

Załącznik nr 1
PROCEDUR ZARZĄDZANIA
INCYDENTAMI
CYBERBZEPÍECZEŃSTWA

INSTRUKCJA ZABEZPIECZANIA KOMPUTERÓW

1. Odsuń w sposób zdecydowany, ale taktowny całą obsługę od komputerów (mogą później być przydatni). Na czas zabezpieczenia zabroń im korzystania z urządzeń komputerowych i łączności.
2. Jeśli urządzenie jest wyłączone, NIE WŁĄCZAJ GO.
3. Jeśli urządzenie jest włączone, NIE próbuj zamykać programów ani wyłączać komputera. Nie przerywaj drukowania, zabezpiecz, jeśli to możliwe, wykonane wydruki. Zanotuj dokładnie wszystkie wiadomości, jakie pojawiają się na ekranie. Zanotuj wszystkie parametry połączeń komputera:
 - a) w przypadku połączenia modemowego, zanotuj numer telefoniczny, adres IP komputera, adresy bramki wychodzącej oraz serwera DNS,
 - b) w przypadku połączenia po sieci kablowej, zanotuj typ połączenia, adres IP komputera, adresy bramki wychodzącej oraz serwera DNS,
 - c) w przypadku połączenia po sieci bezprzewodowej, zanotuj ustawienia zabezpieczenia sieci adres IP komputera, adresy bramki wychodzącej oraz serwera DNS.
4. Przed zabezpieczeniem zanotuj, w jaki sposób poszczególne części stanowiska są ze sobą połączone. Zrób zdjęcia, wykonaj szkic (plan połączeń z opisem wyposażenia). Oznacz odpowiednio wszystkie przewody i połączenia.
5. Następnie ODŁĄCZ WSZYSTKIE KABLE ZEWNĘTRZNE KOMPUTERA. Zanotuj czas odłączenia kabli.
6. Zabezpiecz jednostkę centralną (komputer) oraz inne urządzenia z zainstalowaną na stałe pamięcią masową w wytrzymałych mechanicznie workach foliowych. ZAPŁOMBUI WOREK I WYPEŁNIJ METRYCZKĘ. Metryczka powinna zawierać typ, numer seryjny urządzenia i numer inwentarzowy nadany przez Urząd albo opis jego indywidualnych cech. Zapisz wszystkie wykonane czynności

7. Pakuj ostrożnie okablowanie i sprzęt (klawiatury, monitory, drukarki, plotery, skanery, czytniki kart i pamięci, napędy zewnętrzne itp.).
8. Zabezpiecz wszystkie wymienne nośniki komputerowe: pamięci flash, dyskietki, dyskietki ZIP, JAZZ, taśmy streamera, płyty CD, DVD, MO oraz niezamontowane dyski twarde (także uszkodzone). Grupy nośników pakuj zbiorczo (dyskietki, płyty CD itp.). PAKUJ, NUMERUJ poszczególne paczki, PLOMBUJ I OPISZ W PROTOKOLE. Wpisz do PROTOKOŁU wykonane czynności.
9. Zażądaj od użytkownika spisu oprogramowania zainstalowanego na komputerze, a następnie zgodnie ze spisem - okazania licencji i oryginalnych nośników oprogramowania lub wskazania miejsca przechowywania lub osoby upoważnionej, która zarządza licencjami i oryginalnymi nośnikami oprogramowania. Jeśli użytkownik nie ma spisu oprogramowania, to zażądaj okazania wszystkich posiadanych przez niego licencji i oryginalnych nośników oprogramowania. Oznaczenia licencji i nośników wpisz do protokołu, a następnie zabezpiecz jako materiał porównawczy. Wpisz do protokołu wykonane czynności.
10. Zażądaj od użytkownika przekazania instrukcji programów pisanych na zamówienie lub programów nietypowych. Zabezpiecz jako materiał porównawczy i wpisz do protokołu wykonane czynności.
11. Zażądaj od użytkowników i administratora podania parametrów dostępu do systemu operacyjnego i oprogramowania (kont, haseł, identyfikatorów, itp.), a następnie zabezpiecz je przed osobami postronnymi za pomocą bezpiecznej koperty. Wpisz czynność przejęcia parametrów dostępu do protokołu.
12. Przechowuj zabezpieczone materiały (nośniki i sprzęt) w miejscach suchych i chłodnych z daleka od urządzeń emitujących pole elektromagnetyczne, a bezpieczne koperty w sejfie.
13. Uwagi końcowe:
 - a) sprawdź przed odesłaniem zgodność numerów zabezpieczonych materiałów i dowodów z treścią protokołu (zwróć uwagę na puste pudełka i nośniki pozostawione w napędach komputerowych i innych urządzeniach);

- b) skontaktuj się z odpowiednią komórką organizacyjną Urzędu w celu zorganizowania przewozu
i badań zabezpieczonych materiałów.

PAMIĘTAJ: NIE PRÓBUJ SAMODZIELNIE BADAĆ KOMPUTERA, ANI ZAWARTOŚCI NOŚNIKÓW DANYCH. KAŻDE TWOJE WŁĄCZENIE KOMPUTERA PO ZAKOŃCZENIU ZABEZPIECZENIA WYWOŁUJE POWSTANIE ŚLADÓW WSKAZUJĄCYCH NA NARUSZENIE INTEGRALNOŚCI MATERIAŁU BADAWCZEGO.