ZARZĄDZENIE NR 120.12.2023
BURMISTRZA KAMIEŃSKA
z dnia 30 października 2023 r.

w sprawie wprowadzenia Regulaminu ochrony danych osobowych podczas wykonywania okazjonalnej pracy zdalnej oraz dokumentacji oceny ryzyka zawodowego i informacji zawierającej zasady bezpiecznego i higienicznego wykonywania pracy zdalnej w Urzędzie Miejskim w Kamieńsku

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2023 r., poz. 40 z późn. zm.) oraz art. 67^{26} i art. 226 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz.U. z 2023 r. poz. 1465) i § 39a rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy (t.j. Dz.U. z 2003 r. Nr 169, poz. 1650 z późn. zm.), zarządzam, co następuje:

§ 1. 1. Wprowadzam Regulamin ochrony danych osobowych podczas wykonywania okazjonalnej pracy zdalnej w Urzędzie Miejskim w Kamieńsku, który stanowi załącznik nr 1 do niniejszego zarządzenia.

2. Wprowadzam dokumentację oceny ryzyka zawodowego na stanowisku pracy zdalnej w Urzędzie Miejskim w Kamieńsku, która stanowi załącznik nr 2 do niniejszego zarządzenia.

3. Wprowadzam informację zawierającą zasady bezpiecznego i higienicznego wykonywania pracy zdalnej w Urzędzie Miejskim w Kamieńsku, która stanowi załącznik nr 3 do niniejszego zarządzenia.

§ 2. Przed dopuszczeniem pracowników do wykonywania okazjonalnej pracy zdalnej, zobowiązuję kierowników referatów do zapoznania ich z regulaminem ochrony danych osobowych podczas wykonywania pracy na stanowisku pracy zdalnej, z oceną ryzyka zawodowego oraz informacją zawierającą zasady bezpiecznego i higienicznego wykonywania pracy zdalnej.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
Bogdan Pawłowski

Marek Drzazga
RADCA PRAWNY
Łdz – PI/148

Załącznik Nr 1
do Zarządzenia Nr 120.12.2023
Burmistrza Kamieńska
z dnia 30 października 2023 r.

Regulamin
ochrony danych osobowych
podczas wykonywania pracy zdalnej

w jednostce o nazwie:

URZĄD MIEJSKI W KAMIEŃSKU

§ 1

Wstęp

1. „Regulamin ochrony danych osobowych podczas wykonywania pracy zdalnej" (dalej jako „Regulamin") standaryzuje zasady ochrony danych osobowych w związku z realizacją pracy zdalnej. Regulamin wprowadza się z uwagi na brzmienie art. 24 oraz 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. UE L z 2016 r. 119, s. 1 ze zm.) – dalej RODO oraz Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy.
2. W Regulaminie stosuje się termin:
   1) „Pracownik" – przez co należy rozumieć zarówno osoby zatrudnione w ramach stosunku pracy, jak i współpracowników, na stale wykonujących zadania w ramach umów cywilnoprawnych wymagające dostępu do zasobów sprzętowych i informacyjnych organizacji.
   2) „Pracodawca" – przez co należy rozumieć zarówno pracodawcę zatrudniającego na podstawie Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy, jak i zleceniodawcę.

§ 2

Możliwość podjęcia pracy zdalnej

1. Pracodawca ma wyłączne uprawnienia do podejmowania decyzji dotyczących możliwości podjęcia pracy zdalnej przez pracownika, w oparciu o obecny stan faktyczny i prawno-normatywny.
2. Pracownik może zgłosić swoją chęć podjęcia pracy zdalnej Pracodawcy.
3. Pracodawca określa warunki i zasady pracy zdalnej, w tym zakres i harmonogram wykonywanej pracy zdalnej, w odrębnym regulaminie lub w porozumieniu z Pracownikiem.
4. Pracownik, który podjął pracę zdalną, ma obowiązek przestrzegania określonych zasad ochrony danych osobowych ustalonych w organizacji.
5. Pracownik jest odpowiedzialny za zapewnienie właściwych warunków technicznych i organizacyjnych (w tym lokalowych) zgodnie z obowiązującym Regulaminem.
6. W przypadku niemożności zapewnienia odpowiednich zabezpieczeń, Pracownik jest zobowiązany niezwłocznie zgłosić ten fakt Pracodawcy i postępować zgodnie z udzielonymi instrukcjami.
7. Naruszenie zasad określonych w Regulaminie lub nieprzestrzeganie jego postanowień stanowi naruszenie obowiązków pracowniczych. W przypadku pracowników zatrudnionych na podstawie umów cywilnoprawnych, działanie niezgodne z niniejszym Regulaminem może oznaczać wykonanie zadania w sposób niezgodny z przedmiotem umowy oraz z wymaganą starannością i profesjonalizmem, co może prowadzić do rozwiązania umowy i/lub zastosowania innych sankcji.

§ 3

Miejsce świadczenia pracy zdalnej

1. Pracownik ma obowiązek zapewnienia właściwych warunków umożliwiających efektywne wykonywanie pracy zdalnej, przy zachowaniu odpowiedniego poziomu ochrony informacji.

2. Pracownik jest zobowiązany wykonywać pracę zdalną jedynie pod adresem wskazanym przez Pracodawcę, unikając pracy w miejscach publicznych, takich jak kawiarnie, restauracje, biblioteki, świetlice szkolne itp., gdzie możliwy jest dostęp osób nieuprawnionych do służbowych rozmów lub dokumentów.

3. Pracując w domu, Pracownik ma obowiązek zapewnić prywatność wykonywanej pracy poprzez zachowanie zasady czystego ekranu (uniemożliwienie osobom postronnym pozyskania informacji z ekranu komputera / wyświetlacza telefonu) oraz utrzymanie porządku na biurku, aby uniknąć wglądu domowników w przetwarzane informacje.

4. Praca zdalna powinna być realizowana zgodnie z ustalonym harmonogramem pracy, w godzinach uzgodnionych z Pracodawcą, będąc dostępnym i aktywnym w ustalonych czasookresach.

5. Przed opuszczeniem komputera lub zakończeniem korzystania z służbowego telefonu, pracownik ma obowiązek upewnić się, że urządzenia są zablokowane w celu ochrony poufności danych.

6. Przeprowadzanie służbowych spotkań zdalnych lub rozmów telefonicznych odbywa się w sposób zapewniający poufność przekazywanych informacji, zgodnie z obowiązującymi w organizacji zasadami.

§ 4

Bezpieczeństwo pracy zdalnej

1. Internet

1) Pracownik wykonuje pracę zdalną z użyciem urządzeń służbowych, które zostały dostarczone przez Pracodawcę.

2) W przypadku udostępnienia Pracownikowi przez Pracodawcę modemu internetowego lub telefonu służbowego z funkcją „hotspot", Pracownik korzysta z tych urządzeń do połączenia z internetem. Korzystanie z prywatnej sieci internetowej jest dozwolone jedynie po poinformowaniu i uzyskaniu zgody Pracodawcy.

3) W przypadku korzystania z domowej sieci z dostępem do internetu, należy upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania. W szczególności należy zadbać o to, by urządzenie dostarczające internet (np. domowy router) posiadało następującą konfigurację:

   a) najnowszy dostępny firmware;

   b) wyłączony dostęp do panelu administracyjnego urządzenia z sieci Internet;

   c) ustawione mocne hasło dostępu do panelu administracyjnego urządzenia (minimum 12 znaków, duże, małe litery i cyfry);

   d) ustanowione mocne hasło do sieci Wi-Fi (o ile urządzenie ma ją włączoną);

   e) szyfrowanie sieci Wi-Fi w standardzie minimum WPA PSK2;

   f) wyłączoną funkcję WPS;

   g) wyłączoną funkcję UPnP.

2. Urządzenia służące do pracy zdalnej

1) Zakazuje się udostępniania urządzeń używanych do pracy zdalnej innym osobom między innymi członkom rodziny.

2) Praca zdalna jest wykonywana przy użyciu sprzętu służbowego, takiego jak komputer stacjonarny, laptop, telefon, tablet, itp. (w zależności od delegowanego przez Pracodawcę sprzętu).

3) Pracownik ma prawo zabrać ze sobą komputer stacjonarny do miejsca wykonywania pracy zdalnej, na czas jej wykonywania (po uprzedniej zgodzie Pracodawcy oraz zastosowaniu środka kryptograficznego wobec wewnętrznej pamięci dyskowej).

4) Urządzenie służbowe jest wydawane Pracownikowi na podstawie protokołu.

5) Jeśli z jakiegoś powodu Pracownik nie może wykonywać pracy zdalnej przy użyciu sprzętu służbowego, Pracodawca może wydać zgodę na pracę przy użyciu prywatnych urządzeń.

6) W przypadku korzystania z prywatnego sprzętu Pracownik wyraża zgodę na wykonanie audytu bezpieczeństwa informacji używanego urządzenia przez Dział IT. Pracownik zobowiązany jest to udzielenia na żądanie Pracodawcy pełnego dostępu administracyjnego dla Działu IT, jeśli zajdzie taka potrzeba do celów weryfikacji bezpieczeństwa informacji.

7) Minimalne wymagania dotyczące bezpieczeństwa, które dotyczą zarówno urządzeń prywatnych, jak i służbowych:

   a) na urządzeniu znajduje się legalne i aktualne oprogramowanie;

   b) automatyczne aktualizacje są włączone;

   c) zapora systemowa (firewall) jest włączona;

   d) jest zainstalowany wraz z aktualną bazą wirusów oraz działający program antywirusowy;

   e) logowanie do systemu operacyjnego w komputerze wymaga uwierzytelnienia, np. za pomocą indywidualnego loginu i hasła użytkownika / kodu PIN /fizycznego tokenu;

   f) autouzupełnianie i zapamiętywanie haseł w przeglądarkach internetowych są wyłączone;

   g) zainstalowany jest program umożliwiający szyfrowanie i deszyfrowanie danych (np. program 7-zip do szyfrowania załączników wiadomości e-mail);

   h) Automatyczne blokowanie urządzenia po dłuższym okresie bezczynności jest aktywowane;

   i) jeśli jest taka możliwość, praca na urządzeniu wykonywana jest na koncie z ograniczonymi uprawnieniami użytkownika;

   j) dysk urządzenia (cały(e) wolumen(y)) jest(są) zaszyfrowany(e).

8) Pracodawca ma prawo uruchomić dodatkowe zabezpieczenia na służbowych urządzeniach używanych do pracy zdalnej. Mowa o zabezpieczeniach takich jak:

   a) zablokowanie podłączania nieautoryzowanych nośników zewnętrznych (np. pendrive) portów na pamięci zewnętrznej;

   b) użytkowanie oprogramowania do monitorowania pracy pracownika w kontekście bezpieczeństwa informacji, stosowane zgodnie z przepisami prawa pracy.

9) Instalowanie oprogramowania na urządzeniach służbowych używanych do pracy zdalnej jest możliwe tylko przez pracowników działu IT lub za ich zgodą i zgodnie z ich wytycznymi.

10) Zakazuje się instalowania nielegalnego oprogramowania na urządzeniach służbowych używanych do pracy zdalnej.

11) Pracownik nie może przechowywać na urządzeniach służbowych plików niezwiązanych z wykonywaną pracą lub innych plików lub programów bez odpowiedniej licencji.

12) Pracownik nie może instalować prywatnych aplikacji lub oprogramowania na urządzeniach służbowych używanych do pracy zdalnej.

13) Pracownik jest zobowiązany korzystać z bezpiecznego połączenia VPN (ustalonego przez Pracodawcę / Dział IT) podczas łączenia się z zasobami sieciowymi Pracodawcy.

14) Zewnętrzne urządzenia pamięcionośne pod odłączeniu od urządzenia wykorzystywanego do pracy zdalnej należy przechowywać odrębnie od tegoż urządzenia (np. stacji roboczej w obszarze gospodarstwa domowego) - w przypadku np. spalenia się laptopa, nośnik może pełnić rolę kopii zapasowej.

15) Urządzenia służące do pracy zdalnej powinny być użytkowane w suchym pomieszczeniu – zabrania się użytkowania urządzeń w pomieszczeniach o podwyższonej wilgotności (np. łazienka).

16) Zabrania się użytkowania telefonu podczas deszczu (będąc w otwartej przestrzeni).

17) Podczas pracy pracownik nie powinien kłaść napojów na / w pobliżu urządzeń wykorzystywanych do pracy zdalnej.

18) Pracownika obowiązuje zakaz samodzielnego zlecania lub wydawania sprzętu innym osobom (spoza działu IT Pracodawcy). Jakiekolwiek usterki techniczne, zanieczyszczenia, zabrudzenia w tym degradacja, inne zdarzenia uniemożliwiające wykonywanie pracy zdalnej winny być zgłaszane do przełożonego i/lub Działu IT i/lub bezpośrednio Pracodawcy.

19) Zabrania się korzystać z laptopa w łóżku kładąc go na pościeli - (praca laptopa na pościeli może powodować wciąganie pyłu oraz zwiększa temperaturę laptopa, przez co laptop może ulegać degradacji).

20) Laptop nie powinien być przechowywany przez dłuższy okres czasu w temperze poniżej +5 C. Po dłuższym okresie wychłodzenia, urządzenie przed uruchomieniem powinno zwiększyć swoją temperaturę w warunkach pokojowych.

21) Zabrania się przechowywania oraz użytkowania urządzeń elektronicznych pamięcionośnych w pobliżu takich źródeł jak: mikrofalówka, amplituner (kino domowe wraz z głośnikami w bliskiej odległości), TV, pralka, klimatyzator przenośny, odkurzacz, kuchenka indukcyjna.

22) Zewnętrzne nośniki elektroniczne oraz papierowe powinny być przechowywane oraz użytkowane tylko i wyłącznie w obszarze domowym Pracownika lub w wyznaczonym przez Pracodawcę miejscu.

23) Nie zezwala się na formatowanie przez Pracownika urządzeń zewnętrznych (w szczególności szyfrowanych) bez zgody/asysty Administratora Systemów Informatycznych/Działu IT.

24) Nie zezwala się na samodzielną instalację aplikacji przez Pracownika z oficjalnych repozytoriów (Sklep Google Play; AppStore itd...) i nieoficjalnych repozytoriów oraz w trybie ręcznym (np. instalacja z plików *.apk).

25) Nie zezwala się na wykonanie „root'a" (usunięcie zabezpieczeń producenta na telefonie) przez samego pracownika lub przy udziale innych osób spoza jednostki zatrudniającej.

26) Pracownik będąc uświadomiony, iż powierzony sprzęt ma zapewnić bezpieczeństwo danych oraz wygodę pracy powinien zwracać uwagę na wszelakie odstępstwa od normy w sposobie pracy sprzętu oraz informować Dział IT Pracodawcy/bezpośrednio Pracodawcę. Pracownik powinien zwracać uwagę na między innymi takie elementy jak: ilość zapisanych danych na laptopie/telefonie czy też zewnętrznym nośniku danych, temperaturę urządzenia (laptop, telefon, pendrive) (zawyżona ciepłota wpływa na prędkość działania), ilość jednocześnie uruchomionych programów (laptop, telefon), wersję aktualizacji systemu operacyjnego (laptop, telefon) - (czy jest najnowsza), aktualność oprogramowania antywirusowego (w przypadku laptopa).

3. Zabezpieczanie przekazywanych informacji

1) Pracownik korzysta z programów i systemów udostępnionych przez Pracodawcę na cele realizacji pracy zdalnej.

2) Przed przesłaniem poufnych informacji, w tym danych osobowych, należy je zabezpieczyć hasłem. Informacje te powinny być przesyłane w załączniku zabezpieczonym hasłem, niezależnie od ich charakteru, takich jak imiona, nazwiska czy adresy e-mail. Hasło powinno być skomplikowane i niesłownikowe, zawierać minimum 12 znaków, w tym wielkie i małe litery, cyfry oraz znaki specjalne.

3) Hasło powinno być przekazane odbiorcy inną drogą komunikacji (np. sms, telefonicznie poprzez połączenie głosowe).

4) Stałe hasło może być ustalone tylko w przypadku jednego odbiorcy.

5) Zaleca się zabezpieczenie pliku poprzez nadanie hasła (np. za pomocą programu „7-Zip").

6) W zakresie zabezpieczania pliku(ów) hasłem, Pracownik jest w obowiązku stosować się do „Instrukcji szyfrowania danych (plików i folderów)" stanowiącej zał. nr 1 do Regulaminu.

7) Wysyłając wiadomość, należy sprawdzić, czy jest kierowana do odpowiedniego odbiorcy.

8) W przypadku kilku odbiorców, należy skorzystać z opcji Ukrytej kopii (UDW/BCC) celem uniemożliwienia zapoznania się konkretnego odbiorcy z resztą adresów e-mail.

9) Pracownik może przekazywać pliki z informacjami chronionymi z wykorzystaniem udostępnionych przez Pracodawcę serwerów sieciowych używających bezpiecznych protokołów komunikacyjnych (np. sFTP, WebDav itp...).

10) Przesyłanie treści naruszających prawa własności intelektualnej lub zabronionych prawnie jest zabronione.

11) Nie można korzystać z narzędzi do przesyłania i udostępniania plików oraz komunikatorów internetowych, które nie są używane w organizacji (takich jak np. weTransfer, Google Drive, Dropbox, Discort, Skype, WhatsApp, Messenger, Telegram, Signal itp.).

4. Zasady korzystania z dokumentów w formie papierowej

1) Według obowiązujących u Pracodawcy zasad, dokumenty zawierające poufne informacje, w tym dane osobowe, powinny być przechowywane w szafach zamykanych na klucz w siedzibie organizacji.

2) Zakazane jest zabieranie oryginałów dokumentów poza siedzibę Pracodawcy.

3) Jeśli do pracy zdalnej potrzebny jest dostęp do dokumentów papierowych, Pracownik musi poprosić Pracodawcę o zgodę na ich skopiowanie i zabranie do domu.

4) Po otrzymaniu pisemnej zgody lub służbowej wiadomości e-mail, Pracownik może skopiować niezbędne dokumenty.

5) Po skopiowaniu dokumentów, pracownik musi sporządzić ich zestawienie zawierające informacje o tym, jakie dokumenty i w jakiej liczbie zostały skopiowane.

6) Zestawienie musi być przekazane Pracodawcy.

7) Podczas przewożenia kopii dokumentów do miejsca pracy zdalnej należy zachować szczególną ostrożność, aby ich nie zgubić.

8) Pracownik zapewnia zabezpieczenie kopii dokumentów w miejscu wykonywania pracy zdalnej poprzez przechowywanie ich w szafie zamykanej z ograniczonym dostępem dla osób trzecich, do której tylko on ma dostęp.

9) W przypadku jakiejkolwiek degradacji kopii dokumentu/zniszczenia powinien on zostać przekazany przełożonemu / pracodawcy. Nie należy odzyskiwać dokumentu w sytuacji wymagającej udziału osób trzecich spoza organizacji Pracodawcy.

10) Praca z dokumentami nie może odbywać się w miejscach publicznych, takich jak świetlica w szkole, kawiarnia, restauracja, galeria handlowa itp.

11) Po zakończeniu pracy, wszystkie kopie dokumentów należy zwrócić Pracodawcy, który dokonuje ich weryfikacji pod kątem kompletności.

12) Kopie dokumentów można niszczyć tylko w siedzibie Pracodawcy przy użyciu niszczarek do dokumentacji wykorzystywanych przez organizację.

13) Podczas pracy Pracownik nie powinien kłaść napojów na/w pobliżu kopii dokumentów wykorzystywanych do pracy zdalnej.

§ 5

Szczególne sytuacje

1. Problemy w działaniu udostępnionego sprzętu lub oprogramowania należy niezwłocznie zgłaszać do przełożonego i/lub Działu IT i/lub bezpośrednio Pracodawcy.
2. W przypadku zgubienia lub kradzieży sprzętu, kopii dokumentów lub innych nośników informacji, a także wystąpienia jakichkolwiek incydentów w obszarze ochrony danych osobowych, czy wystąpienia podejrzenia wystąpienia naruszenia, należy niezwłocznie, w dniu zdarzenia zgłosić ów fakt do Działu IT i/lub Inspektora Ochrony Danych.

§ 6

Działania niedozwolone

1. Niedozwolone jest w szczególności:
   1) udostępnianie innym osobom informacji służących do uwierzytelnienia w systemach lub usługach;
   2) przekazywanie poufnych informacji, w tym danych osobowych, bez zabezpieczenia hasłem, w treści wiadomości e-mail;
   3) przekazywanie hasła do chronionych informacji tą samą drogą komunikacji co pliki zabezpieczone hasłem;
   4) korzystanie z urządzeń niezatwierdzonych przez Pracodawcę;
   5) niszczenie dokumentów w domu;
   6) udostępnianie służbowego lub wykorzystywanego do pracy sprzętu innym osobom;
   7) dzielenie się poufnymi informacjami z innymi nieuprawnionymi osobami np. domownikami;
   8) logowanie się na konto innego użytkownika (na posiadanym urządzeniu i/lub podczas połączenia zdalnego z siedzibą Pracodawcy);
   9) zabieranie oryginałów dokumentów;
   10) zabieranie kopii dokumentów bez pisemnej lub wyrażonej w formie wiadomości mailowej zgody Pracodawcy;
   11) niezwrócenie dokumentów po ich użyciu Pracodawcy;
   12) niepotwierdzenie z Pracodawcą zakresu zwróconych danych.

§ 7

Zasady bezpiecznego prowadzenia wideokonferencji

1. Zasady bezpiecznego prowadzenia wideokonferencji określa załącznik nr 2 do Regulaminu.

§ 8

Dodatkowe informacje

1. Pracownik składa Pracodawcy oświadczenie o zapoznaniu się z procedurą ochrony danych osobowych. Wzór oświadczenia stanowi załącznik nr 3 do Regulaminu.

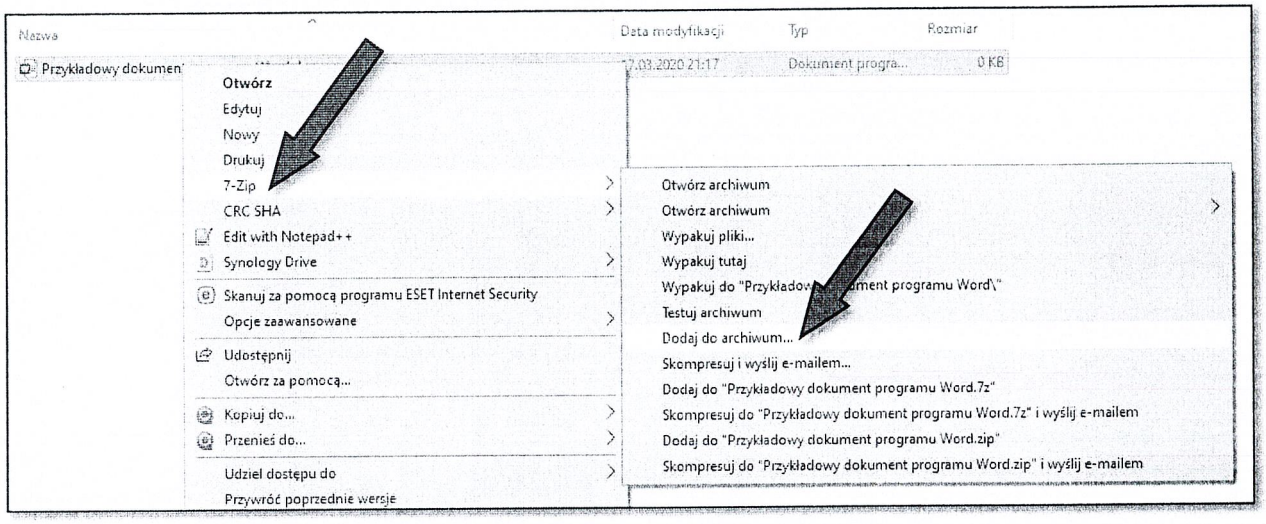
BURMISTRZ

Bogdan Pawłowski

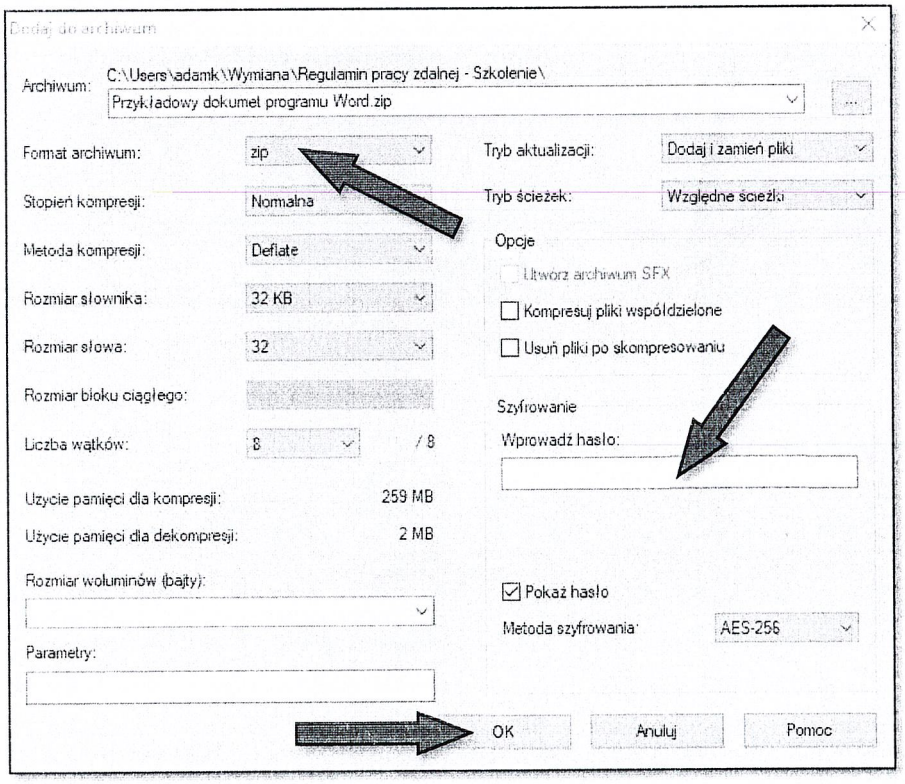
INSTRUKCJA SZYFROWANIA DANYCH (PLIKÓW I FOLDERÓW)

Chcąc zaszyfrować plik lub cały folder, musisz wykonać następujące czynności:

1. Kliknij prawym przyciskiem myszy na wybrany plik(i) lub folder(y). Następnie kliknij w menu „**7-Zip**" oraz „**Dodaj do archiwum...**":



2. Teraz otworzy się okno konfiguracji kompresji i szyfrowania dla wybranego przez Ciebie pliku(ów) lub folderu(ów). Warto ustawić format archiwum na „**ZIP**". W przyszłości automatycznie każda czynności kompresji i szyfrowania będzie zapamiętana dla tego ustawienia. Oczywiście w polu „**Wprowadź hasło**" wpisujemy je. Następnie klikamy „**OK**". Po skompresowaniu („spakowaniu") pliku(ów) lub folderu(ów) plik z rozszerzeniem *.zip zapisze się w macierzystym katalogu, w którym były źródłowe dane. Wszystko gotowe :



BURMISTRZ
Bogdan Pawłowski

Zasady bezpiecznego prowadzenia wideokonferencji

1. Co do zasady korzystaj z oprogramowania dedykowanego w Twojej organizacji do przeprowadzania wideokonferencji.
2. Jeśli musisz skorzystać z innego oprogramowania, upewnij się że zaproszenie które dostałeś pochodzi z zaufanego źródła i od osoby, od której spodziewasz się takiego zaproszenia.
3. Nie dołączaj do spotkań (nie klikaj w linki) z zaproszeń od osób, od których nie spodziewałeś się takiego zaproszenia.
4. Zadbaj o odpowiednią konfigurację ustawień audio/wideo. W ustawieniach włącz opcję, która wycisza mikrofon i wyłącza kamerę za każdym razem, kiedy dołączasz do spotkania. Dla większego bezpieczeństwa – rozważ zasłonięcie obiektywu kamery internetowej, kiedy jej nie używasz. Mikrofon i kamerę włączysz jak będzie to potrzebne.
5. Nie dziel się otrzymanym indywidualnie zaproszeniem na wideokonferencję. Jeśli nawet znany Ci współpracownik potrzebuje tego linku, najprościej i najbezpieczniej poprosić organizatora o dedykowane zaproszenie. Nie udostępniaj linków do wideokonferencji np. w mediach społecznościowych.
6. Nie nagrywaj bez pozwolenia. Jeśli chcesz to robić – zapytaj innych uczestników spotkania, czy nie mają nic przeciwko. Jeśli zrobione zrzuty ekranu lub nagrania chcesz opublikować lub przesłać dalej, zwróć uwagę czy przez przypadek nie udostępniasz wrażliwych informacji lub danych, w tym danych osobowych.
7. Sprawdź, co jest za Tobą. Jeśli masz zamiar korzystać z kamery, skontroluj swoje otoczenie. Sprawdź, czy w zasięgu kamery nie znajdują się żadne osobiste przedmioty, których nie chcesz pokazywać podczas połączenia. Niektóre programy do obsługi wideokonferencji pozwalają na rozmycie lub ustawienie wirtualnego tła. Dzięki temu inni uczestnicy spotkania nie widzą tego, co znajduje się z tyłu.
8. Jeśli chcesz udostępniać ekran komputera, zamknij wszystkie inne aplikacje i ukryj poufne pliki z pulpitu. Wyłącz wszelkie powiadomienia z innych aplikacji. Dzięki temu unikniesz przypadkowego upublicznienia poufnych lub wrażliwych informacji. Zastanów się, czy zamiast udostępniania całego ekranu komputera – nie warto udostępniać tylko tę aplikację, którą chcesz pokazać.
9. Zapoznaj się z ogólnymi warunkami użytkowania lub polityką prywatności programu, z którego będziesz korzystać, w tym sprawdź, o jakie uprawnienia do danych jesteś proszony - lista kontaktów, lokalizacja itp., a także sprawdź, czy aplikacja dysponuje niezbędnymi środkami bezpieczeństwa, takimi jak szyfrowanie transmisji danych.
10. Do zainstalowania aplikacji na komputerze (po uprzedniej zgodzie Pracodawcy / Działu IT) użyj oficjalnej strony aplikacji, z której chcesz korzystać; w przypadku urządzeń mobilnych wybierz oficjalny sklep - Google Play lub App Store.
11. Po zakończeniu wideokonferencji wyłącz mikrofon i kamerę, upewnij się, że zakończyłeś spotkanie on-line i zamknąłeś aplikację oraz sprawdź, czy program do wideokonferencji nie działa w tle.
12. Korzystaj co do zasady z aplikacji webowych, nie desktopowych, chyba że prawidłowe funkcjonowanie programu wideokonferencyjnego poprzez przeglądarkę web znacząco utrudnia komunikację – skontaktuj się z Pracodawcą / Działem IT.
13. Pamiętaj o zabezpieczeniu sieci Wi-Fi silnym hasłem (minimum 12 znaków w tym mała i duża litera, cyfra oraz znak specjalny).
14. Ogranicz ilość podawania danych osobowych - użyj pseudonimu i służbowego adresu e-mail. W szczególności mowa o Twojej nazwie użytkownika (tzw. „Nick") dołączając do wideokonferencji.

15. Używaj haseł o odmiennej strukturze, niż te podawane przez Ciebie w innych usługach.

16. Nie udostępniaj dokumentów służbowych za pomocą czatu, który może być publiczny.

17. Jeśli jesteś organizatorem spotkania wideokonferencyjnego (za zgodą Pracodawcy / Działu IT lub z innych uzasadnionych przyczyn), wymagaj hasła. Ustaw hasło dostępowe do spotkania. Dzięki niemu tylko osoby, które je dostaną będą mogły dołączyć do spotkania. To ważne z uwagi na bezpieczeństwo, prywatność oraz kontrolę dostępu do wideokonferencji.

18. Sprawdź, kogo zapraszasz do spotkania. Zweryfikuj listę zaproszonych na wideokonferencję. Upewnij się, że są na niej tylko osoby, które – Twoim zdaniem – powinny mieć dostęp do informacji przekazywanych w trakcie spotkania. Jeśli ktoś łamie zasady spotkania – usuń taką osobę z wideokonferencji. Zadbaj o komfort uczestników rozmowy – niektóre programy do obsługi wideokonferencji umożliwiają zablokowanie spotkania po jego rozpoczęciu, tak aby nikt więcej - bez zgody - nie mógł do niego dołączyć. Dostępne są również rozwiązania polegające na wstępnym umieszczaniu uczestników w wirtualnej poczekalni – po to, by zweryfikować ich tożsamość.

BURMISTRZ
Bogdan Pawłowski

OŚWIADCZENIE PRACOWNIKA

o zapoznaniu się z Regulaminem ochrony danych osobowych podczas wykonywania pracy zdalnej

	DATA ZŁOŻENIA OŚWIADCZENIA:	*[DATA]*
NAZWA JEDNOSTKI:	*URZĄD MIEJSKI W KAMIEŃSKU*	
IMIĘ I NAZWISKO OSOBY SKŁADAJĄCEJ OŚWIADCZENIE:	*[IMIĘ I NAZWISKO]*	

TREŚĆ OŚWIADCZENIA

*Oświadczam, że zapoznałem się z „**Regulaminem ochrony danych osobowych podczas wykonywania pracy zdalnej**" obowiązującym u mojego Pracodawcy i zobowiązuję się do jego przestrzegania.*

data, miejsce oraz czytelny podpis Pracownika

BURMISTRZ
Bogdan Pawłowski

Załącznik Nr 2
do Zarządzenia Nr 120.12.2023
Burmistrza Kamieńska
z dnia 30 października 2023 r.

OCENA RYZYKA ZAWODOWEGO NA STANOWISKU PRACY ZDALNEJ

METODA RISC SCORE

1. Opis stanowiska pracy

Praca polegająca na wykonywaniu swoich obowiązków całkowicie lub częściowo w miejscu zamieszkania pracownika lub w innym miejscu ustalonym przez pracownika i pracodawcę, z wykorzystaniem środków komunikacji elektronicznej. Wyniki swojej pracy, którą pracownik wykonuje poza zakładem, przekazuje pracodawcy – w szczególności za pośrednictwem komunikacji elektronicznej. Możliwe jest również przekazywanie efektów pracy w inny, ustalony wcześniej sposób.

Podczas wykonywania pracy w trybie zdalnym pracownik wykonuje czynności związane z prowadzeniem dokumentacji biurowej, przygotowaniem dokumentów służących do pracy innym pracownikom, obsługą monitorów ekranowych oraz innych urządzeń biurowych, stanowiących wyposażenie stanowiska pracy, utrzymaniem ładu i porządku w miejscu pracy. Pracownik wykonuje czynności za pomocą środków pracy biurowej ręcznie oraz za pomocą urządzeń biurowych, w tym komputerów. Komunikowanie się z innymi pracownikami odbywa się za pomocą środków porozumiewania się na odległość.

2. Miejsce wykonywania pracy, warunki pracy:

Na stanowisku podczas wykonywania pracy zdalnie pracownicy mogą wykonywać pracę w systemie ośmiogodzinnym jednozmianowym, dwuzmianowym lub w zadaniowym czasie pracy w zależności od indywidualnych ustaleń pomiędzy pracownikiem a pracodawcą.

3. Czynności wykonywane przy pracy zdalnej:

- przygotowanie stanowiska pracy,
- praca przy komputerze/laptopie
- korzystanie z urządzeń biurowych (np. drukarka),
- korzystanie z telefonu,
- inne prace biurowe,
- uczestnictwo w spotkaniach zebraniach za pośrednictwem komunikacji elektronicznej,
- wykonywanie innych czynności zleconych przez przełożonego możliwych do wykonania w warunkach pracy zdalnej.

4. Urządzenia i narzędzia, które mogą być stosowane w procesie pracy (dostępność poszczególnych urządzeń określana jest indywidualnie pomiędzy pracownikiem i pracodawcą):

- komputer stacjonarny, laptop, tablet, telefon,
- kserokopiarka, drukarka, niszczarka,
- urządzenia biurowe multimedialne,

- materiały i akcesoria biurowe (np. segregatory, długopisy, zszywacze, dziurkacze).

5. Szkolenia:

Pracownicy posiadają wymagane przepisami prawa szkolenia w zakresie higieny pracy i bhp oraz orzeczenie lekarza medycyny pracy o braku przeciwwskazań do wykonywania pracy na zajmowanym stanowisku.

BURMISTRZ

Bogdan Pawłowski

Zagrożenie	Możliwe źródła zagrożenia	Możliwe skutki zagrożenia	Środki profilaktyczne	RYZYKO				Ocena ryzyka
				Skutki S	Ekspozycja E	Prawdopodobieństwo P	Ryzyko R	
1	2	3	4	5	6	7	8	9
CZYNNIKI NIEBEZPIECZNE MOGĄCE POWODOWAĆ URAZY								
Porażenie prądem elektrycznym – niebezpieczne napięcie w instalacji elektrycznej	Urządzenia zasilane energią elektryczną. Instalacje elektryczne. Pojawienie się napięcia na urządzeniu biurowym. Niesprawne, niezaizolowane przewody zasilające urządzenia. Uszkodzone obudowy urządzeń elektrycznych	Oprzenia termiczne, poparzenia prądem elektrycznym	Stosowanie wyłącznie sprawnych urządzeń elektrycznych oraz nieuszkodzonych, sprawnych przewodów zasilających. Wykonywanie bieżących kontroli stanu technicznego urządzeń oraz przewodów zasilających. Zakaz wykonywania napraw urządzeń zasilanych energią elektryczną we własnym zakresie.	3	6	3	54	Ryzyko małe
Uderzenie o nieruchome przedmioty	Ograniczone szerokości dojścia do stanowiska pracy. Niezamknięte szuflady, drzwiczki szafek. Zła organizacja stanowiska pracy.	Stłuczenia ciała, drobne urazy	Zachowanie odpowiedniej szerokości dojścia do stanowiska pracy (co najmniej 75 cm) do stanowisk pracy zdalnej. Ład i porządek na stanowisku pracy	1	3	3	9	Ryzyko znikome
Uderzenie przez spadające i przewracające się przedmioty	Niezabezpieczone oraz przeciążone regały i półki przy stanowisku pracy zdalnej.	Stłuczenia ciała, urazy głowy	Stabilnie ustawione i zabezpieczone przed przewróceniem regały biurowe. Stabilne mocowanie półek.	3	6	3	54	Ryzyko małe
Poślizgnięcie się, potknięcie i upadek na tym samym poziomie	Leżące na ciągach komunikacyjnych przewody elektryczne i inne przedmioty. Śliskie nawierzchnie podłóg, rozlane płyny	Stłuczenie ciała, złamania, zwichnięcia, skręcenia	Przestrzeganie porządku na stanowisku pracy zdalnej. Ład i porządek w miejscu pracy zdalnej.	3	6	3	54	Ryzyko małe
Ostre krawędzie przedmiotów	Materiały biurowe oraz przedmioty posiadające ostre krawędzie np. spinacze, zszywki, nożyki, nożyczki.	Drobne urazy rąk	Uwaga, koncentracja. Ład i porządek w miejscu pracy	1	2	1	2	Ryzyko znikome
Przytrzaśnięcie palców	Niewłaściwe wykonywanie czynności, nieuwaga, pośpiech	Stłuczenia, drobne urazy rąk	Uwaga, koncentracja	1	1	0,5	0,5	Ryzyko znikome
Zagrożenia pożarowe	Przypadkowe lub celowe zaprószenie ognia, zwarcie instalacji elektrycznej, palenie tytoniu na stanowisku pracy	Oparzenia termiczne, zatrucia, podrażniania dróg oddechowych	Przestrzeganie zakazu palenia tytoniu na stanowisku pracy zdalnej, przestrzeganie zakazu używania otwartego ognia. Obsługa urządzeń zgodnie z instrukcją obsługi. Bieżące usuwanie zauważonych uszkodzeń (uszkodzona instalacja elektryczna, uszkodzenia urządzeń).	3	6	3	54	Ryzyko małe

CZYNNIKI PSYCHOSPOŁECZNE I ZWIĄZANE Z ORGANIZACJĄ PRACY								
Obciążenie statyczne ciała – układu mięśniowo – szkieletowego	Wymuszona pozycja ciała siedząca	Bóle i schorzenia układu szkieletowo – mięśniowego. Dyskopatie.	Prawidłowa organizacja pracy zdalnej. Wyposażenie stanowiska pracy zdalnej z uwzględnieniem zasad ergonomii,. Stosowanie przerw od pracy w trakcie pracy biurowej.	3	0,5	0,2	0,3	Ryzyko znikome
Obciążenie statyczne rąk	Monotypia czynności roboczych – obsługa urządzeń biurowych	Zespół cieśni nadgarstka	Wyposażenie stanowiska pracy z uwzględnieniem zasad ergonomii. Stosowanie przerw od pracy w trakcie pracy biurowej .	3	0,5	0,2	0,3	Ryzyko znikome
Obciążenie psychospołeczne	Niewłaściwe stosunki interpersonalne, przeciążenie pracą zdalną.	Nerwice, bóle głowy, wypalenie zawodowe	Właściwe wykorzystywanie urlopów wypoczynkowych. Przestrzeganie norm czasu pracy. Stosowanie przerw od pracy.	3	0,5	0,2	0,3	Ryzyko znikome
Stres	Przeciążenie pracą zdalną. Praca pod presją czasu. Duży napływ informacji. Problemy techniczne ze sprzątem IT.	Nerwice, bóle głowy, wypalenie zawodowe. Bezsenność.	Właściwe wykorzystywanie urlopów wypoczynkowych. Przestrzeganie norm czasu pracy. Stosowanie przerw od pracy.	3	0,5	0,2	0,3	Ryzyko znikome
Obciążenie emocjonalne	Brak bezpośredniego kontaktu z innymi pracownikami. Praca w samotnosci.	Znużenie pracą, wypalenie zawodowe	Właściwe wykorzystywanie urlopów wypoczynkowych. Przestrzeganie norm czasu pracy. Stosowanie przerw od pracy. Utrzymywanie kontaktów osobistych z współpracownikami, umożliwienie pracownikowi wykonującemu pracę zdalną udział w imprezach i spotkaniach organizowanych w siedzibie firmy.	3	0,5	0,2	0,3	Ryzyko znikome
CZYNNIKI SZKODLIWE								
Hałas	Hałas pochodzący od pracującego sprzętu biurowego (komputer, drukarka).	Bóle głowy, rozdrażnienie, apatia	Stosowanie przerw od pracy	1	2	1	2	Ryzyko znikome
Obciążenie narządu wzroku	Praca przy monitorze ekranowym. Niewłaściwe oświetlenie stanowiska pracy. Nieodpowiednie ustawienie biurka w stosunku do źródeł światła	Choroby wzroku, zmęczenie, bóle głowy	Prawidłowe oświetlenie stanowiska pracy zdalnej, w razie potrzeby doświetlenie stanowiska pracy lampka biurową. Stosowanie przerw od pracy. Prawidłowa regulacja ustawień monitora komputera.	3	6	3	54	Ryzyko małe

Zostałem(łam) zapoznany(na) z ryzykiem zawodowym pracy zdalnej

Imię i nazwisko	
Podpis	
Data	

BURMISTRZ

Bogdan Pawłowski

Załącznik Nr 3
do Zarządzenia Nr 120.12.2023
Burmistrza Kamieńska
z dnia 30 października 2023 r.

ZASADY BEZPIECZNEGO I HIGIENICZNEGO WYKONYWANIA PRACY ZDALNEJ W URZĘDZIE MIEJSKIM W KAMIEŃSKU

I. UWAGI OGÓLNE

1. Do pracy zdalnej może przystąpić pracownik, który posiada przeszkolenie ogólne oraz stanowiskowe BHP, aktualne zaświadczenie lekarskie o braku przeciwwskazań do pracy na zajmowanym stanowisku, oraz został zapoznany z oceną ryzyka zawodowego na stanowisku pracy, w tym pracy zdalnej.
2. Praca zdalna jest dozwolona wyłącznie wtedy, gdy pracownik posiada warunki lokalowe i techniczne niezbędne do świadczenia tej pracy.
3. W przypadku zmiany warunków lokalowych lub technicznych pracownik powinien o tej zmianie poinformować pisemnie pracodawcę.
4. Urządzenia wykorzystywane przez pracownika do pracy zdalnej, niezapewnione przez pracodawcę muszą spełniać wymagania bezpieczeństwa określone dla maszyn i innych urządzeń technicznych.

II. Przed rozpoczęciem pracy zdalnej pracownik ma obowiązek:

1. Zapewnić wygodne miejsce do ustawienia urządzeń elektronicznych i materiałów pomocniczych wykorzystywanych w trakcie pracy oraz miejscem do wykonywania innych czynności związanych z pracą zdalną, Urządzenia elektroniczne powinny być ustawione w sposób stabilny.
2. Zapewnić, aby temperatura w pomieszczeniu pracy zdalnej wynosiła nie mniej niż 18° C.
3. Dostosować wysokość siedziska do indywidualnych potrzeb, tak żeby zapewnić ergonomiczną pozycję ciała, która powinna zapobiegać nadmiernemu narażeniu na przeciążenie układu mięśniowo- szkieletowego podczas pracy. Szczególną uwagę należy zwrócić na prawidłowe: podparcie kręgosłupa, ułożenie nóg oraz podparcie rąk i dłoni podczas pracy,
4. Sprawdzić wizualnie stan techniczny gniazdka elektrycznego, do którego zostanie podłączony sprzęt elektroniczny oraz kabli zasilających. Gniazdko elektryczne nie powinno być poluzowane, a obudowa powinna być nieuszkodzona, kable nie popękane, wtyczki nieuszkodzone. Gniazdo powinno znajdować się w takiej odległości, żeby podłączone przewody elektryczne nie były naprężone i nie leżały one w ciągu komunikacyjnym, stwarzając tym samym zagrożenie potknięcia się o nie podczas przemieszczania się,
5. Zapewnić odpowiednie oświetlenie w tym odpowiednio ustawić monitor ekranowy względem źródła światła celem uniknięcia efektu odbicia czy olśnienia, Oświetlenie wymagane na stanowisku pracy zdalnej wynosi 500 lx.

6. Przygotować potrzebne dokumenty oraz programy użytkowe do pracy, jeżeli są takie potrzebne.

7. Przygotować urządzenie do pracy zgodnie instrukcją obsługi producenta.

III. Podczas wykonywania pracy zdalnej pracownik:

1. Powinien zrobić 5 minutową przerwę po każdej ciągłej godzinie pracy przy monitorze ekranowym.

2. Stosować odległość ekranu monitora od oczu w zakresie od 400 do 750 mm.

3. W miarę możliwości organizować pracę w sposób urozmaicony, zmieniając wykonywane zadania i pozycje ciała.

4. Nie dopuszczać do urządzeń, na których wykonuje się pracę zdalną osób nieupoważnionych.

5. Zabezpieczyć urządzenia przekazane do wykorzystania podczas pracy zdalnej przed dostępem osób Nieupoważnionych.

UWAGA: Za wypadki spowodowane udostępnieniem powierzonego sprzętu osobom nieupoważnionym oraz niewłaściwym zabezpieczeniem udostępnionego sprzętu odpowiedzialność ponosi pracownik użytkujący ten sprzęt.

IV. Po zakończeniu pracy zdalnej pracownik:

1. Powinien wyłączyć komputer oraz inne urządzenia zasilane energią elektryczną.

2. Uporządkować stanowisko pracy.

3. Zabezpieczyć urządzenia oraz wykorzystywane dokumenty przed dostępem osób nieupoważnionych.

V. Zasady bezpiecznego wykonywania pracy zdalnej:

1. Użytkować sprzęt zgodnie z przeznaczeniem oraz zgodnie z instrukcjami obsługi dla poszczególnych urządzeń.

2. Zapewnić ustawienie biurka oraz krzesła zgodnie z zasadami ergonomii.

3. Stosować okulary korekcyjne bądź soczewki podczas pracy przy monitorze ekranowym zgodne

z zaleceniem lekarza, jeżeli wyniki badań okulistycznych przeprowadzonych w ramach profilaktycznej opieki zdrowotnej wykażą potrzebę ich stosowania.

4. Zapewnić drożność ciągów komunikacyjnych - kable, dywany i wykładziny nie powinny odstawać, aby nie przeszkadzać w poruszaniu się po miejscu pracy zdalnej.

5. Zachować ostrożność przy używaniu urządzeń elektrycznych, w przypadku stwierdzenia nieprawidłowości bądź awarii urządzenia - odłączyć od źródła prądu i zapewnić usunięcie nieprawidłowości, awarii.

6. Zapewnić właściwe oświetlenie miejsca pracy zdalnej.

7. Zachować ład i porządek na stanowisku pracy zdalnej.

8. Oddzielić miejsca spożywania posiłków od miejsca pracy zdalnej oraz zachować ostrożność spożywając gorące napoje.

UWAGA: po każdej nieprzerwanej godzinie pracy zdalnej z komputerem, laptopem zaleca się wykonanie ćwiczeń korekcyjnych.

VI. Na stanowisku pracy zdalnej zabrania się:

1. Pracy na niesprawnych lub niekompletnych urządzeniach.

2. Pracy na urządzeniach pozbawionych obudów i osłon bezpieczeństwa.
3. Czyszczenia urządzeń bez odłączenia od sieci elektrycznej.
4. Spożywania posiłków oraz napojów podczas pracy zdalnej w miejscu pracy urządzenia.
5. Palenia tytoniu i spożywania alkoholu.
6. Wykonywania samodzielnych napraw urządzeń, zwłaszcza elektrycznych, kabli i instalacji.
7. Ograniczania swobodnego dojścia do stanowiska pracy.
8. Obsługi urządzeń elektronicznych przez osoby postronne.

VII. Zasady postępowania w sytuacjach awaryjnych stwarzających zagrożenie dla życia lub zdrowia pracownika:

1. W przypadku awarii urządzenia elektronicznego udostępnionego przez pracodawcę pracownik musi przerwać pracę i skontaktować się z bezpośrednim przełożonym.
2. W przypadku wątpliwości pracownika co do stanu bezpieczeństwa pracy, pracownik musi przerwać pracę, poinformować przełożonego o zaistniałej sytuacji oraz podjąć niezbędne działania mające na celu wyeliminowanie zagrożenia.
3. Każdy zaistniały wypadek przy pracy zdalnej w miejscu wykonywania pracy zdalnej należy niezwłocznie zgłosić przez poszkodowanego lub członka jego rodziny do bezpośredniego przełożonego pracownika. Zaistniałe wypadki należy zgłaszać pisemnie - dozwolona jest forma e -mailowa.
4. W razie zauważenia pożaru podjąć próbę jego ugaszenia, a następnie zaalarmować otoczenie, staż pożarną i przełożonego, a w przypadku ogłoszenia ewakuacji stosować się do wskazówek prowadzącego akcję ratowniczą.

UWAGI KOŃCOWE

1. Czyszczenie komputera i drukarki należy wykonywać za pomocą specjalistycznych preparatów chemicznych, podczas wyłącznego zasilania energią elektryczną.
2. Naprawy mechaniczne i elektryczne urządzeń biurowych powinny być przeprowadzane przez osoby upoważnione lub serwis.

BURMISTRZ

Bogdan Pawłowski