**DOBRE PRAKTYKI POMAGAJĄCE ZACHOWAĆ BEZPIECZEŃSTWO DANYCH**

**PODCZAS ZAJĘĆ ONLINE**

Zasady bezpieczeństwa, o których powinni pamiętać wykładowcy oraz studenci, przygotowując się do zajęć online, aby chronić swoje dane.

1. Na bieżąco aktualizuj systemy operacyjne.
2. Systematycznie aktualizuj programy antywirusowe, antymalware i antyspyware.
3. Regularnie skanuj stacje robocze programami antywirusowymi, antymalware i antyspyware.
4. Pobieraj oprogramowanie wyłącznie ze stron producentów.
5. Nie otwieraj załączników z nieznanych źródeł/od nieznanych nadawców dostarczanych poprzez korespondencję elektroniczną.
6. Nie zapamiętuj haseł w aplikacjach webowych.
7. Nie zapisuj haseł na kartkach.
8. Nie używaj tych samych haseł w różnych systemach informatycznych.
9. Zabezpieczaj sieci bezprzewodowe – Access Point.
10. Stosuj silne hasła: *co najmniej 8 znaków w tym duże i małe litery, cyfry oraz znaki specjalne*.
11. Unikaj wchodzenia na nieznane czy przypadkowe strony internetowe.
12. Nie loguj się do systemów informatycznych w przypadkowych miejscach z niezaufanych urządzeń lub publicznych niezabezpieczonych sieci Wi-Fi.
13. Wykonuj regularne kopie zapasowe.
14. Korzystaj ze sprawdzonego oprogramowania do szyfrowania e-maili lub nośników danych.
15. Szyfruj dane przesyłane pocztą elektroniczną. Np. przesyłane dane spakuj programem kompresującym Zip i zabezpiecz plik hasłem. Hasło do pliku przekaż inna drogą komunikacji.
16. Szyfruj dyski twarde w komputerach przenośnych.
17. Odchodząc od komputera, blokuj stację komputerową.
18. Nie umieszczaj w komputerze przypadkowo znalezionych nośników USB. Może znajdować się na nich złośliwe oprogramowanie.

*Opracowano na podstawie wytycznych UODO.*