ZAŁĄCZNIK
Do Zarządzenia Starosty Cieszyńskiego
nr. WO.120.45.2016....

PROCEDURA UDOSTĘPNIANIA DANYCH PODLEGAJĄCYCH OCHRONIE, A W SZCZEGÓLNOŚCI Z USTAWY O OCHRONIE DANYCH OSOBOWYCH

§ 1
SŁOWNIK POJĘĆ

1. **ASI** – Administrator Systemu Informatycznego, Pracownik do którego zadań należy dbanie o właściwe działanie sprzętu i oprogramowania, w sposób zapewniający właściwy poziom ochrony określony przez ABI,
2. **Baza Wiedzy** - zakładka w HelpDesk, redagowana przez ASI, zawierająca informacje, instrukcje, regulaminy, wzory wniosków oraz sposoby rozwiązywania problemów,
3. **HelpDesk** - portal intranetowy, dostępny w sieci Starostwa, który służy do wykonywania zgłoszeń wg zdefiniowanych w nim kategorii oraz do wymiany informacji.

§ 2
UDOSTĘPNIANIE NA NOŚNIKACH ELEKTRONICZNYCH

1. Udostępnienie danych odbywa się na podstawie "Polityki Bezpieczeństwa Danych Osobowych w Starostwie Powiatowym w Cieszynie" oraz na podstawie innych przepisów prawa.
2. Przed zapisem na nośnik elektroniczny, dane należy zabezpieczyć metodami kryptograficznymi na przykład za pomocą archiwów chronionych hasłem (zip, 7z, itp.). Hasła deszyfracji należy przekazać inną drogą niż nośnik zawierający chronione dane, np: poczta elektroniczna, telefon. Stosowna instrukcja znajduje się w systemie HelpDesk w zakładce Baza Wiedzy.
3. Nośniki elektroniczne zawierające udostępniane dane chronione przekazuje się:
   1) osobiście przez Pracownika właściwej komórki organizacyjnej,
   2) za pośrednictwem korespondencji pocztowej,
   3) za pośrednictwem firmy kurierskiej.

§ 3
UDOSTĘPNIANIE POPRZEZ TRANSMISJĘ DANYCH W SIECI PUBLICZNEJ INTERNET

1. Dla zachowania odpowiedniego poziomu bezpieczeństwa dotyczącego transmisji danych w sieci publicznej internet dopuszcza się następujące metody połączeń:
   1) wirtualnej sieci prywatnej VPN,
   2) szyfrowanego protokołu SFTP.
2. Za określenie parametrów i poziomów szyfrowania oraz infrastruktury sieciowej dla realizacji połączeń, o których mowa w ust. 1 odpowiada ASI.
3. Minimalne parametry zabezpieczeń, o których mowa w par 2. określono w odrębnej, wewnętrznej instrukcji.
4. Podczas transmisji danych za pomocą szyfrowanego protokołu SFTP, dane należy zabezpieczyć dodatkowo metodami kryptograficznymi na przykład za pomocą archiwów chronionych hasłem (zip, 7z, itp.). Hasła deszyfracji należy przekazać inną drogą niż nośnik zawierający chronione dane, np.: poczta elektroniczna, telefon. Stosowna instrukcja znajduje się w systemie HelpDesk w zakładce Baza Wiedzy.