**Instrukcja ochrony danych osobowych w trakcie pracy zdalnej**

**1.** Niniejsza Instrukcja określa zasady bezpieczeństwa informacji i danych osobowych w trakcie pracy zdalnej.

**2.** Pracodawca przeprowadza, w miarę potrzeb, instruktaż i szkolenie w tym zakresie dla pracowników wykonujących pracę zdalną.

**3.** Pracownicy podczas pracy zdalnej mogą przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.

**4.** Pracownik w trakcie pracy zdalnej zobowiązany jest dbać o bezpieczeństwo danych, ich poufność oraz integralność. Na pracowniku ciąży obowiązek dbałości o dobro zakładu pracy w przypadku postępowania z danymi osobowymi w trakcie pracy zdalnej.

**5.** Pracownik zobowiązany jest natychmiastowo powiadomić Sekcję IT oraz bezpośredniego przełożonego o jakimkolwiek incydencie związanym z wyciekiem danych, zarówno w formie elektronicznej, jak i papierowej, jak również o kradzieży lub zaginięciu powierzonego mu sprzętu.

**Bezpieczeństwo pracy na komputerze**

1. Instalowanie jakiegokolwiek oprogramowania na laptopie służbowym jest możliwe tylko przez pracowników Sekcji IT lub za ich zgodą i zgodnie z ich wytycznymi.
2. Na laptopie służbowym ani na telefonie służbowym nie może być instalowane żadne nielegalne oprogramowanie.
3. Pracownik odpowiada za zabezpieczenie sprzętu służbowego przed dostępem osób trzecich, a w szczególności domowników i dzieci.
4. Pracownik nie może przechowywać żadnych danych ani informacji na innych nośnikach niż udostępnione mu przez ASP.
5. Zabronione jest używanie prywatnego sprzętu lub prywatnych kont pocztowych do przetwarzania danych osobowych. Sprawy służbowe mogą być załatwiane tylko przy użyciu laptopa służbowego oraz telefonu służbowego.
6. Pracownik nie może przechowywać na laptopie ani telefonie służbowym plików niezwiązanych z wykonywaną pracą lub jakichkolwiek innych plików lub programów, które nie posiadają stosownej licencji.
7. Pracownik nie może bez uzgodnienia z Sekcją IT instalować na telefonie służbowym ani na laptopie służbowym prywatnych aplikacji lub oprogramowania.
8. Pracownik odpowiada za ochronę powierzonego mu sprzętu służbowego, nie może korzystać z laptopa służbowego w miejscach publicznych.
9. Laptop służbowy oraz telefon służbowy chronione są hasłem, a laptopy dodatkowo są szyfrowane.
10. Hasła do poczty elektronicznej nie powinny być zapisywane przez przeglądarkę internetową.
11. Należy stosować silne hasła oraz menadżer haseł.
12. Pracownik powinien upewnić się, że sprzęt, z którego korzysta posiada aktualny i aktywny program antywirusowy.
13. Pliki wykorzystywane do bieżącej pracy należy zapisywać na okres pracy zdalnej na szyfrowanym lokalnym dysku lub we wskazanym przez Sekcję IT zasobie sieciowym.
14. Po zakończonej pracy należy wylogować się ze wszystkich usług i konta użytkownika,
a następnie wyłączyć i zabezpieczyć komputer.

**Bezpieczeństwo w sieci**

1. Pracownik powinien korzystać jedynie z zaufanego punktu dostępu do Internetu.
2. Pracownik powinien wykorzystywać funkcję hot-spot w telefonie służbowym, zawsze wtedy, gdy to możliwe.
3. Nie należy logować się do otwartych sieci Wi-Fi.
4. W razie potrzeb pracownik uruchamia VPN po zalogowaniu się do komputera.
5. Podczas korzystania z aplikacji chmurowych należy stosować zaufaną przeglądarkę.
6. Po zakończonej pracy należy wylogować się z usług chmurowych oraz zamknąć połączenie VPN.

**Bezpieczna komunikacja**

1. W komunikacji biznesowej należy wykorzystywać jedynie służbową skrzynkę pocztową.
2. Nie należy włączać przekierowań wiadomości e-mail ze skrzynki służbowej na skrzynkę prywatną.
3. Należy zwracać szczególną uwagę na otrzymywane maile – należy dokładnie czytać ich treść, linki otwierać dopiero po upewnieniu się, że są bezpieczne.
4. Należy szyfrować wiadomości e-mail zawierające dane osobowe.
5. Przy wysyłaniu wiadomości e-mail pracownik zobowiązany jest każdorazowo upewnić się co do poprawności wpisanych adresów mailowych jej adresatów.
6. Do celów służbowych nie należy używać komunikatorów dostępnych w sieci.

**Bezpieczne zarządzanie dokumentacją papierową**

1. 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.
2. Po otrzymaniu zgody na piśmie lub w formie służbowej wiadomości e-mail, pracownik może sporządzić kopie niezbędnych dokumentów.
3. Zabronione jest zabieranie poza siedzibę pracodawcy oryginałów dokumentów.
4. Po skopiowaniu dokumentów pracownik przygotowuje ich zestawienie, zawierające informacje jakie dokumenty, w jakiej liczbie zostały skopiowane
5. Informacja jest przekazywana pracodawcy.
6. Podczas przewożenia dokumentów do miejsca realizowania pracy zdalnej, należy zachować szczególną ostrożność, aby ich nie zgubić.
7. Praca z dokumentami nie może być wykonywana w miejscu publicznym (kawiarnia, restauracja, galeria handlowa, itp.).
8. Po zakończeniu pracy, wszystkie dokumenty należy zwrócić pracodawcy, który weryfikuje ich kompletność.
9. Jeśli nie jest to niezbędne do prawidłowego wykonywania powierzonych zadań nie należy drukować dokumentacji służbowej w domu oraz innych miejscach, gdzie wykonywana jest praca zdalna.
10. Jeżeli dokumentacja służbowa została wydrukowana, po skorzystaniu z niej należy zwrócić ją pracodawcy albo zniszczyć w domu lub po powrocie do placówki.
11. W przypadku skanowania dokumentów należy zapisywać je na szyfrowanym dysku lokalnym lub we wskazanym przez Sekcję IT zasobie sieciowym. W sytuacji skanowania dokumentów
z wykorzystaniem aplikacji na telefon należy usunąć plik z aplikacji lub folderu, w którym zeskanowany plik został zapisany.