INSTRUKCJA UŻYTKOWANIA KOMPUTERÓW PRZENOŚNYCH PRZEZ OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

Wielkopolskie Samorządowe Centrum Kształcenia Zawodowego i Ustawicznego w Gnieźnie z siedzibą przy ul. Mieszka I 27, 62-200 Gniezno

Data wprowadzenia:	27-11-2018 r.
Opracował:	Jacek Andrzejewski- inspektor ochrony danych
Zatwierdził:	Elżbieta Kabzińska- Dyrektor

1. Każdy Użytkownik komputera przenośnego typu laptop, będąc jednocześnie upoważnionym do przetwarzania danych osobowych w imieniu Wielkopolskiego Samorządowego Centrum Kształcenia Zawodowego i Ustawicznego w Gnieźnie (dalej: WSCKZiU), winien zapoznać się z niniejszą instrukcją użytkowania komputerów przenośnych, zobowiązując się jednocześnie do jej przestrzegania.

2. Użytkownik komputera przenośnego przed rozpoczęciem pracy na urządzeniu powinien zapoznać się z procedurami dotyczącymi ochrony danych osobowych które stanowią odrębne dokumenty zawierający wytyczne w zakresie bezpieczeństwa przetwarzania danych osobowych.

3. W przypadku przechowywania na komputerze przenośnym danych osobowych lub danych stanowiących tajemnicę przedsiębiorstwa Użytkownik zobowiązany jest do przechowywania ich na dysku szyfrowanym, zabezpieczonym co najmniej 8 znakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).

4. Na komputerach przenośnych przeznaczonych **do zewnętrznych prezentacji multimedialnych** nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub dane stanowiące tajemnicę instytucji.

5. W przypadku kradzieży, zagubienia lub zniszczenia komputera przenośnego, Użytkownik powinien niezwłocznie (maksymalnie do 2h) powiadomić o tym fakcie inspektora ochrony danych oraz Dyrektora, wskazując jednocześnie w miarę precyzyjnie jakiego rodzaju dane były na tym urządzeniu przechowywane.

6. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu i wynoszenia poza siedzibę WSCKZiU, a w szczególności:
    a. zaleca się przenoszenie go w specjalnym futerale zabezpieczającym przed uszkodzeniami mechanicznymi lub innymi czynnikami środowiskowymi.
    b. zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru.
    c. podczas poruszania się środkami komunikacji publicznej futerał z komputerem powinien znajdować się w rękach Użytkownika.

d. podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego pod siedzeniem kierowcy. Zabrania się przewożenia go np. na siedzeniach, co może skutkować kradzieżą na skrzyżowaniach, przejściach dla pieszych lub podczas zatrzymania pojazdu na dłuższą chwilę.

7. W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, **Użytkownik jest zobowiązany do przeanalizowania czy nie zachodzi potrzeba do stosowania kabla zabezpieczającego**. W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, szkoleń itp.

8. W przypadku pozostawiania komputerów przenośnych w biurze mieszczącym się w budynku WSCKZiU zaleca się umieszczanie ich po zakończeniu pracy w zamykanych na klucz szafkach.

9. Zgodnie z wewnętrznymi ustaleniami Użytkownik komputera przenośnego jest zobowiązany do przekazywania urządzenia informatykowi w celu wykonania kopii bezpieczeństwa danych.

10. Przed opuszczeniem biura o którym mowa w pkt. 8, Użytkownik powinien wykonać kopię ostatnich zmodyfikowanych lub utworzonych plików umieszczając je w specjalnym katalogu na „serwerze plików" lub na zewnętrznym dysku twardym. Po skopiowaniu danych nośnik ten powinien być odpowiednio zabezpieczony przed dostępem osób nieupoważnionych.

11. Bezwzględnie zabrania się udostępniania komputera innym osobom nieupoważnionym przez administratora do przetwarzania danego zakresu danych.

12. Zabrania się korzystania z niezabezpieczonych sieci Wi-Fi, publicznych punktów dostępu do Internetu typu HOT-SPOT, sieciach udostępnianych w miejscach publicznych takich jak restauracje, stacje paliw czy hotele.

13. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na monitorze

informacje przed wglądem osób nieupoważnionych. W tym celu może stosować filtry prywatyzujące lub w przypadku ich braku- zachować szczególną ostrożność i środki bezpieczeństwa w tym dostosować odpowiedni czas włączenia się wygaszaczy ekranu i automatycznej blokady systemu.