**OKREŚLENIE ŚRODKÓW TECHNICZNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH –TECHNICZNE ŚRODKI OCHRONY DANYCH OSOBOWYCH**:

1. W Starostwie obowiązuje zasada czystego biurka. Polega ona na  zabezpieczeniu przed  dostępem osób nieuprawnionych wszelkich dokumentów zawierających dane osobowe oraz nośników danych znajdujących się na stanowisku pracy.
   * 1. W Urzędzie należy przestrzegać zasady czystego ekranu, polegającej na  zastosowaniu  zabezpieczenia przed nieupoważnionym użyciem urządzenia komputerowego pozostawionego bez nadzoru.
     2. W obszarze przetwarzania danych osobowych, monitory urządzeń komputerowych powinny być ustawione w sposób uniemożliwiający odczytanie danych przez  osoby  postronne.
     3. W momencie pozostawiania komputera bez nadzoru lub opuszczania pomieszczania biurowego, w którym znajduje się sprzęt komputerowy, należy zablokować to    urządzenie (w przypadku komputerów stacjonarnych z  zainstalowanym systemem   operacyjnym Microsoft Windows poprzez naciśnięcie klawiszy „Windows + L” albo „CTRL + ALT + Delete”, a następnie ENTER).
     4. W przypadku zakończenia pracy użytkownik zobowiązany jest do  zamknięcia aktywnych sesji, wylogowania się z systemu oraz upewnienia się, że urządzenie komputerowe zostało wyłączone.
     5. Komputerowe nośniki informacji, zawierające dane osobowe, które utraciły praktyczne znaczenie i – zgodnie z   przepisami powszechnie obowiązującymi oraz  wewnętrznymi – nośniki uszkodzone lub w złym stanie technicznym, podlegają  trwałemu komisyjnemu zniszczeniu.
     6. Hasła użytkowników wymagane do uwierzytelniania się w systemie podlegają szczególnej ochronie:

systemy wchodzące w skład systemu teleinformatycznego, które służą do przetwarzania danych osobowych, zabezpieczone są hasłem znanym tylko  osobie upoważnionej do przetwarzania danych osobowych;

oprogramowanie systemowe nie może przechowywać ani zapisywać hasła w postaci jawnego tekstu;

użytkownik systemu teleinformatycznego jest odpowiedzialny za zachowanie w tajemnicy wszelkich posiadanych haseł chroniących jego konta użytkownika w systemie teleinformatycznym (hasła należy utrzymywać w tajemnicy również po upływie ich ważności);

użytkownikom zabrania się zapisywania i pozostawiania haseł w miejscu, w  którym mogłyby zostać ujawnione osobom nieuprawnionym;

* + 1. użytkownikom zabrania się wpisywania haseł w obecności osób trzecich, jeśli mogą one zauważyć treść wpisywanego hasła;
    2. użytkownikom zabrania się ujawniania haseł bez względu na okoliczności (w szczególności nie należy go ujawniać przez telefon lub pocztę elektroniczną osobom, które mogą podawać się np. za pracowników pomocy technicznej).
    3. Osoby upoważnione do przetwarzania danych osobowych mają obowiązek przechowywania dokumentów i nośników informacji zawierających dane osobowe w  miejscach uniemożliwiających dostęp do nich osobom nieuprawnionym. Elektroniczne nośniki informacji i dokumenty papierowe zawierające dane osobowe   należy przechowywać w  obszarze przetwarzania danych osobowych w   zabezpieczonych pomieszczeniach w  szafach/sejfach/kasetkach zamykanych na  klucz.
    4. Za zabezpieczenie kluczy do szaf i szuflad, w których przechowywane są dane osobowe odpowiada pracownik.
    5. Wszelkie zbędne nośniki, na których zapisane są dane osobowe należy zniszczyć niezwłocznie i trwale, tzn. w sposób uniemożliwiający odzyskanie danych - niszczenie dokumentów w formie papierowej zawierających dane osobowe odbywa się w niszczarce.
    6. Klucze i hasła dostępu do pomieszczeń, w których przetwarzane są dane osobowe mogą być przekazane pracownikowi po podpisaniu oświadczenia:

o zachowaniu poufności (załącznik nr 3 do PBI);

o zapoznaniu się z dokumentacją SBI (załącznik nr 4 do PBI);

o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych, w  którym zobowiązuje się do zachowania w tajemnicy danych osobowych wraz  ze  sposobami ich zabezpieczenia (załącznik nr 5 do niniejszej Polityki).

* + 1. Zgodnie z Polityką Bezpieczeństwa Fizycznego Starostwa Powiatowego w Lublinie, dane osobowe są przetwarzane w pomieszczeniach II strefy pracowniczej i III strefy pracowniczej szczególnie chronionej. W II strefie pracowniczej przebywać mogą    osoby uprawnione przez Właściciela strefy. Obowiązuje zakaz pozostawiania  samych interesantów/gości w strefie pracowniczej  lub  pracowniczej szczególnie chronionej. Osoby z zewnątrz/przedstawiciele strony trzeciej mogą znajdować się   w  pomieszczeniu, w którym przetwarza się dane osobowe tylko  w  obecności pracownika Starostwa. Właściciel strefy, w  uzasadnionych przypadkach,  może    nałożyć dodatkowe restrykcje dotyczące przebywania w  strefie. Zasady  zabezpieczania, dostępu i pracy w  pomieszczeniach strefy III określane są przez Właścicieli tych stref. Strefa II i III chronione są przez     pracowników tych stref, poprzez    zastosowanie organizacyjnych i    technicznych   środków zapewniających poufność i integralność danych przetwarzanych w tych strefach. Zasady przydzielania uprawnień dostępu do  stref  oraz  zasady postępowania z  kluczami do pomieszczeń zostały opisane w rozdziale II ust. 2 i 3 Polityki Bezpieczeństwa Fizycznego.
    2. Pracownik ma obowiązek zamknąć na klucz drzwi do pomieszczenia biurowego stanowiącego obszar przetwarzania danych w przypadku opuszczania tego pomieszczenia (jeżeli  nie ma w pomieszczeniu innego pracownika uprawnionego do przebywania w nim).
    3. W przypadku pomieszczeń stanowiących obszar przetwarzania danych osobowych obowiązuje zakaz pozostawiania kluczy w drzwiach od strony zewnętrznej.