

REGULAMIN

korzystania ze służbowych urządzeń mobilnych

I. Wprowadzenie

1. Niniejszy regulamin określa zasady korzystania ze służbowego sprzętu i obowiązuje każdego użytkownika sprzętu bez wyjątku.
2. W Regulaminie pod określeniem „użytkownik” należy rozumieć zarówno osoby zatrudnione w ramach stosunku pracy, jak i współpracowników, na stałe wykonujących zadania w ramach umów cywilnoprawnych, które korzystają ze służbowego sprzętu elektronicznego.
3. Przez „pracodawcę” należy rozumieć zarówno pracodawcę, jak i zlecającego usługi. Pracodawca jest podmiotem, który powierza użytkownikowi sprzęt służbowy.
4. Użytkownik ma obowiązek wykorzystywać do realizowania powierzonych mu zadań służbowe urządzenia mobilne powierzone przez pracodawcę, tzn. telefon, smartfon, laptop, tablet lub inne urządzenia elektroniczne.
5. Korzystanie z prywatnych urządzeń jest dopuszczalne tylko i wyłącznie po otrzymaniu wcześniejszej, udokumentowanej zgody pracodawcy.
6. Właściwe użytkowanie służbowych urządzeń mobilnych ma duże znaczenie dla bezpieczeństwa zasobów informacyjnych w organizacji.
7. Złamanie zasad określonych w Regulaminie lub niedostosowanie się do postanowień niniejszego Regulaminu może stanowić naruszenie obowiązków pracowniczych. W przypadku osób realizujących zadania w oparciu o umowy cywilnoprawne postępowanie niezgodnie z niniejszym Regulaminem może oznaczać wykonanie zadania niezgodnie z przedmiotem umowy i z wymaganą przez pracodawcę starannością i zawodowym profesjonalizmem i skutkować rozwiązaniem umowy, a także przewidzianymi w umowie karami umownymi.

II. Warunki korzystania z urządzeń mobilnych

1. Urządzenie mobilne powierzone przez pracodawcę jest przeznaczone do realizowania przez użytkownika powierzonych mu zadań i w takim celu należy je wykorzystywać.

2. Niedozwolone jest wykorzystywanie służbowych urządzeń mobilnych do prywatnych celów.
3. Użytkownikowi nie wolno pożyczać lub udostępniać powierzonego mu sprzętu innym osobom.
4. Użytkownik odpowiada za zapewnienie ochrony fizycznej powierzonych mu urządzeń mobilnych, gdy korzysta z nich poza siedzibą pracodawcy. W przypadku jego utraty lub zgubienia, użytkownik niezwłocznie zgłasza ten fakt pracodawcy. Następnie należy podjąć działania minimalizujące ryzyko negatywnych skutków zdarzenia, zgodnie z Procedurą postępowania w przypadku naruszenia ochrony danych osobowych oraz incydentu dla naruszenia bezpieczeństwa informacji.
5. Pracodawca powierza użytkownikowi sprzęt z zainstalowanym oprogramowaniem, które jest niezbędne do realizowania jego zadań. Użytkownik jest zobowiązany korzystać tylko i wyłącznie z oprogramowania zainstalowanego i dostarczonego przez pracodawcę. Zabronione jest samodzielne instalowanie oprogramowania, a w przypadku złamania zakazu użytkownik ponosi odpowiedzialność wynikającą zarówno z postanowień licencyjnych tego oprogramowania, jak i ewentualnego nieprawidłowego działania lub naruszenia bezpieczeństwa zasobów informacyjnych pracodawcy.
6. Pracodawca zapewnia na udostępnionych urządzeniach mobilnych zabezpieczenia, jak: program antywirusowy, automatyczne aktualizacje, zaporę sieciową, szyfrowanie, ograniczenie uprawnień. Zabronione jest ingerowanie w zabezpieczenia zainstalowane na urządzeniach.
7. Użytkownik niezwłocznie zgłasza pracodawcy wszelkie problemy techniczne, jak problemy związane z aktualizacją oprogramowania, błędy programu antywirusowego, podejrzane działania oprogramowania, itp.
8. Użytkownik korzystając z urządzeń mobilnych przestrzega zasad ochrony danych osobowych, wynikających z wewnętrznych polityk ochrony danych obowiązujących u pracodawcy.
9. Ze względu na bezpieczeństwo danych przechowywanych w służbowych urządzeniach mobilnych, zakazane jest podłączanie tych urządzeń do publicznych sieci WiFi (np. w hotelach, galeriach handlowych, środkach komunikacji publicznej, lotniskach) oraz sieci WiFi u kontrahentów (w przypadku wizyt służbowych u kontrahentów).

10. Użytkownik jest zobowiązany do zapewnienia poufności danych dostępowych do jego służbowych urządzeń mobilnych i do pracowania tylko i wyłącznie na swoim koncie użytkownika. Zabronione jest posługiwanie się cudzym loginem.
11. W przypadku używania zewnętrznych nośników danych (np. dysk zewnętrzny, CD, pendrive) użytkownik jest zobowiązany wykonać przed otwarciem zawartości urządzenia skanowanie nośnika programem antywirusowym.
12. Przekazywanie informacji poufnych, w tym danych osobowych drogą elektroniczną, wymaga uprzedniego zabezpieczenia hasłem tych informacji. Hasło w takim wypadku powinno zostać przekazane odbiorcy inną drogą komunikacji.
13. Niedozwolone jest podejmowanie pracy na służbowych urządzeniach mobilnych, gdy niezbędny jest dostęp do danych osobowych, w miejscach publicznych i ogólnodostępnych, jak kawiarnie, restauracje, galerie handlowe, gdzie osoby postronne mogłyby usłyszeć fragmenty służbowych rozmów lub zapoznać się z fragmentami wykonywanej pracy.
14. Pracując w domu użytkownik musi zapewnić, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu urządzenia, a także blokowanie go podczas zawieszenia pracy i wylogowanie po zakończeniu pracy.
15. Użytkownik przekazuje służbowe urządzenie mobilne do przeglądu na każde wezwanie wyznaczonego w Urzędzie Informatyka.
16. Służbowe urządzenie mobilne może zostać przekazane innemu użytkownikowi, tylko po uprzednim, skutecznym usunięciu z niego informacji, w tym danych osobowych. Za usunięcie danych na urządzeniach przeznaczonych do wtórnego użytku oraz ich przygotowanie do przekazania innemu użytkownikowi odpowiada wyznaczony w Urzędzie Informatyk.
17. Użytkownik nie jest uprawniony do samodzielnego przekazania urządzenia innemu użytkownikowi.
18. Korzystanie z programów służących do przetwarzania danych osobowych na służbowych urządzeniach mobilnych odbywa się po uwierzytelnieniu użytkownika do tego programu. Konieczność zabezpieczenia aplikacji poprzez dodatkowe hasło dostępu, dotyczy także smartfonów, gdzie może być niezbędne ręczne ustawienie konieczności podania dodatkowego hasła do aplikacji. Wsparcia w zakresie konfiguracji ustawień udziela wyznaczony w Urzędzie Informatyk, jednakże to

użytkownik odpowiada za nadzór, aby na użytkowanych przez niego urządzeniach zostały spełnione wskazane warunki bezpieczeństwa dostępu do aplikacji.

III. Bezpieczeństwo korzystania z Internetu

1. W biurze użytkownik powinien korzystać ze służbowej sieci internetowej.
2. Poza Urzędem użytkownik powinien korzystać z dostępu do Internetu zapewnionego przez pracodawcę w ramach dostarczonych narzędzi służbowych, tzn. modem, router, punkt HotSpot udostępniony ze służbowego urządzenia, itp.
3. Użytkownik informuje pracodawcę, jeżeli do prawidłowego użytkowania służbowych urządzeń mobilnych jest niezbędne udostępnienie mu narzędzi do bezpiecznego łączenia się z Internetem.
4. Zabronione jest korzystanie z publicznych sieci WiFi.
5. Dopuszczalne jest korzystanie z domowej sieci WiFi, jednakże pod wskazanymi warunkami:
 - a) Korzystanie z Internetu wymaga uwierzytelnienia, np. poprzez hasło,
 - b) Hasło dostępu spełnia warunki, jakie stawia hasłom wewnętrzna polityka ochrony danych u pracodawcy.
 - c) Login do panelu administracyjnego routera został zmieniony z domyślnego na własny.
 - d) Dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej.
 - e) Został zmieniony domyślny adres routera (najczęściej 192.168.1.1.) na inny.
6. Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udziela wyznaczony w Urzędzie Informatyk.