nieprzydatności kopii zapasowych zbiorów nośnik zostaje pozbawiony danych lub wybrakowany w inny sposób uniemożliwiający dalszy odczyt informacji.

10. Odzyskiwanie z kopii zapasowych. Odzyskiwanie danych z kopii zapasowych jest wykonywane w następujących przypadkach:
    a) utraty całości lub części danych na serwerze
    b) utraty integralności całości lub części danych na serwerze
    c) w celu odtworzenia poprzedniej wersji danych
    d) na wniosek organu kontrolnego (np.: NIK)
    e) przy przenoszeniu danych na nowy serwer
11. Odzyskiwanie całego systemu informatycznego sprzętowej lub systemowej nośników danych uniemożliwiającej korzystanie z danego systemu.
12. Za odzyskiwanie danych z kopii zapasowych odpowiada administrator systemu jest wykonywane w wypadku awarii, na których jest on zlokalizowany.
13. Programy zainstalowane na stacjach roboczych stacjonarnych i na komputerach przenośnych obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich, zgodnie z posiadanymi licencjami.
14. Oprogramowanie może być używane tylko zgodnie z prawami licencji. Oprogramowanie typu Freeware, Shareware lub inne oprogramowanie dostarczane bez opłat jest uznawane jako nieautoryzowane, jeżeli nie otrzyma stosownej aprobaty ASI.
15. Przed zainstalowaniem nowego oprogramowania ASI lub inna upoważniona osoba, zobowiązana jest sprawdzić jego działanie pod kątem bezpieczeństwa całego systemu.
16. Sieć teleinformatyczna wykorzystywana do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu informatycznego.
17. Infrastruktura techniczna związana z siecią teleinformatyczną i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych.
18. Wdrażanie aplikacji i oprogramowania eksploatowanych systemów powinno być poprzedzone testami.
19. Należy zapewnić synchronizację zegarów wszystkich stosowanych systemów służących do przetwarzania danych osobowych z uzgodnionym, dokładnym źródłem czasu.

B. METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM.

1. Dostęp do zbiorów danych osobowych, które przetwarzane są na wydzielonej stacji komputerowej i komputerze przenośnym, zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła.
2. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
3. Identyfikator

1) Identyfikator nadaje Administrator Systemu Informatycznego.
2) Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

4. Hasło użytkownika

1) Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem, miesiącem oraz nazwą łatwą do odgadnięcia.
2) Użytkownicy powinni stosować hasła, które:
    a) są łatwe do zapamiętania, a trudne do odgadnięcia,
    b) nie są oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących właściciela konta (np. imię, nazwisko, numer telefonu, data urodzenia itp.),
    c) zawierają przynajmniej jedną dużą literę, jedną małą literę, jedną cyfrę lub znak specjalny.