Uniwersytet
Humanistyczno-Przyrodniczy
im. Jana Długosza
w Częstochowie

KOMUNIKAT Nr R021.2.15.2020
REKTORA UNIWERSYTETU HUMANISTYCZNO –PRZYRODNICZEGO
IM. JANA DŁUGOSZA W CZĘSTOCHOWIE
z dnia 31 marca 2020r.
w sprawie
OCHRONY DANYCH OSOBOWYCH
PODCZAS PRACY ZDALNEJ

Porady dotyczące bezpieczeństwa danych osobowych podczas pracy poza Uczelnią.

Urządzenia

1. Urządzenia i oprogramowanie przekazane przez pracodawcę do pracy zdalnej służą **tylko do wykonywania obowiązków służbowych**.
2. Nie instaluj dodatkowych aplikacji i oprogramowania niezgodnych z polityką bezpieczeństwa Uczelni.
3. Upewnij się, że wszystkie urządzenia z jakich korzystasz mają **niezbędne aktualizacje** systemu operacyjnego (IOS lub Android), oprogramowania oraz systemu antywirusowego.
4. Zanim przystąpisz do pracy, **wydziel sobie odpowiednią przestrzeń**, tak aby ewentualne osoby postronne nie miały dostępu do dokumentów, nad którymi pracujesz.
5. Odchodząc od stanowiska pracy każdorazowo **blokuj urządzenie**, na którym pracujesz.
6. Zabezpieczaj swój komputer poprzez używanie **silnych haseł dostępu**, wielopoziomowe uwierzytelnianie. Pozwoli to na ograniczenia dostępu do urządzenia, a jednocześnie na ograniczenia ryzyka utraty danych w przypadku kradzieży lub zgubienia urządzenia.
7. Podejmij szczególne środki, aby urządzenia z których korzystasz podczas pracy, szczególnie te wykorzystywane do przenoszenia danych, jak dyski zewnętrzne nie zostały zgubione.
8. Jeśli zgubiłeś urządzenie, na którym pracujesz lub zostało ono skradzione natychmiast podejmij odpowiednie kroki, aby o ile to możliwie, **zdalnie wyczyścić jego pamięć**.
9. Zadbaj aby przechowywane dane były **w bezpieczny sposób zarchiwizowane**.

Email

1. Postępuj zgodnie z obowiązującymi w Uczelni zasadami dotyczącymi korzystania ze służbowej poczty elektronicznej (e-mail).
2. Używaj przede wszystkim **służbowych kont e-mail**.
3. Jeśli pracujesz przetwarzając dane osobowe i musisz używać prywatnego e-maila, upewnij się, że treść i załączniki są **właściwie szyfrowane**. Unikaj używania danych osobowych lub poufnych informacji w temacie wiadomości.
4. Przed wysłaniem maila upewnij się, że wysyłasz go do **właściwego adresata**, zwłaszcza jeśli wiadomość zawiera dane osobowe lub dane wrażliwe.

5. Dokładnie sprawdź nadawcę maila. **Nie otwieraj wiadomości od nieznanych adresatów**, a zwłaszcza nie otwieraj załączników oraz nie klikaj w link zawarty w takiej wiadomości. To może być atak phishingowy.
6. Nie przesyłaj mailem informacji zaszyfrowanej razem z hasłem. Nawet w osobnej wiadomości. Ten kto ma dostęp do Twojej poczty bez problemu odszyfruje wiadomość.

Na podstawie Protecting Personal Data When Working Remotely przygotowanego przez DPC Ireland.

Rektor
Uniwersytetu Humanistyczno-Przyrodniczego
im. Jana Długosza w Częstochowie

Prof. dr hab. Anna Wypych-Gawrońska