przed dostępem osób trzecich zanim nośnik lub element systemu zostanie przekazany podmiotowi innemu niż Administrator bezpieczeństwa informacji.