8. Metody i środki uwierzytelniania w systemie informatycznym

1. Zabezpieczenie zasobów informacyjnych przed dostępem do nich osób niepowołanych wymaga podjęcia działań związanych zarówno z bezpieczeństwem fizycznym pomieszczeń, w którym znajdują się komponenty informatyczne, jak i z ochroną dostępu logicznego do samego systemu informatycznego.
2. Pomieszczenia, w którym znajduje się sprzęt informatyczny, powinny być zabezpieczony przed dostępem osób nieupoważnionych poprzez instalację odpowiednich zamków. Osoby niebędące pracownikami mogą przebywać w pomieszczeniu wyłącznie w asyście upoważnionego pracownika.
3. Użytkownicy systemu informatycznego są odpowiedzialni za zabezpieczenie powierzonych im informacji przed dostępem osób nieupoważnionych. Dotyczy wszelkich dokumentów w postaci papierowej, które podobnie jak przenośne nośniki danych (pendriv-y, CD-ROM-y), powinny być przechowywane w zamykanych szafach. Zaleca się, aby na stacjach roboczych użytkowników były otwarte tylko te aplikacje, które są przez nich w danej chwili użytkowane.
4. System informatyczny powinien umożliwiać pracę Użytkownikowi na wszystkich stanowiskach z tymi samymi uprawnieniami bez względu na ich umiejscowienie jak również możliwość ograniczenia pracy jedynie w godzinach pracy Użytkownika.
5. System informatyczny wyposażony jest w mechanizmy uwierzytelniania użytkownika oraz kontroli dostępu do tych danych.
6. Identyfikator wraz z jego imieniem i nazwiskiem wpisuje się do ewidencji osób upoważnionych do przetwarzania danych osobowych prowadzonej przez, ASI.
7. Identyfikator nie powinien być zmieniany, a po wyrejestrowaniu Użytkownika z Systemu informatycznego nie powinien być przydzielany innej osobie.
8. Użytkownik, który utracił uprawnienia dostępu do danych osobowych, należy bezzwłocznie wyrejestrować z Systemu informatycznego, w którym są one przetwarzane, unieważnić jego hasło oraz podjąć stosowne działania w celu zapobieżenia dalszemu dostępowi tego Użytkownika do danych osobowych.
9. W pomieszczeniach, w których przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w te dane.
10. Niepowtarzalny login oraz hasło jednorazowe jest przydzielone użytkownikowi przez ASI po nadaniu uprawnień do przetwarzania danych osobowych.
11. Hasło jednorazowe jest przekazane Użytkownikowi przez ASI w formie pisemnej.
12. Bezpośredni dostęp do danych Użytkownik uzyskuje po podaniu loginu i właściwego hasła.
13. Bezpieczne korzystanie z haseł wymaga implementacji podstawowych, opisanych poniżej zasad:
    A) hasło jest znane tylko użytkownikowi, któremu zostało przydzielone
    B) hasło nie jest udostępniane innym osobom (możliwe są wyjątki, np. wspólne hasła administracyjne, ale nawet w takich przypadkach zaleca się, aby każdy administrator dysponował oddzielnym kontem administracyjnym i oddzielnym hasłem)
    C) hasło jest przechowywane w bezpiecznym miejscu – najlepiej, jeżeli jest zapamiętane

D) hasła administracyjne są przechowywane w bezpiecznym miejscu dostępnym tylko osobom upoważnionym

E) w przypadku podejrzenia hasła użytkownik natychmiast zmienia hasło i musi poinformować o tym IOD oraz ASI, który podejmuje kroki w celu wyjaśnienia, czy hasło to nie zostało wykorzystane do nieuprawnionego dostępu do systemu informatycznego i czy na skutek tego nie zaistniały szkody

F) minimalna długość hasła powinna wynosić 8 znaków

G) hasło nie powinno być pojedynczym wyrazem

H) hasło nie powinno bezpośrednio nawiązywać do jego użytkownika (na przykład nie powinno być numerem jego telefonu, datą urodzenia, adresem itp.)

I) hasło powinno zawierać wielkie i małe litery, cyfry lub / i znaki specjalne (na przykład #, *, &), o ile jest to technicznie możliwe ze względu na aplikację wykorzystującą mechanizm haseł

J) w przypadku nadawania użytkownikowi po raz pierwszy uprawnień lub kasowania hasła ASI powinien wygenerować hasło tymczasowe, które powinno być zmienione przy pierwszym dostępie do aplikacji

K) hasła powinny być okresowo zmieniane przez użytkowników – zaleca się zmianę, co 90 dni w przypadku haseł chroniących do informacji zwykłych (możliwych do sklasyfikowania, jako informacje wewnętrzne) oraz co 30 dni w przypadku haseł chroniących dostęp do informacji wrażliwych, w tym danych osobowych – wymuszona zmiana hasła przez system.

L) zabronione jest używanie polskich znaków diaktrycznych (ą, ś, ć, ń, ż, ź, ę, ł, ó) w hasłach,

M) zabronione jest zapisywanie hasła w pobliżu miejsca pracy lub w postaci zapisu elektronicznego w pliku w komputerze

N) przy zmianie hasła użytkownik nie powinien wprowadzać, jako nowego hasła jednego z kilku poprzednich używanych (zaleca się, aby nowe hasło było różne od 4 ostatnich haseł)

O) aplikacje sprawdzające tożsamość przy pomocy hasła nie powinny wyświetlać go na ekranie monitora podczas wprowadzania przez użytkownika

P) wprowadzenie hasła nie powinno być zautomatyzowane na przykład poprzez przypisanie go klawiszowi funkcyjnemu

Q) w przypadku kilkukrotnego błędnego wprowadzenia hasła (3 razy) konto użytkownika powinno ulec zablokowaniu, może być ono odblokowane przez ASI.

14. Użytkownicy systemu informatycznego są niezwłocznie rejestrowani lub wyrejestrowywani przez ASI, gdy uzyskują lub tracą prawo dostępu do systemu.
15. Login po wyrejestrowaniu użytkownika zostaje zablokowany przez ASI.
16. Login po wyrejestrowaniu użytkownika nie jest przydzielany innej osobie.
17. Hasła do serwerów, aktywnych urządzeń sieci i istotnych programów konfiguracyjnych Administrator Systemu umieszcza w zapieczętowanych kopertach i składa. Otwarcie koperty może nastąpić w przypadku:

    A) zamiaru zniszczenia nieaktualnych haseł przez Administratora Systemu,

B) zaistnienia konieczności zapoznania się z jej zawartością spowodowanej rezygnacją z pracy, pozbawieniem uprawnień lub śmiercią Administratora Systemu; uprawnienie w tym zakresie posiada Administrator Danych Osobowych.