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

Jako Administrator Danych Osobowych, na podstawie art. 32 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Ogólne Rozporządzenie o Ochronie Danych) (Dz.U.UE.L.2016.119.1) – dalej **RODO (GDPR)**, określam techniczne i organizacyjne środki niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych:

1. Wyznaczenie Inspektora Ochrony Danych.
2. Wyznaczenie Administratora Systemów Informatycznych.
3. Wprowadzenie procedur regulujących procesy przetwarzania danych.
4. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych zgodnie ze wzorem ewidencji stanowiącym załącznik nr 4 do niniejszej Polityki Ochrony Danych Osobowych.
5. Do przetwarzania danych osobowych są dopuszczone tylko osoby upoważnione zgodnie ze wzorem upoważnienia stanowiącym załącznik nr 6 do niniejszej Polityki Ochrony Danych Osobowych.
6. Przeprowadzanie okresowych przeglądów sieci informatycznej, w tym przeprowadzanie cyklicznych testów odtwarzania serwera z kopii zapasowej.
7. Dostęp do systemu informatycznego następuje z użyciem Identyfikatora   
   i Hasła.
8. Zastosowanie mechanizmów rozliczalności działań poszczególnych Użytkowników.
9. Zastosowanie oprogramowania antywirusowego w tym systematyczne instalowanie wymaganych przez producentów oprogramowania aktualizacji związanych z bezpieczeństwem.
10. Zastosowanie zapory ogniowej (firewall) ze zdefiniowanymi listami dostępów.
11. Szczegółowe zabezpieczenia fizyczne są opisane w dokumentacji prowadzonej przez Specjalistę ds. obronnych. Dokumentacja może być udostępniona tylko osobom upoważnionym przez Kanclerza ASP.
12. Obowiązkowe szkolenia pracowników ASP odbywające się w miarę uzasadnionych potrzeb, w zakresie ochrony danych osobowych.
13. W celu zapewnienia rozliczalności dostępu do danych:
    1. z dniem rozwiązania stosunku pracy z użytkownikiem:
       * ASI zamyka konto użytkownika w systemie informatycznym oraz zabezpiecza dostęp do danych hasłem;
       * dane z konta użytkownika, z którym rozwiązano stosunek pracy, są archiwizowane lub usuwane – zgodnie z decyzją kierownika jednostki organizacyjnej, w której zatrudniony był użytkownik,
       * IOD lub osoba zastępująca wpisuje w ewidencji osób upoważnionych do przetwarzania danych osobowych, datę wygaśnięcia upoważnienia do przetwarzania danych osobowych,
    2. w karcie obiegowej użytkownika, z którym rozwiązano stosunek pracy:
       * ASI potwierdza zamknięcie konta pracownika w systemie informatycznym,
       * IOD lub osoba zastępująca potwierdza wpisanie do ewidencji osób upoważnionych daty wygaśnięcia upoważnienia.