1. **Cel**

Określenie zasad dotyczących postępowania zapewniającego bezpieczeństwo urządzeń lub/i nośników informacji zawierających dane osobowe.

1. **Zakres obowiązywania**

Procedura obowiązuje wszystkich użytkowników upoważnionych do przetwarzania danych osobowych w systemie informatycznym.

1. **Opis postępowania**
   1. Przekazywanie, niszczenie nośników zawierających dane osobowe:
      1. Urządzenia lub/i nośniki danych przeznaczone do likwidacji należy wcześniej pozbawiać zapisanych danych w sposób uniemożliwiający ich odzyskanie lub uszkodzone, w taki sposób aby odczyt danych stał się niemożliwy.
      2. Z urządzeń i/lub nośników danych zawierających dane osobowe przed przekazaniem podmiotowi nieuprawnionemu do przetwarzania danych osobowych należy te dane usunąć w sposób trwały uniemożliwiający późniejsze ich odczytanie/odtworzenie.
      3. Z urządzeń i/lub nośników danych zawierających dane osobowe przed przekazaniem do naprawy należy usunąć te dane w sposób trwały uniemożliwiający późniejsze odczytanie/odtworzenie lub naprawiać w obecności osoby upoważnionej.
      4. Dopuszcza się przekazanie urządzeń i/lub nośników danych bez usunięcia danych osobowych jedynie w przypadku przekazywania ich specjalistycznej firmie w celu odzyskania danych i po uzyskaniu zgody Administratora Danych Osobowych.

W takiej sytuacji wymagane jest zobowiązanie firmy zewnętrznej do podpisania umowy powierzenia danych osobowych.

* + 1. Transport urządzeń i/lub nośników zawierających dane osobowe poza granice obszarów przetwarzania firmy powinien być:
* dokonywany w sposób uniemożliwiający uzyskanie dostępu do nich przez osoby nieuprawnione,
* dokonywany z zachowaniem szczególnej uwagi, tak aby nośnik informacji nie został zgubiony, skradziony lub uszkodzony.
  + 1. W przypadku zlecania transportu urządzeń i/lub nośników danych należy korzystać z godnego zaufania transportu i kurierów.
  1. Wymagania dotyczące szyfrowania urządzeń i/lub nośników:
* szyfrowanie musi być wykonywane algorytmem 256 bitowym lub mocniejszym,
* klucz musi mieć minimum 12 znaków (w tym litery, cyfry i znaki specjalne),
* klucz znakowy musi być zabezpieczony przed dostępem osób nieuprawnionych poprzez zdeponowanie w miejscu, do którego dostęp jest monitorowany i ściśle ewidencjonowany,
* raz użyty klucz znakowy nie może być wykorzystany ponownie.
  1. Przechowywanie nośników danych:
     1. W przypadku przechowywania danych osobowych (nośników) poza obszarem wyznaczonym jako obszar przetwarzania danych osobowych, dane te powinny być zabezpieczone środkami dodatkowymi w celu zachowania poufności i integralności.
     2. Urządzenia lub/i nośniki danych, w tym również kopie zapasowe i archiwalne należy przechowywać w wydzielonym pomieszczeniu i/lub szafie/sejfie w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
     3. Warunki środowiskowe przechowywania nośników są zgodne z wytycznymi producentów nośników i urządzeń.
     4. Kopie zapasowe usuwa się (niszczy) niezwłocznie po ustaniu ich użyteczności.
     5. W przypadku jeśli dostęp do nośników ma więcej niż jedna osoba zaleca się, aby wprowadzony system kontroli dostępu zapewniał identyfikacje, autoryzację oraz rozliczalność osoby.
  2. Zabrania się wynoszenia urządzeń i/lub nośników danych poza obszar zidentyfikowany jako obszar przetwarzania danych bez zgody Administratora Danych Osobowych.