Załącznik nr 1 do zapytania ofertowego

Minimalne wymagania dotyczące zabezpieczenia komputerów

1. Wejście i zmiana ustawień BIOS/UEFI powinna wymagać podania hasła.
2. Możliwość uruchamiania systemu z sieci lub innych nośników niż dysk twardy komputera powinna być wyłączona.
3. Długość hasła BIOS/UEFI: nie mniej niż 10 znaków (co najmniej 1 duża litera i 1 cyfra).
4. Zainstalowany i działający system zabezpieczający przed atakami zewnętrznymi typu firewall.
5. Wdrożone mechanizmy zapewniające bieżącą aktualizację systemu firewall.
6. Wdrożony i uruchomiony system aktualizacji systemu operacyjnego oraz jego składników.
7. Zainstalowane i działające oprogramowanie antywirusowe czasu rzeczywistego.
8. Wdrożone mechanizmy zapewniające aktualizację sygnatur antywirusowych nie rzadziej niż raz w tygodniu.
9. Wdrożone regulacje zapewniające pełne skanowanie antywirusowe co najmniej raz w tygodniu.
10. Wdrożony wymóg podania loginu i hasła przed uzyskaniem dostępu do danych umieszczonych na komputerze.
11. Hasło użytkownika powinno być zmieniane co 30 dni.
12. Hasło nie powinno być łatwe do odgadnięcia, to znaczy:
13. powinno składać się z minimum 8 znaków,
14. hasła nie mogą zawierać nazwy konta użytkownika ani części jego pełnej nazwy dłuższej niż dwa kolejne znaki,
15. hasła muszą zawierać znaki z trzech spośród następujących czterech kategorii:
16. wielkie litery alfabetu łacińskiego (od A do Z)
17. małe litery alfabetu łacińskiego (od a do z)
18. cyfry systemu dziesiętnego (od 0 do 9)
19. znaki niealfabetyczne (na przykład !, $, #, %)
20. Użytkownik jest zobowiązany do nie pozostawiania komputera bez nadzoru oraz nie udostępniania go osobom trzecim.
21. Bieżąca praca na komputerze powinna się odbywać z wykorzystaniem konta użytkownika nieposiadającego uprawnień administracyjnych chyba, że bieżąca praca tego wymaga.
22. Login i hasło do konta umożliwiającego dostęp do danych na komputerze lub poczcie elektronicznej nie mogą być przekazywane osobom trzecim.
23. Hasło powinno być chronione przed dostępem osób trzecich; w każdym przypadku gdy hasło zostało ujawnione innej osobie, użytkownik jest zobowiązany do jego zmiany.
24. Po skasowaniu danych należy opróżnić „kosz” systemowy.
25. W przypadku wątpliwości lub dodatkowych pytań związanych z zapewnieniem minimalnych wymagań dotyczących zabezpieczeń komputerów istnieje możliwość uzyskania wsparcia pod adresem it@ore.edu.pl.