

§ 1. Miejsce świadczenia pracy zdalnej

1. Pracownik musi zapewnić warunki umożliwiające mu skuteczną pracę zdalną z zachowaniem właściwego poziomu bezpieczeństwa informacji.
2. Niedozwolone jest podejmowanie pracy zdalnej w miejscach publicznych, gdzie osoby postronne mogą zapoznać się z treścią wykonywanej pracy lub służbowych rozmów.
3. Wykonywanie pracy zdalnej nie zwalnia pracownika z obowiązku przestrzegania postanowień Polityki Bezpieczeństwa Informacji wraz z dokumentami powiązanymi.

§ 2. Sprzęt

1. Pracownik może wykonywać pracę zdalną wyłącznie z wykorzystaniem urządzeń służbowych.
2. Zabronione jest udostępnianie urządzeń służbowych innym osobom, np. domownikom.
3. Problemy z działaniem udostępnionego sprzętu należy zgłaszać do Wydziału Informatyki.
4. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie zgłosić zdarzenie do przełożonego, który poinformuje o tym Wydział Informatyki i Inspektora Ochrony Danych.

§ 3. Bezpieczeństwo danych elektronicznych

1. Niedozwolone jest korzystanie z publicznego dostępu do sieci Internet, w tym punktów HotSpot.
2. W przypadku korzystania z domowego łącza internetowego:
 - a. Panel administracyjny urządzenia dostępowego jest zabezpieczony hasłem o długości co najmniej 10 znaków,
 - b. Dostęp do bezprzewodowej sieci Wi-Fi jest zabezpieczony protokołem szyfrowania WPA2 lub WPA3,
 - c. Hasło dostępu do sieci Wi-Fi składa się z co najmniej 10 znaków.
3. Urządzenie do pracy zdalnej łączy się z zasobami Starostwa szyfrowanym połączeniem VPN.
4. Pracodawca może dodatkowo wprowadzić na urządzeniu inne zabezpieczenia, jak:
 - a. szyfrowanie dysku,
 - b. wyłączenie portów USB,
 - c. geolokalizacja,
 - d. oprogramowanie do monitorowania pracy.
5. W przypadku zakończenia lub przerwania pracy na urządzeniu, pracownik zobowiązany jest do jego zablokowania, aby uniemożliwić korzystanie z niego przez osoby postronne.

§ 4. Bezpieczeństwo dokumentów papierowych

1. Zgodnie z obowiązującym u pracodawcy zasadami wszystkie dokumenty zawierające informacje poufne, w tym dane osobowe, powinny być przechowywane w szafach zamykanych na klucz w siedzibie pracodawcy.
2. Obowiązuje ogólny zakaz zabierania dokumentów lub ich kopii poza siedzibę pracodawcy.

3. Jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów papierowych, pracownik zgłasza do pracodawcy prośbę o możliwość ich skopiowania oraz zabrania do domu na czas wykonywania pracy zdalnej.
4. Po otrzymaniu zgody na piśmie lub w formie służbowej wiadomości e-mail, pracownik może sporządzić kopie niezbędnych dokumentów.
5. Zabronione jest zabieranie poza siedzibę pracodawcy oryginałów dokumentów.
6. Po skopiowaniu dokumentów pracownik przygotowuje ich zestawienie, zawierające informacje jakie dokumenty, w jakiej liczbie zostały skopiowane.
7. Informacja jest przekazywana pracodawcy.
8. Podczas przewożenia dokumentów do miejsca realizowania pracy zdalnej, należy zachować szczególną ostrożność, aby ich nie zgubić.
9. Praca z dokumentami nie może być wykonywana w miejscu publicznym (świetlica w szkole, kawiarnia, restauracja, galeria handlowa, itp.)
10. Poza czasem pracy, dokumenty powinny być przechowywane w zamkniętej na klucz szafie, szufladzie, itp.
11. Po zakończeniu pracy, wszystkie dokumenty należy zwrócić pracodawcy, który weryfikuje ich kompletność.