PROCEDURA POSTĘPOWANIA NA WYPADEK ZAISTNINEIA SYTUACJI KRYZYSOWEJ

CEL PROCEDURY

Celem procedury jest określnie zasad postępowania osób zatrudnionych na wypadek wystąpienia sytuacji kryzysowych.

ZAKRES PROCEDURY

Procedura dotyczy:

A) Lokalnego Administratora Bezpieczeństwa Informacji

B) Administratorów Systemów Informatycznych

C) Pracownik stwierdzający naruszenie

TRYB POSTĘPOWANIA

1. Przez sytuację kryzysową rozumiemy zdarzenia nagłe, trudne do przewidzenia, które może poważnie zagrozić bezpieczeństwu przetwarzanych informacji oraz spowodować uszkodzenia sprzętu komputerowego. Do takich zdarzeń zaliczamy: pożar, powódź lub zalanie pomieszczeń wodą, zwarcie instalacji elektrycznej, zawalenie się stropu, huragan, atak terrorystyczny, sabotaż.

2. Potencjalne zagrożenia jakie mogą wystąpić w wyniku zaistnienia sytuacji kryzysowej to:

- Uszkodzenie sprzętu komputerowego
- Uszkodzenie, zniszczenie lub utrata zasobów informatycznych
- Trwała lub czasowa utrata dostępu do zasobów informatycznych
- Nieuprawniona lub nieprawidłowa modyfikacja zasobów
- Udostępnienie zasobów osobom nieuprawnionym

1. Podstawowym celem działania wszystkich pracowników w sytuacji kryzysowej powinno być podjęcie zdecydowanych działań mających na celu:

- Przywrócenie sprawności sprzętu komputerowego
- Przywrócenie zasobów informatycznych do stanu sprzed sytuacji kryzysowej.
- Uniemożliwienie dostępu do zasobów osobom nieupoważnionym.

1. W przypadku pojawienia się sytuacji kryzysowej każdy z pracowników jest zobowiązany do postępowania według następujących zasad:

1. Natychmiast powiadomić o zaistniałej sytuacji kryzysowej Administratora Systemu Informatycznego, Lokalnego Administratora Bezpieczeństwa Informacji.

2. Powiadomić, w zależności od zaistniałej potrzeby, odpowiednie służby ki pogotowia zewnętrzne czyli policję, straż pożarną, pogotowie ratunkowe, pogotowie energetyczną, pogotowie gazowe, pogotowie wodno-kanalizacyjne, telekomunikację.

3. Wszyscy pracownicy zobowiązani są włączyć się do akcji zabezpieczenia zagrożonego sprzętu i zasobów informatycznych. Każdy pracownik powinien wykonywać ściśle polecenia przełożonych oraz osób kierujących akcją ratowniczą.

4. Nie czekając na działanie wyspecjalizowanych służb przystąpić do zabezpieczenia pomieszczeń i sprzętu objętych działaniem sytuacji kryzysowej. W szczególności w miarę możności, z zachowaniem przepisów BHP, wyłączyć zgodnie z instrukcją, pracujące serwery, a następnie wyłączyć całkowicie dopływ energii elektrycznej. Należy uniemożliwić dostęp do pomieszczeń osób postronnych lub nieupoważnionych. Jeżeli jest to możliwe należy usunąć ze strefy zagrożenia sprzęt komputerowy.

5. Po ustąpieniu zagrożenia pracownicy zobowiązani są w możliwie najkrótszym czasie, przystąpić do likwidacji szkód powstałych w wyniku zaistnienia sytuacji kryzysowej. Oznacza to przywrócenie sprawności sprzętu komputerowego oraz odtworzenie zasobów informatycznych w stanie sprzed sytuacji kryzysowej.

6. Ze względu na powagę zaistniałych zagrożeń oraz wielkość możliwych strat, osoby, które nie podporządkują się poleceniom przełożonych będą pociągnięte do odpowiedzialności służbowej lub karnej.

W przypadku perspektywy długiego przestoju systemu informatycznego należy powiadomić użytkowników systemu oraz Administratora Bezpieczeństwa Informacji.