Załącznik nr 14 do Polityki Bezpieczeństwa

Danych Osobowych w Uniwersytecie Opolskim

## Ogólny opis organizacyjnych środków bezpieczeństwa

Aby zapewnić prawidłowość przetwarzania danych osobowych Administrator wdraża następujące środki organizacyjne:

* 1. Polityka Bezpieczeństwa Przetwarzania Danych Osobowych – określa zasady ochrony i przetwarzania danych osobowych w Uniwersytecie Opolskim.
  2. Opracowanie i wdrożenie instrukcji zarządzania systemem informatycznym.
  3. System wydawania upoważnień do przetwarzania danych osobowych – w celu ograniczenia ilości pracowników Uczelni mających dostęp do konkretnych danych osobowych - do przetwarzania danych dopuszczone są wyłącznie osoby posiadające upoważnienie.
  4. Prowadzenie ewidencji osób dopuszczonych do przetwarzania danych osobowych.
  5. Zobowiązanie osób przetwarzających dane osobowe do zachowania ich w tajemnicy.
  6. System nadawania uprawnień dostępu do systemu informatycznego – w celu ograniczenia uprawnień w systemach wyłącznie do wymaganych dla realizacji zadań służbowych ze względu na rolę w systemie informatycznym (ograniczenia ilości osób a uprawnieniami administratorów systemów).
  7. Prowadzenie ewidencji osób mających dostęp do systemu, w którym przetwarzane są dane osobowe.
  8. System wykonywania kopii zapasowych – kopie zapasowe zbioru danych osobowych muszą być przechowywane w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.
  9. Wzór umowy powierzenia przetwarzania danych osobowych.
  10. System szkolenia pracowników z zasad ochrony danych osobowych.
  11. Szkolenie osoby zatrudnionej przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.
  12. Wyznaczenie inspektora ochrony danych.
  13. Wyznaczenie administratora systemów informatycznych.
  14. Wyznaczenie lokalnych administratorów danych osobowych (LADO).
  15. Utrzymywanie kompletnej i aktualnej dokumentacji systemów informatycznych oraz bieżąca aktualizacja tych systemów.
  16. Wprowadzenie zakazu wykonywania przez użytkowników kopii całych zbiorów danych. Zbiory danych w całości mogą być kopiowane tylko przez Administratora Systemu Informatycznego/Lokalnego Administratora Systemu Informatycznego lub automatycznie przez oprogramowanie do wykonywania kopii zapasowych, z zachowaniem procedur ochrony danych osobowych.
  17. Wprowadzenie zakazu wynoszenia poza teren UO na jakichkolwiek nośnikach całych zbiorów danych osobowych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej.
  18. Wprowadzenie obowiązku szyfrowania plików z danymi osobowymi, które znajdują się na przenośnych urządzeniach i nośnikach danych, jak również plików przesyłanych drogą elektroniczną, przechowywane ww. w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).