7. Jeżeli użytkownik otrzymał zgodę administratora na wykorzystanie prywatnego urządzenia elektronicznego lub prywatnego nośnika informacji, to korzystanie z niego jest dozwolone. Urządzenie musi być zabezpieczone przed nieuprawnionym dostępem osób postronnych.
8. Pracownik korzysta wyłącznie z pendrive dopuszczonych przez ADO lub ASI. Po wykorzystaniu danych osobowych przenoszonych na pendrive należy dane usunąć formatując nośnik lub przekazać ASI, który dokona usunięcia danych.

2.3. ŚRODKI TECHNICZNE OCHRONY DANYCH OSOBOWYCH

A. ŚRODKI SPRZĘTOWE, INFRASTRUKTURY INFORMATYCZNEJ I TELEKOMUNIKACYJNEJ.

1. Zbiory danych osobowych przetwarzane są przy użyciu komputerów stacjonarnych i przenośnych.
2. Komputery służące do przetwarzania danych osobowych są połączone z lokalną siecią komputerową.
3. Wykonywanie kopii systemów informatycznych / serwerów. Na potrzeby zachowania ciągłości działania systemów informatycznych i utrzymania integralności danych wykonuje się kopie zapasowe zbiorów danych. Zadanie to realizowane jest codziennie w dni robocze. Kopie awaryjne są wykonywane automatycznie przez dedykowane oprogramowanie poza godzinami pracy według ustalonego harmonogramu. Harmonogram zawiera również określenie jakie zasoby i systemy są kopiowane. Kopie tworzone są przyrostowo, tzn. kopiowane są pliki nowe i te których zawartość uległa zmianie. Kopie trafiają do „serwera backupu" (rozwiązanie zależne od wielkości jednostki) . Wyniki tworzenia kopii zapasowych są rejestrowane.
4. Zakres tworzenia kopii zapasowych obejmuje:
   a) Bazy danych zlokalizowane na serwerach
   b) Pliki i katalogi na serwerach
   c) Systemy operacyjne serwerów
   d) Pliki i katalogi wskazane przez administratora
5. Kopie zapasowe sporządza się również w następujących przypadkach:
   a) przed dokonaniem istotnej zmiany konfiguracyjnej (np. aktualizacji oprogramowania, ustawień systemowych),
   b) po przeprowadzeniu zmiany konfiguracyjnej (np. aktualizacji oprogramowania, ustawień systemowych, zmianie praw dostępu).
6. Kopie zapasowe, wykonane w danym dniu przechowywane są przez okres 2 miesięcy orazzabezpieczone są przed nieumyślnym skasowaniem, przy czym kopia danych z ostatniego dnia miesiąca jest przechowywana przez okres jednego roku a kopia z ostatniego dnia roku przez okres niezbędny wynikający z przepisów prawa np. dane rachunkowe 7 lat (5 lat + rok rozpoczęty + rok na poinformowanie przez US o wszczęciu postępowania.) Po ustaniu użyteczności kopii zapasowej jest ona niezwłocznie usuwana. Kopie zapasowe konfiguracji systemów operacyjnych serwerów wykonuje administrator systemu po każdej zmianie konfiguracji oprogramowania (np. po utworzeniu, rekonfiguracji lub usunięciu konta użytkownika w systemie, zmianie praw dostępu itp.)
7. Za prawidłowość tworzenia kopii zapasowych odpowiada administrator systemu.
8. Za wykonywanie kopii zapasowych danych znajdujących się na poszczególnych stacjach roboczych poza serwerownią odpowiadają użytkownicy tych stacji roboczych. Częstotliwość tworzenia kopii zapasowych na stacjach roboczych zależy od ilości i wagi przetwarzanych informacji. Niedopuszczalne jest przechowywanie kopii zapasowych na tych samych nośnikach, na których są one przetwarzane. Użytkownicy mogą zlecać administratorowi systemu wykonanie kopii przetwarzanych przez nich danych (np. kopii folderów osobistych skrzynek pocztowych).
9. Testowanie kopii zapasowych. Kopie zapasowe sprawdzane są okresowo pod kątem ich dalszej przydatności przez administratora systemu nie rzadziej niż raz na miesiąc. Polega to na testowym odtworzeniu zawartości kopii na innym urządzeniu. Administrator systemu sporządza notatkę po każdym teście. Po stwierdzeniu