ZARZĄDZENIE NR 12/2020
DYREKTORA SZKOŁY PODSTAWOWEJ NR 18
IM. MACIEJA RATAJA W LUBLINIE
Z DNIA 26 PAŹDZIERNIKA 2020 R.

w sprawie przyjęcia Regulaminu pracy zdalnej obowiązującego w Szkole Podstawowej nr 18 im. Macieja Rataja w Lublinie

Na podstawie Rozporządzenia Ministra Edukacji Narodowej z dnia 20 marca 2020 r. w sprawie szczególnych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz.U. 2020 poz. 493 z późniejszymi zmianami); Rozporządzenia Ministra Edukacji Narodowej z dnia 12 sierpnia 2020 r. zmieniające rozporządzenie w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach (Dz.U. 2020 poz. 1386); Rozporządzenia Ministra Edukacji Narodowej z dnia 12 sierpnia 2020 r. w sprawie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz.U. 2020 poz. 1389),

zarządzam, co następuje:

§ 1
Wprowadzam *Regulamin pracy zdalnej obowiązujący w Szkole Podstawowej nr 18 im. Macieja Rataja w Lublinie* stanowiący załącznik do zarządzenia.

§ 2
Regulamin pracy zdalnej obowiązujący w Szkole Podstawowej nr 18 im. Macieja Rataja w Lublinie jest aktem wewnętrznym Pracodawcy i powstał w celu ustalenia reguł pracy zdalnej.

§ 3
Regulamin pracy zdalnej obowiązujący w Szkole Podstawowej nr 18 im. Macieja Rataja w Lublinie obowiązuje wszystkie osoby, które wykonują pracę zdalną bez względu na formę zatrudnienia.

§ 4
Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 1 do Zarządzenia nr 12/2020
Dyrektora Szkoły Podstawowej nr 18 im. Macieja Rataja w Lublinie
z dnia 26 październik 2020 r. w sprawie wprowadzenia

Regulamin pracy zdalnej
obowiązujący Szkole Podstawowej nr 18 im. Macieja Rataja w Lublinie

§ 1.

Postanowienia ogólne

1. Niniejszy regulamin określa zasady podejmowania i wykonywania pracy zdalnej oraz związane z tym prawa i obowiązki Pracodawcy i Pracowników.
2. Regulamin jest aktem wewnętrznym Pracodawcy i powstał w celu ustalenia reguł pracy zdalnej.
3. Regulamin obowiązuje wszystkie osoby, które wykonują pracę zdalną bez względu na formę zatrudnienia.
4. Ilekroć w niniejszym dokumencie jest mowa o:

1) ***Pracodawcy, Administratorze danych*** – oznacza to Szkołę Podstawową nr 18 im. Macieja Rataja w Lublinie, Al. Długosza 8, 20-054 Lublin. Określenie „Pracodawca" oznacza zarówno zatrudniającego na podstawie umowy o pracę oraz innej umowy cywilnoprawnej, w tym umowy zlecenia.
2) ***Pracowniku*** – oznacza to osobę zatrudnioną w oparciu o umowę o pracę oraz inną umowę cywilnoprawną, w tym umowę zlecenia, umowę o współpracy, umowę o dzieło, jeśli realizacja tej umowy wiąże się z wykonywaniem obowiązków na rzecz Pracodawcy w miejscu ich stałego wykonywania wyznaczonym przez Pracodawcę.
3) ***Pracy zdalnej*** – oznacza to świadczenie na rzecz Pracodawcy pracy określonej w umowie o pracę, jak również wykonywanie obowiązków na podstawie umowy cywilnoprawnej, w tym umowy zlecenia, umowy o współpracy oraz innej umowie cywilnoprawnej łączącej Pracownika z Pracodawcą, zgodnie z zapisami niniejszego dokumentu, poza miejscem jej stałego wykonywania (w szczególności poza siedzibą Pracodawcy), za zgodą/na polecenie Pracodawcy. Praca zdalna oznacza w szczególności pracę wykonywaną na podstawie przepisów ustawy z dnia 02.03.2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. z 2020 r., poz. 374 z późn. zm.).
4) ***Osobie nieupoważnionej*** – oznacza to osoby nie posiadające nadanego przez Administratora danych upoważnienia do przetwarzania danych osobowych; w sytuacji pracy zdalnej za osoby nieupoważnione do przetwarzania danych osobowych uważa się wszystkie osoby z otoczenia Pracownika (m.in. domowników, współlokatorów, osoby odwiedzające, postronne, itp.).
5) ***Informacji poufnej*** – oznacza to wszelkie informacje, uzyskane przez Pracownika w związku z realizacją obowiązków służbowych, które nie zostały podane do wiadomości publicznej, w tym wszelkie informacje stanowiące dane osobowe w rozumieniu powszechnie obowiązujących przepisów o ochronie danych osobowych.
6) ***Regulaminie*** – oznacza to niniejszy regulamin.

5. Dokument niniejszy opracowany został na podstawie następujących aktów prawnych:
   1) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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

(ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L z 04.05.2016 r., Nr 119, str. 1 oraz Dz. Urz. UE L z 23.05.2018 r., Nr 127, str. 2), dalej w skrócie: „RODO”;
2) ustawy z dnia 10.05.2018 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781), dalej w skrócie: „uodo”;
3) ustawy z dnia 02.03.2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. z 2020 r., poz. 374 z późn. zm.), dalej w skrócie odpowiednio: „ustawa o szczególnych rozwiązaniach związanych z COVID-19”;
4) ustawy z dnia 26.06.1974 r. Kodeks pracy (t.j.: Dz. U. z 2020 r., poz. 1320 z późn. zm.); dalej w skrócie odpowiednio: „Kodeks pracy”.

6. Praca zdalna nie stanowi telepracy w rozumieniu Kodeksu pracy.

§ 2.
Warunki dopuszczalności pracy zdalnej podczas obowiązywania przepisów ustawy o szczególnych rozwiązaniach związanych z COVID-19

Pracownik jest zobowiązany do świadczenia pracy zdalnej w związku z przeciwdziałaniem COVID-19:

1) po wydaniu polecenia przez Pracodawcę lub bezpośredniego przełożonego Pracownika pracy zdalnej w dowolnej formie, w tym w formie pisemnej lub elektronicznej.
2) po udzieleniu zgody na pracę zdalną przez Pracodawcę lub bezpośredniego przełożonego w związku z wnioskiem Pracownika o umożliwienie pracy zdalnej, jeśli wykonywanie pracy na danym stanowisku umożliwia pracę w innym miejscu niż miejsce stałego jej wykonywania oraz jeśli jest to niezbędne do przeciwdziałania i zapobiegania rozprzestrzeniania się COVID-19.

§ 3.
Warunki korzystania z trybu pracy zdalnej na zasadach ogólnych

1. Pracodawca daje możliwość wykonywania obowiązków służbowych w trybie pracy zdalnej, jeśli wykonywanie pracy na danym stanowisku umożliwia ich realizację w innym miejscu niż miejsce stałego ich wykonywania oraz gdy do realizacji tych obowiązków nie jest niezbędne przebywanie Pracownika w miejscu stałego ich wykonywania, określonym w umowie, na podstawie której świadczona jest praca.
2. Pracodawca może wyrazić zgodę na pracę zdalną po złożeniu przez Pracownika wniosku.
3. Pracownik składa wniosek do Pracodawcy lub bezpośredniego przełożonego o umożliwienie wykonywania obowiązków służbowych w trybie pracy zdalnej najpóźniej na dzień przed terminem rozpoczęcia pracy w tym trybie.
4. Dni wykonywania pracy zdalnej są dniami świadczenia pracy.
5. 5. Możliwość wykonywania pracy zdalnej jest dobrowolna, chyba że zachodzą szczególne przesłanki, które uniemożliwiają pracę w miejscu jej stałego świadczenia, określonym w umowie regulującej stosunek pracy, lub zachodzą przesłanki, zgodnie z którymi Pracodawca jest zmuszony wydać Pracownikowi polecenie wykonywania pracy w trybie pracy zdalnej.
6. Wykonywanie przez Pracownika powierzonych obowiązków w formie pracy zdalnej nie wpływa na treść umowy o pracę. W związku ze świadczeniem pracy zdalnej nie jest wymagana zmiana treści umowy o pracę na mocy porozumienia stron, czy też przez wypowiedzenie zmieniające warunki pracy.

7. W trakcie wykonywania pracy zdalnej Pracownik pracuje w systemie czasu pracy wynikającym z regulaminu pracy lub obwiązującej go umowy o pracę.
8. Praca zdalna powinna być wykonywana w godzinach i w dniach normalnej pracy, w których dany Pracownik pracował w miejscu stałego jej wykonywania.
9. Praca wykonywana na zasadach określonych w regulaminie, ponad obowiązujące Pracownika normy czasu pracy, może być podyktowana jedynie szczególnym potrzebami Pracodawcy i jest świadczona na jego wyraźne polecenie.
10. 15. Pracownik, wykonując pracę zdalną, powinien przestrzegać przepisów o czasie pracy, a zwłaszcza dotyczących nieprzerwanego 11-godzinnego odpoczynku dobowego.
11. 16. Możliwość wykonywania pracy zdalnej na podstawie innej umowy niż umowa o pracę określa się w aneksie do umowy zawartej z Pracodawcą. Zasady tak określonej pracy zdalnej powinny być zgodne z regulaminem.

§ 4.
Urlopy i absencje

1. Pracownik wykonujący pracę zdalną składa wnioski o urlopy wypoczynkowe za pośrednictwem e-maili wysyłanych do bezpośredniego przełożonego oraz do wiadomości do Pracownika odpowiedzialnego za prowadzenie spraw kadrowych u Pracodawcy.
2. Za pośrednictwem maila i telefonu Pracownik zgłasza również inne nieobecności w pracy, do których ma prawo na podstawie powszechnie obowiązujących przepisów prawa pracy i Karty Nauczyciela.
3. W zakresie nieuregulowanym w niniejszym regulaminie do zasad usprawiedliwiania nieobecności w pracy stosuje się odpowiednie regulacje przepisów regulaminu pracy.

§ 5.
Prawa i obowiązki Pracodawcy

1. Pracodawca zobowiązuje się do przekazywania Pracownikowi zadań do wykonania, udzielania informacji merytorycznych oraz organizowania procesu pracy w sposób umożliwiający Pracownikowi pracę zdalną.
2. Pracodawca zapewnia, jeśli to możliwe, warunki do wykonywania pracy zdalnej poprzez udostępnianie stosownego sprzętu oraz oprogramowania niezbędnego do wykonywania obowiązków służbowych (takich jak komputer stacjonarny, laptop, smartfon, tablet, itp.), w ramach posiadanych możliwości.
3. Pracodawca ma obowiązek zapewnić, o ile to możliwe, pełny dostęp do zasobów Pracodawcy z uwzględnieniem przedmiotu i charakteru pracy wykonywanej przez Pracownika.
4. Pracodawca ma prawo:

1) powierzyć określone zadania, które powinny być wykonane podczas pracy zdalnej;
2) monitorowania wyników pracy (w szczególności za pośrednictwem przyjętego środka komunikacji);
3) kontrolować i weryfikować wykonywanie powierzonych zadań, w tym również żądać od Pracownika informacji o ich wynikach, potwierdzenia ich wykonania, np. poprzez przesłanie raportu dziennego lub tygodniowego.

§ 6.
Prawa i obowiązki Pracownika

1. Pracownik wykonuje pracę zdalną w miejscu zamieszkania lub innym miejscu uzgodnionym z Pracodawcą. Jeżeli wykonywanie pracy będzie wiązało się ze zmianą miejsca wcześniej ustalonego z Pracodawcą, Pracownik zobowiązany jest taką zmianę uzgodnić z Pracodawcą.
2. Pracownik jest zobowiązany do wykonywania pracy zgodnie z treścią umowy łączącej go z Pracodawcą oraz zakresem obowiązków.
3. Ponadto Pracownik zobowiązuje się do:

1) pozostawania dyspozycyjnym dla Pracodawcy w ustalonych godzinach pracy i przyjmowania do realizacji bieżących zadań przekazywanych Pracownikowi w ramach zakresu jego obowiązków, w szczególności z wykorzystaniem środków komunikacji elektronicznej;
2) bieżącego informowania o wynikach swojej pracy oraz przedstawiania Pracodawcy wyników swojej pracy, przy pomocy środków komunikacji elektronicznej, takich jak: wiadomości e-mail, dziennik elektroniczny, Teams, rozmowy i wiadomości telefoniczne, telekonferencje, a także prowadząc zestawienie wykonanych zadań (w formie dziennego lub cotygodniowego zestawienia – w zależności od uzgodnień z Pracodawcą, wpisując do tabeli i przekazując w formie elektronicznej na wskazany przez Pracodawcę adres poczty e-mail);
3) potwierdzania obecności w pracy w sposób określony przez Pracodawcę. Jeżeli Pracodawca nie wskaże Pracownikowi innego sposobu potwierdzania obecności w pracy, wystarczające jest wysłanie przez Pracownika komunikatu o treści: „Rozpoczynam pracę" drogą mailową na adres Pracodawcy niezwłocznie po przystąpieniu do realizacji obowiązków służbowych w danym dniu;
4) dbania o powierzony sprzęt, w tym chronienia udostępnionych urządzeń przed zalaniem, zniszczeniem lub kradzieżą,
5) korzystania z urządzeń oraz oprogramowania dostarczonego przez Pracodawcę;
6) korzystania z poczty służbowej w celu wykonywania swoich obowiązków służbowych;
7) zapoznania się z niniejszym regulaminem i potwierdzenia tego stosownym oświadczeniem. Wzór oświadczenia Pracownika stanowi załącznik nr 2 do regulaminu.

4. Pracownik ma prawo do wsparcia technicznego ze strony Pracodawcy. Pracownik niezwłocznie zgłasza Pracodawcy wszelkie uzasadnione potrzeby w tym zakresie.
5. Pracownik zobowiązuje się zorganizować stanowisko do pracy zdalnej w sposób zapewniający bezpieczne i higieniczne warunki pracy oraz właściwy poziom bezpieczeństwa informacji.

§ 7.
Ochrona danych osobowych i bezpieczeństwo informacji

1. Pracownik jest zobowiązany do wykonywania obowiązków służbowych z zachowaniem szczególnej ostrożności w stosunku do tajemnicy służbowej oraz przetwarzanych informacji, w tym danych osobowych.
2. Pracownik podczas wykonywania pracy zdalnej zobowiązany jest przestrzegać wszystkich zasad związanych z ochroną danych osobowych i bezpieczeństwem informacji. Wykonywanie obowiązków w trybie pracy zdalnej nie zwalnia Pracownika z przestrzegania zasad określonych w obowiązującej u Pracodawcy dokumentacji z zakresu ochrony danych osobowych i bezpieczeństwa informacji, w tym politykach

bezpieczeństwa danych osobowych, politykach ochrony danych osobowych, instrukcjach, regulaminach.

3. Pracownik, przed przystąpieniem do wykonywania pracy zdalnej, zobowiązany jest do zapoznania się z obowiązkowymi zasadami postępowania w związku z przetwarzaniem danych osobowych i zalecanymi formami zabezpieczeń technicznych i organizacyjnych. Dokument opisujący obowiązkowe zasady postępowania w związku z przetwarzaniem danych osobowych i zalecane formy zabezpieczeń technicznych i organizacyjnych stanowi załącznik nr 1 do regulaminu.
4. W przypadku wykrycia lub podejrzenia zaistnienia incydentu związanego z ochroną danych osobowych Pracownik jest zobowiązany zgłosić go niezwłocznie do Pracodawcy w sposób u niego przyjęty.
5. W przypadku zgłoszenia podmiotu danych o zrealizowanie jego praw Pracownik zobowiązany jest przyjąć żądanie, a gdy żądanie zostanie wysłane na adres inny niż wskazany przez Pracodawcę w obowiązku informacyjnym, Pracownik zobowiązany jest do przekazania takiego żądania do osób odpowiedzialnych za ten obszar w sposób przyjęty u danego Pracodawcy.
6. Pracownik jest zobowiązany do zabezpieczenia urządzeń przed dostępem osób trzecich w trakcie pracy jak i po jej zakończeniu.
7. Pracownik jest zobowiązany do wykonywania kopii zapasowych danych wykorzystywanych do świadczenia pracy zdalnej. Częstotliwość, zakres i inne parametry kopii zapasowych powinny być zgodne z procedurami obowiązującymi w tym zakresie u Pracodawcy.
8. Zabronione jest podłączenie do urządzeń udostępnionych przez Pracodawcę nośników zewnętrznych z wyjątkiem tych dostarczonych przez Pracodawcę.
9. Jeżeli powierzone zostaną dokumenty papierowe, Pracownik ma obowiązek wydzielenia odrębnego miejsca do ich przechowania, tak aby dokumenty nie uległy uszkodzeniu, zgubieniu bądź zniszczeniu.
10. Pracownik zobowiązany jest do zgłaszania wszelkich niepokojących przypadków mających wpływ na poziom ochrony danych do pracodawcy niezwłocznie w sposób u niego przyjęty.
11. Jeżeli Pracownik nie ma możliwości świadczenia pracy zdalnej z zapewnieniem właściwych zabezpieczeń, w szczególności ze względu na siłę wyższą (np. brak prądu lub Internetu), niezwłocznie zgłasza to Pracodawcy i postępuje zgodnie z jego instrukcjami.

§ 8.

Bezpieczeństwo pracy zdalnej - warunki jakie powinny zostać spełnione w związku ze świadczenia pracy zdalnej

I. Miejsce pracy zdalnej

1. Pracownik jest zobowiązany zapewnić właściwe warunki umożliwiające mu skuteczną pracę zdalną z zachowaniem właściwego poziomu bezpieczeństwa informacji.
2. Niedozwolone jest podejmowanie pracy zdalnej w miejscach publicznych, takich jak kawiarnie, restauracje, galerie handlowe, dworce, świetlice szkolne, gdzie osoby postronne mogłyby usłyszeć fragmenty służbowych rozmów lub zapoznać się z fragmentami wykonywanej pracy.
3. Pracując w miejscu zamieszkania lub innym uzgodnionym miejscu, Pracownik powinien zapewnić, aby osoby nieupoważnione, w tym domownicy lub współlokatorzy, nie miały

wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera, a także zapewnienie pracy z dokumentami w sposób uniemożliwiający wgląd.
4. Odchodząc od komputera lub kończąc korzystanie z innego sprzętu elektronicznego należy upewnić się, że urządzenie zostało zablokowane.
5. Odchodząc od stanowiska pracy Pracownik jest zobowiązany schować i zabezpieczyć dokumenty przed dostępem osób trzecich.
6. Pracownik jest zobowiązany chronić dokumenty przed uszkodzeniem, zniszczeniem lub zagubieniem.
7. Pracownik nie może zostawiać osób trzecich samych w pomieszczeniu ze służbowymi dokumentami i sprzętem wykorzystywanym do wykonywania pracy (w szczególności jeżeli przetwarzane są dane osobowe).

II. Urządzenia służące do pracy zdalnej

1. Jeżeli do świadczenia pracy zdalnej zostały Pracownikowi udostępnione urządzenia służbowe (m.in. komputer stacjonarny, laptop, tablet, itp.), Pracownik zobowiązany jest do wykonywania obowiązków służbowych z wykorzystaniem sprzętu otrzymanego od Pracodawcy.
2. Wyrażenie przez Pracodawcę zgody na pracę zdalną obejmuje zgodę na korzystanie ze służbowego sprzętu w innym miejscu niż miejsce stałego wykonywania pracy (poza siedzibą Pracodawcy). Pracownik jest uprawniony także do zabrania komputera stacjonarnego do miejsca wykonywania pracy zdalnej, na czas wykonywania tej pracy.
3. Udostępnienie Pracownikowi służbowych urządzeń potwierdzone zostaje w postaci użyczenia.
4. Jeżeli nie jest możliwe wykonywanie przez Pracownika pracy zdalnej z wykorzystaniem służbowego sprzętu, informuje on o tym Pracodawcę. Pracodawca może wydać zgodę na pracę z wykorzystaniem prywatnych urządzeń, uzgadniając z Pracownikiem, z jakich urządzeń będzie korzystał w celu zrealizowania obowiązków służbowych.
5. Zabronione jest udostępnianie służbowych urządzeń wykorzystywanych do realizowania pracy zdalnej innym osobom nieupoważnionym, np. domownikom, współlokatorom, itd.
6. Przed przystąpieniem do świadczenia pracy zdalnej urządzenia, na których praca będzie wykonywana powinny zostać poddane przeglądowi obejmującemu m.in. ich sprawdzenie w zakresie bezpieczeństwa, z zachowaniem następujących zasad:

1) przeglądu dokonuje osoba odpowiedzialna u Pracodawcy za sprzęt niezbędny do wykonywania pracy;
2) w sytuacji, gdy dokonanie przeglądu przed wydaniem sprzętu nie jest możliwe, częściowy przegląd może zostać wykonany zdalnie;
3) w przypadku, gdy dokonanie przeglądu przez osobę odpowiedzialną jest niemożliwe, Pracownik sam dokonuje przeglądu, sprawdzając, czy spełnione są minimalne wymagania w zakresie bezpieczeństwa;
4) obowiązek dokonania przeglądu dotyczy także urządzeń prywatnych, które będą wykorzystywane do świadczenia pracy zdalnej.

7. Minimalne wymagania w zakresie bezpieczeństwa urządzeń wykorzystywanych do pracy zdalnej są następujące:

1) oprogramowanie na urządzeniu jest legalne i aktualne;
2) automatyczne aktualizacje zostały włączone;
3) zapora systemowa została włączona;
4) program antywirusowy został zainstalowany i działa w tle;

5) zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika, kod PIN, token;
6) w przeglądarce internetowej wyłączono autouzupełnianie i zapamiętywanie hasła;
7) program umożliwiający zaszyfrowanie i odszyfrowanie danych (np. 7-ZIP) został zainstalowany;
8) automatyczne blokowanie urządzenia po dłuższym braku aktywności użytkownika zostało ustawione;
9) jeżeli praca będzie wykonywana na sprzęcie prywatnym Pracownika, w celu odseparowania danych służbowych od danych prywatnych i zapewnienia niedostępności danych służbowych dla innych użytkowników, utworzono odrębne konto użytkownika do systemu operacyjnego, a zalogowanie się wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika.

III. Internet

1. Jeżeli Pracodawca udostępnia Pracownikowi modem internetowy lub telefon służbowy z dostępem do Internetu, który może pełnić funkcję HotSpot, Pracownik powinien w pierwszej kolejności korzystać z tych urządzeń.
2. W przypadku korzystania z domowej sieci Wi-Fi, Pracownik zobowiązany jest upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania, w szczególności:

1) korzystanie z Internetu powinno wymagać uwierzytelnienia, np. poprzez hasło;
2) hasło dostępu powinno składać się z co najmniej 8 znaków, w tym z dużych i małych liter oraz cyfr i znaków specjalnych;
3) jeśli to możliwe, należy zmienić login do panelu administracyjnego routera na własny;
4) dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej;

3. Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udziela Pracownik odpowiedzialny za obsługę informatyczną.

IV. Zabezpieczanie przekazywanych informacji

1. Do pracy zdalnej Pracownik powinien wykorzystywać tylko i wyłącznie służbowe programy i systemy udostępnione mu przez Pracodawcę.
2. Jeżeli niezbędne jest przesłanie, w tym przekazywanie z wykorzystaniem poczty elektronicznej (e-mail), informacji o charakterze poufnym, w szczególności danych osobowych, to powinny zostać udostępnione w załączniku zabezpieczonym hasłem.
3. Zabezpieczeniu powinny podlegać wszelkiego rodzaju dane osobowe, niezależnie od ich charakteru, nawet jeżeli są to jedynie imiona, nazwiska, czy adresy e-mail pozwalające na identyfikację osoby fizycznej.
4. Hasło powinno zostać przekazane odbiorcy inną drogą komunikacji niż dostarczono dane.
5. Hasło powinno być odpowiednio skomplikowane i niesłownikowe.
6. Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą.
7. Rekomendowane metody zabezpieczania hasłem:

1) nadanie hasła do pliku, w którym znajdują się dane osobowe;
2) zabezpieczenie pliku lub plików poprzez kompresję z zabezpieczeniem archiwum wynikowego hasłem.

8. Każda wiadomość powinna być wysyłana z zachowaniem należytej staranności i ostrożności, polegającej w szczególności na sprawdzeniu przed wysłaniem, czy jest kierowana do odpowiedniego adresata (odbiorcy).

9. W przypadku wysyłania informacji do kilku odbiorców należy skorzystać z opcji „Ukrytej kopii” („UDW”/ang. „BCC”), tzn. adresy wpisać w to pole, tak aby nie były widoczne dla innych odbiorców, a wiadomość zaadresować do siebie.

V. Zasady korzystania z dokumentów w formie papierowej

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 miejsce stałego wykonywania pracy (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 uzgodnionego miejsca wykonywania pracy zdalnej na czas jej wykonywania.
4. Po otrzymaniu zgody, Pracownik może sporządzić kopie niezbędnych dokumentów.
5. Zabronione jest zabieranie poza siedzibę Pracodawcy oryginałów dokumentów.
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 (świetlica w szkole, kawiarnia, restauracja, galeria handlowa, dworzec, itp.).
8. Po zakończeniu pracy, wszystkie dokumenty należy zwrócić Pracodawcy.

VI. Szczególne sytuacje

1. Problemy w działaniu udostępnionego sprzętu lub oprogramowania należy niezwłocznie zgłaszać do Pracownika odpowiedzialnego u Pracodawcy za obsługę informatyczną.
2. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do Pracodawcy.

VII. Działania niedozwolone

Przy wykonywaniu pracy zdalnej Pracownikowi niedozwolone jest:

1) udostępnianie innym osobom danych służących do uwierzytelnienia do systemów i/lub usług (m.in. poprzez pozostawienie w miejscu widocznym lub oczywistym zapisanego hasła dostępu do bazy danych, systemu lub sieci), jak również jego współdzielenie z osobami trzecimi;
2) przekazywanie informacji chronionych, w szczególności danych osobowych bez zabezpieczenia hasłem, w szczególności w treści wiadomości e-mail;
3) przekazywanie hasła do zabezpieczonych informacji tą samą drogą komunikacji, którą przekazywany jest zabezpieczony hasłem plik lub pliki;
4) korzystanie z urządzeń, które nie zostały zatwierdzone przez Pracodawcę;
5) uniemożliwienie przeglądu urządzenia lub odmówienie Pracownikowi odpowiedzialnemu
6) za obsługę informatyczną dokonania takiego przeglądu;
7) samodzielne niszczenie dokumentów służbowych w miejscu realizowania pracy zdalnej, w tym w domu; w szczególności wyrzucanie dokumentów do zwykłych śmietników w stopniu zniszczenia umożliwiającym ich odczytanie.
8) udostępnianie służbowego sprzętu lub sprzętu wykorzystywanego do realizowania zadań służbowych innym osobom;
9) dzielenie się informacjami poufnymi z innymi osobami, w szczególności domownikami, współlokatorami, znajomymi;
10) logowanie się na konto innego użytkownika;

11) zabranie oryginałów dokumentów;
12) niezwrócenie dokumentów;
13) wpuszczanie do pomieszczeń, w których wykonywana jest praca, osób nieznanych i
14) dopuszczanie do ich kontaktu z służbowym sprzętem komputerowym lub dokumentami
15) służbowymi – pozostawianie osób nieupoważnionych bez nadzoru;
16) otwieranie poczty elektronicznej pochodzącej od nieznanych nadawców, a w szczególności załączników;
17) korzystanie z publicznie dostępnych sieci Wi-Fi, które nie posiadają żadnej autoryzacji – brak hasła;
18) wysłanie mailingu masowego z wpisaniem adresów w pole „DO:" lub „DW:" zamiast „UDW:".

§ 9.
Bezpieczeństwo i higiena pracy

1. Pracownik powinien zorganizować swoje stanowisko do pracy zdalnej w sposób zapewniający bezpieczne i higieniczne warunki pracy.
2. W razie wypadku przy wykonywaniu pracy zdalnej Pracownik jest zobowiązany niezwłocznie poinformować o tym telefonicznie Pracodawcę.
3. Pracownik powinien współdziałać z powołanym zespołem powypadkowym w celu ustalenia przyczyn i okoliczności wypadku przy pracy, a jeśli to niezbędne, umożliwić członkom zespołu oględziny miejsca wypadku.

§ 10.
Postanowienia końcowe

1. Regulamin wchodzi w życie z dniem następnym po dniu jego ogłoszenia i jest udostępniany Pracownikom, którzy pracują zdalnie drogą mailową.
2. Każdy z Pracowników ma obowiązek zapoznania się z regulaminem. Sposób potwierdzenia zapoznania się z regulaminem określa Pracodawca.
3. Regulamin o aktualnej treści obowiązuje do czasu jego zmiany. W szczególności regulamin obowiązuje w okresie zagrożenia rozprzestrzeniania się SARS-CoV-2 z uwzględnieniem stosowania przepisów ustawy o szczególnych rozwiązaniach związanych z COVID-19.
4. W sprawach nieuregulowanych niniejszym regulaminem, stosuje się przepisy prawa powszechnie obowiązującego, w tym z zakresu prawa pracy i ochrony danych osobowych, a także wewnętrzne polityki, instrukcje, procedury oraz regulaminy obowiązujące u Pracodawcy z uwzględnieniem dokumentacji z zakresu ochrony danych osobowych i bezpieczeństwa informacji.

Załączniki do regulaminu pracy zdalnej:

1) Załącznik nr 1: Obowiązkowe zasady postępowania w związku z przetwarzaniem danych osobowych. Zalecane formy zabezpieczeń technicznych i organizacyjnych.
2) Załącznik nr 2: Oświadczenie Pracownika o zapoznaniu się z regulaminem pracy zdalnej.

Załącznik nr 1
do Regulaminu pracy zdalnej obowiązującego
w Szkole Podstawowej nr 18 im. Macieja Rataja w Lublinie

Obowiązkowe zasady postępowania w związku z przetwarzaniem danych osobowych

Zalecane formy zabezpieczeń technicznych i organizacyjnych

I. Obowiązkowe zasady postępowania w związku z przetwarzaniem danych osobowych

Administrator danych, w związku z wykonywaniem pracy zdalnej, przypomina i poleca stosować najważniejsze zasady mające na celu zgodne z prawem przetwarzanie danych osobowych.

1. ***Zasada legalności oraz przejrzystości*** – przetwarzanie danych osobowych musi odbywać się zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Musi istnieć podstawa prawna przetwarzania, jak np. zgoda osoby, której dane dotyczą lub niezbędność przetwarzania danych do wykonania umowy (np. podanie danych przez pracownika jest niezbędne do wykonania umowy o pracę, w tym wypłacenia należnego mu wynagrodzenia). Podstawy przetwarzania zostały określone w art. 6 i 9 RODO.
2. ***Zasada celowości*** – cel przetwarzania danych osobowych musi być z góry określony i informacja ta musi zostać przekazana osobie, której dane dotyczą. Aby dane mogły być przetwarzane musi istnieć konkretny, wyraźny i prawnie uzasadniony cel. Przetwarzanie danych w sposób niezgodny z ustalonymi celami jest zakazane.
3. ***Zasada adekwatności*** (minimalizacji danych) – administrator powinien przetwarzać tylko te dane, które są niezbędne ze względu na cel ich zbierania, np. nieadekwatne będzie pozyskiwanie kserokopii dowodu osobistego w trakcie zawierania umowy ze zleceniobiorcą, pracownikiem.
4. ***Zasada merytorycznej poprawności*** – dane osobowe muszą być prawdziwe, kompletne i aktualne ze względu na cel jakiemu mają służyć. Nie można zbierać danych osobowych ze źródeł nieznanego pochodzenia. Należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.
5. ***Zasada ograniczenia przechowywania*** – dane osobowe mogą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te zostały pozyskane (np. gdy celem zbierania CV była konkretna rekrutacja, administrator nie powinien przechowywać CV kandydatów na potrzeby przyszłych rekrutacji bez dodatkowej zgody, oraz powinien je usunąć po zakończeniu rekrutacji).
6. ***Zasada integralności i poufności danych*** – przetwarzanie danych powinno następować w sposób zapewniający im odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych po uwzględnieniu ryzyk.
7. ***Zasada rozliczalności*** – administrator jest odpowiedzialny za przestrzeganie przepisów o ochronie danych osobowych i musi być w stanie wykazać, że się do nich stosuje (np. w razie kontroli powinien wykazać, że realizuje względem osób, których dane dotyczą, obowiązek informacyjny lub stosuje odpowiednie środki techniczne

i organizacyjne zabezpieczające przed nieuprawnionym dostępem do danych ze strony osób trzecich).

8. ***Polityka czystego biurka*** – należy pamiętać o konieczności przechowywania wszelkich nośników danych osobowych (np. dokumentów) poza zasięg wzroku i zasięg dłoni osób postronnych (w przypadku pracy zdalnej w domu – także domowników), a także o przechowywaniu ich pod kluczem.
9. ***Polityka czystego ekranu*** – należy pamiętać o konieczności blokowania komputerów i innych urządzeń, na których przetwarzamy dane osobowe, przed każdorazowym, nawet chwilowym opuszczeniem stanowiska pracy (np. stosować skrót klawiszowy WIN+L). Dodatkowo należy uniemożliwiać wgląd w treści wyświetlane na monitorach osobom nieupoważnionym – choćby poprzez odpowiednie ustawienie ekranu lub stosowanie filtrów prywatyzujących (w przypadku pracy zdalnej w domu – osobami nieupoważnionymi są także domownicy).
10. ***Polityka czystego druku*** – należy pamiętać o konieczności odbierania wszelkich wydruków z urządzeń drukujących niezwłocznie po ich wydrukowaniu.
11. ***Procedura niszczenia*** – należy pamiętać o konieczności niszczenia dokumentów zawierających dane osobowe z wykorzystaniem niszczarek o odpowiedniej klasie niszczenia lub pojemników do utylizacji dokumentacji zawierającej dane osobowe. Zakazane jest wyrzucanie dokumentów do zwykłych śmietników w stopniu zniszczenia umożliwiającym ich odczytanie.
12. ***Procedura korzystania z urządzeń mobilnych*** – należy pamiętać o konieczności zabezpieczania sprzętu informatycznego (laptopy, smartfony, tablety, pendrive'y) przed wyniesieniem ich poza obszar pracy (obszar przetwarzania danych) – hasłem, PINem, przy zastosowaniu technologii biometrycznych oraz szyfrowaniu zawartych na nich danych.
13. ***Procedura korzystania z Internetu*** – należy pamiętać o zakazie stosowania zapamiętywania haseł w przeglądarkach internetowych oraz historii wyszukiwania – okresowo należy czyścić historię przeglądania lub wyłączyć jej zapamiętywanie.
14. ***Procedura korzystania z poczty elektronicznej*** – należy pamiętać o weryfikacji adresów mailowych w procesie wysyłania, tak aby adresacja była prawidłowa – w szczególności należy weryfikować opcje: „ukryte - do wiadomości"/ „jawne – do wiadomości". Jeżeli wysyłamy maila do więcej niż jednego adresata – odbiorców wpisujemy w opcji „UDW" – do ukrytej widomości, a maila adresujemy do siebie. Dodatkowo nie wolno korzystać z odnośników znajdujących się w mailach nieznanego pochodzenia ani otwierać znajdujących się w nich załączników.

II. Zalecane formy zabezpieczeń technicznych i organizacyjnych zapewniających bezpieczeństwo informacji i danych osobowych podczas pracy poza miejscem jej stałego wykonywania

W celu zapewnienia bezpieczeństwa informacji i ochrony danych osobowych przetwarzanych podczas pracy zdalnej Administrator danych zaleca:

URZĄDZENIA

1. Urządzenia i oprogramowanie przekazane przez pracodawcę do pracy zdalnej służą do wykonywania obowiązków służbowych. Dlatego też postępuj zgodnie z przyjętą w organizacji procedurą ochrony danych osobowych i bezpieczeństwa informacji.
2. Nie instaluj dodatkowych aplikacji i oprogramowania niezgodnych z procedurą bezpieczeństwa organizacji.

3. Korzystaj tylko ze swojego konta użytkownika. Nie udostępniaj swojego konta użytkownika innym osobom. Monitoruj aktywności na koncie.
4. Stosuj oprogramowanie antywirusowe.
5. Upewnij się, że wszystkie urządzenia z jakich korzystasz mają niezbędne aktualizacje systemu operacyjnego (m.in. Windows, IOS lub Android), oprogramowania oraz systemu antywirusowego.
6. Zanim przystąpisz do pracy, wydziel sobie odpowiednią przestrzeń, tak aby ewentualne osoby postronne, nie miały dostępu do używanych urządzeń i dokumentów, nad którymi pracujesz.
7. Odchodząc od stanowiska pracy każdorazowo blokuj urządzenie, na którym pracujesz i chowaj dokumenty do szafy zamykanej na klucz. Korzystaj z automatycznego blokowania komputera lub innego urządzenia elektronicznego w przypadku każdego odejścia od stanowiska pracy (także w razie krótkiego okresu nieaktywności). Odchodząc od komputera lub kończąc korzystanie z innego urządzenia elektronicznego (np. służbowego smartfona) upewnij się, że urządzenie zostało zablokowane. Szybka blokada komputera w systemach Windows jest możliwa za pomocą skrótu klawiszowego WIN+L.
8. Zabezpieczaj swój komputer poprzez używanie silnych haseł dostępu, wielopoziomowe uwierzytelnianie. Pozwoli to na ograniczenia dostępu do urządzenia, a jednocześnie na ograniczenie ryzyka utraty danych w przypadku kradzieży lub zgubienia urządzenia.

1) Minimalne wymogi co do hasła: powinno składać się z co najmniej 8 znaków, w tym z dużych i małych liter oraz cyfr i znaków specjalnych.
2) Skuteczne hasło to: długi zwrot (nie słownikowy) zawierający ww. znaki.
3) Minimalna zasada złożoności hasła - P@$w0rd!”1
4) Tworząc hasło nie używaj:

a) popularnych kombinacji kolejnych klawiszy z klawiatury (np. qwerty, 123456,
b) itp.);
c) samych liter lub cyfr, np. abcdefgh, 123654, itp.;
d) informacji o sobie takich jak: daty urodzenia, numery pesel, imion członków rodziny, zwierząt, ulubionych miejsc, przedmiotów, itp.;
e) frazy użytej do tworzenia loginu;
f) imion, nazwisk lub nazw znanych postaci lub popularnych słów, np. kasia1, batman2, itp.,
g) krótszych niż 8 znaków. Hasła tego typu są proste do zapamiętania, ale także proste do złamania.

5) Dobrą praktyką przy tworzeniu hasła jest używanie:

a) fraz złożonych z kombinacji wszystkich znaków, które nie mają powszechnego sensu, ale są łatwe do zapamiętania, bo mają sens jedynie dla użytkownika, który je wymyślił;
b) fraz bardzo długich: 15-20 znaków, w tym cyfry, słowa zapisane z celowym błędem – ustawione w określonym porządku, gdzie litery zastąpiono znakami specjalnymi, np. a-@, i-1, o=0, s=% itp.

6) Używaj unikatowych haseł, które nie są podobne do poprzednich.
7) Im hasło jest bardziej skomplikowane, tym jego odszyfrowanie przez osobę trzecią lub maszynę będzie bardziej pracochłonne.
8) Hasło powinno być znane wyłącznie Tobie jako użytkownikowi. Nie udostępniaj go, ani nie zapisuj w miejscach dostępnych dla innych osób (m.in. nie zapisuj haseł w przeglądarkach internetowych, na karteczkach, w notatnikach, na tablicach, monitorze czy innych źródłach, które mogą dostać się w niepowołane ręce lub są ogólnodostępne).

9) Stosuj zasadę: jeden program, system, witryna – to jedno hasło, w przypadku jego złamania, pozostałe dane są nadal bezpieczne.
10) Zmieniaj hasła okresowo, a bezzwłocznie gdy choćby podejrzewasz jego ujawnienie.
11) Obowiązkowo zmień hasła w sytuacji podejrzenia jego ujawnienia, np. zgubienia notesu, gdzie było zapisane, lub dowolnego urządzenia czy nośnika gdzie było zapisane, infekcji wirusowej dowolnego urządzenia bądź włamania lub wycieku danych z serwisu, do którego dostępu służyło.
12) Nie zmieniaj hasła w przewidywalny sposób, np. poprzez zwiększanie liczby, zmianę litery na podobnie wyglądający symbol, usuwanie znaku specjalnego lub przełączanie kolejności cyfr lub znaków specjalnych.
13) Korzystaj z managerów haseł.
9. Korzystaj z podwójnego uwierzytelniania w sytuacjach, w których jest to możliwe.
10. Stosuj szyfrowanie dysku komputera.
11. Zachowaj szczególną ostrożność i podejmij odpowiednie środki, aby urządzenia, z których korzystasz podczas pracy, w tym te wykorzystywane do przenoszenia danych, jak laptop, dysk zewnętrzny, pendrive, nie zostały zgubione.
12. Jeśli zgubiłeś urządzenie, na którym pracujesz lub zostało skradzione, natychmiast podejmij odpowiednie kroki, aby o ile to możliwie, zdalnie wyczyścić jego pamięć.
13. Regularnie wykonuj kopie zapasowe – tylko na zabezpieczonych nośnikach (szyfrowany dysk lub pendrive).
14. Wyłącz/zaklej kamery w laptopie (kwestia prywatności pracownika) chyba, że jest on niezbędna do wykonywania obowiązków służbowych, np. do prowadzenia wideokonferencji.

E-MAIL

1. Postępuj zgodnie z obowiązującymi zasadami w organizacji dotyczącymi korzystania ze służbowej poczty elektronicznej (e-mail).
2. Używaj służbowych kont e-mail (odpowiednio zabezpieczonych poprzez szyfrowanie). Jeśli pracujesz przetwarzając dane osobowe i musisz używać prywatnego e-maila, upewnij się, że treść i załączniki są właściwie szyfrowane. Nie używaj danych osobowych lub poufnych informacji w temacie wiadomości ani w treści maila.
3. Przed wysłaniem maila upewnij się, że wysyłasz go do właściwego adresata – sprawdź ponownie odbiorcę. Zachowaj szczególną ostrożność, zwłaszcza jeśli wiadomość zawiera dane osobowe lub informacje poufne.
4. Dokładnie sprawdź nadawcę maila. Nie otwieraj wiadomości od nieznanych adresatów, a zwłaszcza nie otwieraj załączników oraz nie klikaj w link zawarty w takiej wiadomości. To może być atak phishingowy. Otwierając załączniki od nieznanych nadawców (zwłaszcza typu: .zip, .xlsm, .pdf, .exe) lub klikając na link w mailu od nieznanego nadawcy można zainfekować komputer oraz inne komputery w sieci (lub inne urządzenia). Takie zachowania to wysokie ryzyko bezpowrotnej utraty danych.
5. Korzystając z funkcji poczty elektronicznej, umożliwiającej wysłanie wiadomości do wielu odbiorców naraz, stosuj opcję: „ukryte do wiadomości” (w skrócie: „UDW”, ang.: „BCC”), zamiast opcji: „do wiadomości” (w skrócie: „DW”, ang.: „CC”). Pole „UDW” pozwala na wysyłkę wiadomości w taki sposób, że odbiorcy nie widzą wzajemnie swoich adresów.

INTERNET

1. Nie korzystaj z otwartych sieci Wi-Fi.

2. W przypadku korzystania z prywatnej (domowej) sieci Wi-Fi – odpowiednio zabezpiecz sieć poprzez ustawienie silnego hasła dostępowego oraz sprawdzenie oprogramowania routera Wi-Fi (aktualizuj jego oprogramowanie).
3. Unikaj mediów społecznościowych jako środka komunikacji służbowej, w szczególności do przekazywania danych osobowych.
4. O ile to możliwe stosuj oprogramowanie pozwalające na podłączenie wirtualnej sieci prywatnej VPN (dotyczy zapewnienia bezpieczeństwa transferowanych danych oraz możliwości dostępu do zasobów danych Pracodawcy).
5. Zachowaj szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania loginu, hasła, PINu, numeru kart płatniczych przez Internet. Szczególnie dotyczy to żądania podania takich informacji przez rzekomy bank.

DOKUMENTY

1. Chroń dokumenty przed uszkodzeniem, zniszczeniem lub zagubieniem, a także dostępem osób nieupoważnionych.
2. Odchodząc od stanowiska pracy schowaj i zabezpiecz dokumenty, tak aby osoby nieupoważnione nie miały wglądu do nich.
3. Nie zostawiaj osób nieupoważnionych samych w pomieszczeniu z służbowymi dokumentami.
4. Unikaj fotografowania dokumentacji – robienie zdjęć za pomocą telefonu komórkowego wiąże się z zapisywaniem danych w jego pamięci, a istnieje prawdopodobieństwo przesłania ich do usług chmurowych (np. zdjęcia Google).
5. Unikaj drukowania dokumentów na prywatnych drukarkach – większość prywatnych drukarek posiada możliwość łączenia się z siecią i jest podatna na uzyskanie nieautoryzowanego dostępu, dodatkowo drukarki posiadają własną pamięć podręczną, w której mogą pozostać drukowane pliki z danymi służbowym.

DOSTĘP DO SIECI I CHMURY, ARCHIWIZACJA

1. Korzystaj tylko z zaufanego dostępu do sieci lub chmury oraz przestrzegaj wszelkich zasad i procedur organizacyjnych dotyczących logowania i udostępniania danych.
2. Jeśli natomiast nie pracujesz w chmurze lub nie masz dostępu do sieci, zadbaj aby przechowywane dane były w bezpieczny sposób zarchiwizowane.

III. Najczęściej występujące zagrożenia w związku z przetwarzaniem danych osobowych

Administrator danych przypomina o najczęściej występujących zagrożeniach – sytuacjach, które zagrażają bezpieczeństwu danych osobowych.

1. Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji lub systemu operacyjnego, umożliwiające dostęp do bazy danych osobowych osobie nieuprawnionej (w przypadku pracy zdalnej w domu jako osoby nieuprawnione należy traktować również domowników).
2. Dopuszczenie do korzystania z systemu operacyjnego lub aplikacji umożliwiających dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony.
3. Pozostawienie w miejscu widocznym lub oczywistym zapisanego hasła dostępu do urządzenia wykorzystywanego do przetwarzania danych, konta użytkownika, systemu

(aplikacji), bazy danych osobowych lub sieci, jak również jego współdzielenie z osobami trzecimi.

4. Przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób nieupoważnionych – w zasięgu ich wzroku lub dłoni (w przypadku pracy zdalnej w domu jako osoby nieuprawnione należy również traktować domowników).
5. Wyrzucanie dokumentów do zwykłych śmietników w stopniu zniszczenia umożliwiającym ich odczytanie – niekorzystanie z niszczarek o odpowiedniej klasie niszczenia.
6. Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe – niezapewnienie polityki czystego ekranu.
7. Sporządzanie kopii danych na nośnikach danych w sytuacjach nieprzewidzianych procedurą – nieautoryzowane wynoszenie danych osobowych.
8. Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym i dokumentami zawierającymi dane osobowe lub informacje poufne – pozostawianie osób nieupoważnionych bez nadzoru.
9. Otwieranie poczty elektronicznej pochodzącej od nieznanych nadawców, a w szczególności załączników, odnośników.
10. Korzystanie z publicznie dostępnych sieci Wi-Fi, które nie posiadają żadnej autoryzacji – brak hasła.
11. Wysłanie wiadomości e-mail do wielu odbiorców (mailingu masowego) z wpisaniem adresów w pole „DO:” lub „DW:” zamiast „UDW:”.

Załącznik nr 2
do Regulaminu pracy zdalnej obowiązującego
w Szkole Podstawowej nr 18 im. Macieja Rataja w Lublinie

Oświadczenia Pracownika o zapoznaniu się z Regulaminem pracy zdalnej

.....
(miejscowość, data)

.....
.....
(dane pracownika, stanowisko)

Oświadczenie Pracownika

Ja, niżej podpisany/podpisana
……. oświadczam, że:

- zapoznałem /am się, przed rozpoczęciem pracy w trybie pracy zdalnej z:
  1. regulaminem pracy zdalnej obowiązującym u Pracodawcy;
  2. załącznikiem nr 1 pn.: „Obowiązkowe zasady postępowania w związku z przetwarzaniem danych osobowych. Zalecane formy zabezpieczeń technicznych i organizacyjnych.”;
  3. rozporządzeniem Ministra Pracy i Polityki Socjalnej z dnia 01.12.1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe (Dz.U. z 1998 r., Nr 148, poz. 973).
- znane są mi zasady ochrony danych osobowych;
- znane są mi zasady bezpieczeństwa i higieny pracy;

.....
(data i podpis pracownika)