załącznik 1 do Uchwały Zarządu nr 06/V/2023

Aneks nr 1 do dokumentu pn. „Polityka bezpieczeństwa danych osobowych”

Zasady ochrony informacji oraz danych osobowych w trakcie pracy zdalnej

1. Niedozwolone jest podejmowanie pracy zdalnej przy użyciu publicznych punktów dostępu do Internetu.
2. Każda osoba kierowana na pracę zdalną przechodzi obligatoryjne udokumentowane szkolenie prowadzone przez zakładowego inspektora ochrony danych/pracownika ds. informatycznych.
3. W przypadku korzystania z domowej sieci Wi-Fi, zaleca się skonfigurować router
w sposób minimalizujący ryzyko włamania, w szczególności:
a) korzystanie z Internetu powinno wymagać uwierzytelnienia, np. poprzez hasło;
b) hasło dostępu powinno składać się z co najmniej 16 znaków, w tym dużych i małych liter oraz cyfr i znaków specjalnych (tzw. silne hasło);
c) jeśli to możliwe, należy zmienić login do panelu administracyjnego routera na własny;
d) dostęp do panelu administratora routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej;
e) został zmieniony domyślny adres routera (najczęściej 192.168.1.1.) na inny;
4. Zabronione jest udostępnianie innym osobom, np. domownikom sprzętu, służbowego.
5. Zgoda na pracę zdalną obejmuje zgodę na korzystanie ze służbowego sprzętu poza siedzibą pracodawcy.
6. Przy wykonywaniu pracy zdalnej pracownik może używać narzędzi lub materiałów niezapewnionych przez pracodawcę pod warunkiem, że umożliwia to poszanowanie i ochronę informacji niejawnych/ poufnych oraz innych tajemnic prawnie chronionych, w tym tajemnicy przedsiębiorstwa lub danych osobowych, a także informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.
7. Urządzenie służbowe jest wydawane pracownikowi po potwierdzeniu jego odbioru podpisem pracownika.
8. Po otrzymaniu zgody na pracę zdalną pracownik niezwłocznie zgłasza ten fakt do Wydziału Informatyki.
9. Wydział Informatyki odnotowuje wydane urządzenia, które będą wykorzystywane przez pracownika do pracy zdalnej, a jeśli to niezbędne, przeprowadza ich przegląd.
10. Zalecane wymagania w zakresie bezpieczeństwa:
a) na urządzeniu jest legalne i aktualne oprogramowanie, w szczególności przeglądarka internetowa na komputerze prywatnym pracownika;
b) zostały włączone automatyczne aktualizacje;
c) została włączona zapora systemowa;
d) został zainstalowany i działa w tle program antywirusowy;
e) zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika, kod PIN, token.
11. Do pracy zdalnej pracownik powinien wykorzystywać wyłącznie służbowe programy/aplikacje oraz systemy udostępnione mu przez pracodawcę.
12. Jeżeli jest niezbędne przesłanie informacji o charakterze poufnym, w szczególności danych osobowych, muszą one zostać zabezpieczone silnym hasłem.
13. Jeżeli informacje niejawne/poufne będą przekazywane z wykorzystaniem poczty e-mail, muszą zostać udostępnione w załączniku zabezpieczonym silnym hasłem.
14. Zabezpieczeniu powinny podlegać wszelkiego rodzaju dane osobowe, niezależnie od ich charakteru.
15. Hasło powinno zostać przekazane odbiorcy inną drogą komunikacji.
16. Hasło zawsze powinno być odpowiednio skomplikowane i niesłownikowe.
17. Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą.
18. Rekomendowane metody zabezpieczania hasłem:

a) nadanie hasła do pliku, w którym są dane osobowe;
b) zabezpieczenie pliku lub plików poprzez kompresję z zabezpieczeniem archiwum wynikowego hasłem.
19. Każda wiadomość powinna być wysłana z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy.
20. W przypadku wysyłania informacji do kilku odbiorców, którzy nie znają się wzajemnie i/lub ich adresy e-mail są adresami prywatnymi, należy skorzystać z opcji Ukrytej kopii (UDW/BCC), tzn. adresy wpisać w to pole.
21. Pracownik może także przekazywać pliki z informacjami chronionymi po ich uprzednim zaszyfrowaniu (korzystając z narzędzi 7-zip lub AESCrypt) przed wysłaniem. Hasło szyfrowania musi spełniać wymagania polityki haseł i musi być przekazane adresatowi odrębnym kanałem przesyłu informacji.
22. Wykorzystywanie innych narzędzi do przesyłania i udostępniania plików (WeTransfer, Google Drive, DropBox) może odbywać się tylko po wcześniejszym zaszyfrowaniu plików jak opisano powyżej.
23. Jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów papierowych, pracownik zgłasza do bezpośredniego przełożonego prośbę o możliwość ich skopiowania oraz korzystania z kopii w miejscu świadczenia pracy zdalnej.
24. Po otrzymaniu zgody na piśmie lub w formie służbowej wiadomości e-mail pracownik może sporządzić kopie niezbędnych dokumentów.
25. W miejscu wykonywania pracy zdalnej zabronione jest korzystanie z oryginałów dokumentów.
26. Po skopiowaniu dokumentów pracownik przygotowuje ich pisemne zestawienie, zawierające informacje jakie dokumenty, w jakiej liczbie zostały skopiowane. Informacja jest przekazywana bezpośredniemu przełożonemu.
27. Należy zachować szczególną ostrożność podczas transportowania kopii dokumentów do miejsca realizowania pracy zdalnej.
28. Po zakończeniu pracy wszystkie kopie dokumentów należy zwrócić bezpośredniemu przełożonemu, który weryfikuje ich kompletność.
29. Pracownik wykonujący pracę zdalną jest zobowiązany do przestrzegania obowiązującej u pracodawcy polityki ochrony danych osobowych oraz powiązanych regulacji wewnętrznych.
30. Pracownik zobowiązany jest do zapewnienia właściwych warunków umożliwiających skuteczną pracę zdalną z zachowaniem należytego poziomu bezpieczeństwa danych/informacji.
31. Pracownik jest zobowiązany do zabezpieczenia sprzętu służbowego oraz posiadanych danych/informacji przed osobami postronnymi, w tym domownikami, w sposób uniemożliwiający dostęp/poznanie treści służbowych/skopiowanie w jakiejkolwiek postaci.
32. Niedozwolone jest:
a) udostępnianie innym osobom danych służących do uwierzytelniania do systemów i/lub usług;
b) przekazywanie informacji chronionych, w szczególności danych osobowych bez zabezpieczenia hasłem, zwłaszcza w treści wiadomości e-mail;
c) przekazywanie hasła do zabezpieczonych informacji tą samą drogą komunikacji, którą przekazywany jest zabezpieczony hasłem plik lub pliki;
d) drukowanie dokumentów służbowych w domu;
e) niszczenie dokumentów służbowych w domu;
f) fotografowanie ekranu z danymi/informacjami służbowymi oraz fotografowanie/skanowanie dokumentów służbowych w domu;
g) utrwalanie w jakikolwiek inny sposób danych/informacji służbowych na nośnikach prywatnych;
h) udostępnianie służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom;
i) dzielenie się informacjami niejawnymi/poufnymi z innymi osobami, w szczególności z domownikami;
j) jakiekolwiek logowanie się na konto innego użytkownika.

….....….....
(data i podpis)