Załącznik do pisma z dnia 21.12.2020 r.

Wybrane metody obniżania ryzyka udostępnienia danych osobowych:

1. Szkolenie z zakresu ochrony danych osobowych. Każdy z pracowników w ramach obowiązków pracowniczych jest zobowiązany do wzięcia udziału w takim szkoleniu i podpisaniu stosownego oświadczenia. Kurs jest dostępny dla każdego pracownika na platformie COME: https://kampus-pracownik.ckc.uw.edu.pl/course/view.php?id=39 Kurs on-line można zrealizować w dogodnym dla siebie czasie.

2. Dobra znajomość narzędzi teleinformatycznych m.in. programów komputerowych, aplikacji używanych do badań i dydaktyki, mediów społecznościowych itp. wykorzystywanych w pracy zawodowej. Osoby pragnące podnieść swoje kwalifikacje mogą skorzystać z oferty szkoleń UW, które organizuje m.in. ZIP.

3. W miejscu wykonywania obowiązków zawodowych stosujemy zasadę "czystego biurka". Papierowe dokumenty trzymamy poza zasięgiem wszystkich interesantów. Monitory muszą być odwrócone tyłem do interesantów i osób postronnych. Ta sama zasada dotyczy tzw. „czystego pulpitu".

4. Stosowanie bezpiecznych haseł i tam gdzie jest to możliwe należy zastosować dwuskładnikowe uwierzytelnianie. Komputery, na których Państwo przetwarzacie dane osobowe, powinny być bezwzględnie zabezpieczone przed dostępem osób nieupoważnionych. Szczegółowe instrukcje ustawienia hasła do komputera są dostępne pod adresem: https://wdib.uw.edu.pl/ochrona-danych/haslo

5. Odchodząc od stanowiska zawsze blokujemy komputery wciskając klawisze **Windows+L** na klawiaturze.

6. Odradzamy drukowania dokumentów z wrażliwymi danymi na drukarkach w innych pokojach (także tej w dziekanacie).

7. Zewnętrzne nośniki na pamięci takie jak dyski, pendrive, karty pamięci, płyty CD/DVD/BlueRay powinny być zaszyfrowane. W przypadku systemu operacyjnego Windows można użyć systemowo wbudowanej funkcji BitLocker. Nie wolno nagrywać żadnych dokumentów zawierających dane osobowe na nośnikach zewnętrznych, które nie są zaszyfrowane. Szczegółowe instrukcje szyfrowania nośników zewnętrznych są dostępne pod adresem: https://wdib.uw.edu.pl/ochrona-danych/szyfrowanie

8. Komputery przenośne, smartfony, tablety nie powinny być pozostawiane bez nadzoru w miejscach, w których są narażone na kradzież. Zaleca się równolegle zabezpieczyć tego typu urządzenia poprzez zaszyfrowanie ich zawartości. W przypadku systemów Windows można włączyć funkcję BitLocker. Szczegółowe instrukcje szyfrowania laptopów, smartfonów, tabletów są dostępne pod adresem: https://wdib.uw.edu.pl/ochrona-danych/szyfrowanie

9. Należy absolutnie unikać logowania do uczelnianych systemów teleinformatycznych takich jak: USOSweb, APD, Ankieter, Poczta UW itp. na publicznie dostępnych komputerach. Powyższe dotyczy także komputerów znajdujących się w salach dydaktycznych.

10. Należy absolutnie unikać zachowywania danych do logowania w przeglądarkach internetowych albo zapisywania loginów i haseł w łatwo dostępnych miejscach np. w plikach tekstowych.

11. Należy zakładać hasła do plików zawierających dane osobowe. Taką możliwość posiadają np. pliki pakietu MS Office.

12. Zaleca się na bieżąco podnosić kwalifikacje w zakresie umiejętności korzystania z komputerów i oprogramowania.

Działania zabronione, których należy się bezwzględnie wystrzegać:

1. Zabronione jest ujawnianie osobom niepowołanym nazw użytkowników (loginów) i haseł do posiadanych kont i systemów teleinformatycznych.

2. Zabronione jest podłączenie komputera do przypadkowych lub publicznych sieci komputerowych.

3. Zabronione jest podłączanie nieznanych urządzeń, w tym nieznanych nośników pamięci do komputera na którym są przetwarzane dane osobowe.

4. Nie wolno przetwarzać żadnych danych na komputerze (urządzeniu), które nie posiada oryginalnego i legalnego oprogramowania (systemu operacyjnego i programów) oraz aktualnego oprogramowania antywirusowego.

5. Nie wolno na komputerze na którym przetwarzamy dane osobowe uruchamiać programów nieznanego pochodzenia. W razie wątpliwości proszę się skontaktować z **Marcinem Roguskim (mt.roguski@uw.edu.pl)**.

6. Nie wolno klikać w podejrzane linki i nieznane załączniki, które pojawiają się w skrzynce pocztowej.

7. Nie wolno udostępniać własnego komputera osobom trzecim – nawet na chwilę.

8. Nie wolno udostępniać zdalnego pulpitu osobom trzecim.

9. Nie wolno wysyłać do kogokolwiek plików i informacji dostępnych na komputerze do osób nieupoważnionych do przetwarzania informacji zawartych w tych plikach.

10. Nie wolno podawać danych logowania dla systemów Uniwersytetu (logowanie PESEL-em czy Active Direvctory) do stron nieznajdujących się w domenie uw.edu.pl.

11. Należy wystrzegać się zapisywania danych dostępowych do systemów w miejscach ogólnodostępnych. Jeżeli nie da się tego uniknąć, nie kojarzymy jednoznacznie hasła z usługą, której ono dotyczy albo stosujemy system „kodowania" haseł w sobie znany sposób (np. przed podmienianie lub dopisywanie liter.