**ZALECENIA DOTYCZĄCE OCHRONY DANYCH PODCZAS WIDEOKONFERENCJI**

**Członkowie Wspólnoty Uczelni są zobowiązani do przestrzegania poniższych zaleceń, służących do zapewnienia bezpieczeństwa danych osobowych**

**I. Przed rozpoczęciem wideokonferencji**

1. Należy się upewnić się, że osoby postronne nie mają dostępu do ekranu.
2. Należy zabezpieczyć sieć Wi-Fi silnym hasłem.
3. Przed udostępnieniem swojego ekranu podczas rozmowy należy zamknąć wszystkie okna, tak aby inni uczestnicy konferencji ich nie zobaczyli.
4. Przy podłączeniu się do telekonferencji należy korzystać z kodów dostępu/PIN-ów.

**II. W trakcie korzystania z wideokonferencji**

1. Należy używać służbowy adres e-mail.
2. Należy używać innego hasła, niż używane w innych usługach.
3. Nie należy udostępniać linków do konferencji w mediach społecznościowych.
4. Należy włączyć, jeśli to możliwe, domyślną ochronę hasłem spotkania on-line.
5. Należy zarządzać opcjami udostępniania ekranu.
6. Nie należy udostępniać dokumentów służbowych, za pomocą czatu, który może być publiczny.
7. Należy korzystać, jeżeli to możliwe, z opcji zamazywania tła (tak, żeby rozmówcy nie widzieli otoczenia).
8. Należy korzystać z opcji „poczekalnia” tak, abyś można było kontrolować osoby uczestniczące w telekonferencji. W ten sposób uniknie się przypadkowych lub niechcianych osób.
9. Logując się do telekonferencji należy wyłączyć mikrofon i kamerę oraz włączyć je , gdy będzie to potrzebne.

**III. Po skorzystaniu z wideokonferencji**

1. Należy wyłączyć mikrofon i kamerę.
2. Należy upewnić się, że zakończyło się spotkanie on-line i zamknięto aplikację.
3. Należy sprawdzić, czy program do telekonferencji nie działa w tle.

Opracowano na podstawie: PUODO, Jak bezpiecznie korzystać z wideokonferencji? https://uodo.gov.pl/pl/138/1525 [dostep 20.05.2020]