



Procedura postępowania z urządzeniami mobilnymi (telefony, laptopy, tablety itp.).

1. Po co ta procedura?

Celem procedury jest określenie zasad postępowania z **komputerami, urządzeniami mobilnymi (telefonami) oraz nośnikami przenośnymi** zawierającymi dane osobowe. Chodzi o to, aby zapisane na nich informacje nie dostały się do osób nieuprawnionych do jej otrzymania (zasada poufności), a także, aby nie dopuścić do dokonania nieautoryzowanych zmian w danych przez nieuprawnione osoby lub procesy (zasada integralności), albo do przypadkowego utracenia, zniszczenia itp. (naruszenie ochrony danych wg RODO).

2. Kto odpowiada za przestrzeganie procedury?

Za przestrzeganie zasad wymienionych w niniejszej procedurze odpowiadają użytkownicy takich urządzeń mobilnych.

3. Co należy do Ciebie?

1. Jeśli korzystasz ze sprzętu mobilnego powierzonego przez pracodawcę, to odpowiadasz za niego materialnie.
2. Nie możesz oddawać do używania sprzętu mobilnego nikomu poza Tobą – tak partnerowi życiowemu i dzieciom też.
3. Upewnij się, że Twoje urządzenie mobilne jest przygotowane do używania, co w szczególności polega na:
 - a) formalnym wydaniu urządzenia,
 - b) stosowania blokady kodem PIN lub hasłem/szyfrowanie dysku.
4. Niestety samodzielnie nie możesz instalować jakiegokolwiek oprogramowania lub aplikacji czy nakładek, chyba że dostaniesz na to pisemną zgodę działu IT.
5. Instalacji oprogramowania dokonuje dział IT.
6. Przypominamy, że niestety nie możesz do celów służbowych wykorzystywać prywatnych nośników oraz podłączać ich do urządzenia, które Ci przekazaliśmy.
7. Przypominamy, że nie możesz transferować jakichkolwiek danych z urządzenia służbowego na swoje urządzenie prywatne np. wysyłanie plików, e-maili, zdjęć, wiadomości sms itp. Z urządzenia służbowego do urządzenia prywatnego.
8. Przypominamy, że nie możesz robić kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonania obowiązków służbowych przez Ciebie. Wyjątkowo możesz kopiować dane, ale tylko na nośniki, które mogą być zaszyfrowane i zabezpieczone przed naruszeniem. Jeśli kopia nie będzie już konieczna, trwale ją zniszcz – czyli tak, żeby nie można było jej odczytać, a jeśli masz z tym problem, skontaktuj się z działem IT, on może to zrobić za Ciebie.

9. Wszelkie nośniki, które nie są Ci przydatne musisz przekazać celem zniszczenia do działu IT. Pod żadnym pozorem nie wyrzucaj ich do kosza na śmieci ani w firmie, ani w domu.

4. Jak transportować sprzęt mobilny?

1. Przede wszystkim zachowaj ostrożność i miej tzw. głowę na karku. To sprzęt, który zawiera dane osobowe i tajemnicę UIK, dlatego musisz o nim szczególnie myśleć.
2. Nie zostawiaj go w samochodzie, kiedy Cię w nim nie ma. A jeśli musisz, to w miejscu niewidocznym (takim miejscem nie jest fotel pasażera, tylna kanapa czy podłoga).
3. Nie zapomnij zabrać urządzenia z miejsca, w którym się znajdujesz np.: siedziba klienta, restauracja itp. Szczególnie dotyczy to telefonów.

5. Korzystanie z urządzenia poza UIK

1. Nie podłączaj urządzenia do sieci innych podmiotów lub Internetu (w tym tzw. HotSpotów). Korzystaj z tego połączenia, które Ci gwarantujemy np. Internet w telefonie komórkowym.
2. Nie zlecaj jakichkolwiek napraw i przeglądów urządzenia komukolwiek poza działem IT.
3. Nie zapisuj hasła w lub na urządzeniu (karteczki przylepne itp.).
4. O wszelkich nieprawidłowościach stwierdzonych w trakcie pracy, a także zaginięciu urządzenia poinformuj dział IT i ADO.

6. Praca zdalna

Zasady pracy zdalnej w UIK określa odrębna dokumentacja i procedury – Regulamin Pracy Zdalnej.