Dekalog pracy zdalnej (+7 punktów)

Grupa wsparcia dla pracy zdalnej:
https://www.facebook.com/groups/241148550257024

1. Zanim zaczniesz pracę upewnij się, że masz zainstalowane wszystkie najnowsze aktualizacje do swojego systemu operacyjnego.
    a. Windows 10 aktualizujemy tak: https://www.laptopmag.com/articles/update-windows-10
    b. MacOS aktualizujemy tak: https://support.apple.com/pl-pl/guide/mac-help/mchlpx1065/mac

2. Upewnij się, że masz zaktualizowany program antywirusowy. Wystarczy ten wbudowany w Windows 10. Tutaj jest opis jak upewnić się, że jest włączony: https://support.microsoft.com/en-us/help/17464/windows-10-help-protect-my-device-with-windows-security

3. Każdy student i pracownik może skorzystać z narzędzi G Suite for Education dostępnych w centralnej umowie UW z Google, np.: poczta elektroniczna - mail.google.com; wideokonferencje - meet.google.com; wirtualna tablica - classroom.google.com. Informacje jak aktywować konta studenckie i pracownicze są dostępne na it.uw.edu.pl.
4. Podłącz sobie Google Drive (każdy pracownik UW ma do niego dostęp przez konto Poczty UW) i rób tam backup danych. Dodatkowo możesz zainstalować oprogramowanie Google Drive (https://www.google.com/drive/download/) i będziesz miał dostęp do swoich plików jakby były na Twoim komputerze.
5. Nie klikaj w dziwne i podejrzane linki np. informacje o zajęciu oszczędności w związku z wirusem czy zablokowaniu konta. Pamiętaj, administrator nigdy nie poprosi Cię o podanie hasła. W razie obaw wyszukaj tą informację w Internecie albo zapytaj na grupie.
6. Zwracaj uwagę na certyfikaty stron które odwiedzasz - “zielone kłódeczki” - szczególnie jak podajesz na nich swoje dane.
7. Gdy jesteś zalogowany do VPNa (https://it.uw.edu.pl/pl/uslugi/UslugiInternetVPN/) i masz dostęp do aplikacji UW (np. USOS, dyski sieciowe) nie dawaj dostępu do komputera innym osobom.
8. Ustaw hasło na swojego użytkownika i odchodząc od komputera zawsze blokuj ekran (WinKey + L / Control-Command-Q).
9. Upewnij się, że sieć bezprzewodowa do której się łączysz ma bezpieczne hasło, a oprogramowanie na routerze jest aktualne. Jeżeli nie wiesz jak to zrobić - zapytaj na grupie.
10. Korzystając z ogólnodostępnych sieci koniecznie używaj VPN (https://it.uw.edu.pl/pl/uslugi/UslugiInternetVPN/). Dzięki temu cały Twój ruch sieciowy będzie szyfrowany.

11. Jeśli przetwarzasz dane osobowe, dane finansowe lub inne informacje wrażliwe to po zakończonej pracy zabezpiecz je, zwłaszcza, gdy z komputera korzystają inni domownicy.
12. Do pracy zdalnej na domowym komputerze załóż sobie osobnego użytkownika, zabezpieczonego hasłem. Nie ma co mieszać życia prywatnego z zawodowym.
13. Do prowadzenia wideokonferencji, zdalnych wykładów itp. stosuj narzędzia uruchomione przez UW lub narzędzia na które UW ma podpisane umowy. Gdy stosujesz narzędzia dostępne publicznie, których nie mamy uregulowanych umowami, narażasz się na wątpliwości np. dotyczące ochrony danych osobowych.
14. Każdy student i pracownik może skorzystać z centralnej platformy UW do e-zajęć - kampus.come.uw.edu.pl. Studenci i pracownicy logują się kontami USOSweb.
15. Jeśli Twój Wydział korzysta z dedykowanych Wydziałowi narzędzi lub dedykowanych Wydziałowi umów na korzystanie z narzędzi, upewnij się, że Wydział potwierdza, że można ich używać do oficjalnych spotkań, zajęć, egzaminów.
16. Jeżeli nadal masz jakieś obawy lub wątpliwości - pytaj swój dział IT albo napisz na grupie. Lepiej zapytać niż potem mieć problem - better safe then sorry :)
17. Tworząc konferencję na Google Meet pamiętaj, żeby wybrać losową nazwę pokoju (najlepiej niech Google sam ją ustawi) - inaczej może się okazać, że wybrałeś nazwę już przez kogoś używaną i traficie do tego samego pokoju rozmów