

Zarządzenie Nr 529/2020

Burmistrza Pyrzyc

z dnia 10 listopada 2020 roku

w sprawie wprowadzenia Regulaminu pracy zdalnej dla pracowników Urzędu Miejskiego w Pyrzycach

Na podstawie art. 3 ustawy z dnia 2 marca 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. 1842) oraz art. 33 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz.U. z 2020 r., poz. 713), zarządzam co następuje:

§1. W celu zapobiegania, przeciwdziałania COVID-19 wprowadza się Regulamin pracy zdalnej obowiązujący pracowników Urzędu Miejskiego w Pyrzycach, którego treść określa załącznik do niniejszego zarządzenia.

§2. Uchyla się Zarządzenie Nr 359/A Burmistrza Pyrzyc z dnia 23 marca 2020 r.

§ 3. Wykonanie zarządzenia powierza się Sekretarzowi Gminy Pyrzyce.

§ 4. Zarządzenie wchodzi w życie z dniem podjęcia.


BURMISTRZ
Marzena Podzińska

Załącznik do Zarządzenia Nr 529/2020

Burmistrza Pyrzyc z dnia
10 listopada 2020r.

REGULAMIN PRACY ZDALNEJ

Rozdział 1

Postanowienia ogólne

§ 1

1. Pracodawca może polecić Pracownikowi wykonywanie, przez czas oznaczony, pracy określonej w umowie o pracę, poza miejscem jej stałego wykonywania (praca zdalna) w okresie obowiązywania stanu zagrożenia epidemicznego albo stanu epidemii, ogłoszonego z powodu COVID-19, oraz w okresie 3 miesięcy po ich odwołaniu, w celu przeciwdziałania COVID-19.
2. Niniejszy Regulamin określa zasady podejmowania i wykonywania pracy zdalnej oraz związane z tym prawa i obowiązki Pracodawcy i Pracowników.
3. Regulamin obowiązuje wszystkie osoby, które wykonują pracę zdalną bez względu na formę zatrudnienia.
4. Praca zdalna wskazana w ust. 1 nie stanowi telepracy w rozumieniu Kodeksu pracy.

§ 2

Niniejszy Regulamin został opracowany na podstawie następujących aktów prawnych:

- a) 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: „RODO”;
- b) ustawy z dnia 10.05.2018 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781), dalej: „uodo”;
- c) 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: „ustawa o szczególnych rozwiązaniach związanych z COVID-19”;
- d) ustawy z dnia 26.06.1974 r. Kodeks pracy (t.j.: Dz. U. z 2019 r., poz. 1040 z późn. zm.); dalej: „Kodeks pracy”.

Rozdział 2

Polecenie pracy zdalnej

§ 3

1. Polecenie pracy zdalnej wydawane jest na wniosek Pracownika lub na polecenie Pracodawcy według wzoru określonego w **Załączniku nr 1**.
2. Polecenie pracy zdalnej musi zostać wcześniej uzgodnione z Administratorem Danych Osobowych (ADO) oraz Administratorem Systemów Informatycznych (ASI).
3. W przypadku Polecenia pracy zdalnej, ADO lub bezpośredni przełożony wydaje zgodę na świadczenie pracy w trybie zdalnym **Załącznik nr 2**.
4. Wyżej wymienione polecenia korespondują z wcześniej wydanymi upoważnieniami do przetwarzania danych osobowych.

§ 4

1. Wykonywanie pracy zdalnej może zostać polecane lub uzgodnione z Pracownikiem na jego wniosek, jeżeli Pracownik ma umiejętności i możliwości techniczne oraz lokalowe do wykonywania takiej pracy i pozwala na to rodzaj pracy. W szczególności praca zdalna może być wykonywana przy wykorzystaniu środków bezpośredniego porozumiewania się na odległość lub dotyczyć wykonywania części wytwórczych lub usług materialnych.
2. W Poleceniu pracy zdalnej określa się w miarę możliwości termin wykonywania pracy zdalnej.
3. Pracodawca w każdej chwili może cofnąć polecenie lub zgodę na wykonywanie pracy zdalnej oraz zobowiązać Pracownika do świadczenia pracy w stałym miejscu świadczenia pracy określonym w umowie o pracę.

Rozdział 3

Przystąpienie do pracy zdalnej

§ 5

1. Pracownik przed przystąpieniem do pracy zdalnej przechodzi szkolenie zgodnie z **Załącznikiem nr 4**, które otrzymuje w formie pisemnej (wydruk) lub drogą elektroniczną (e-mail).
2. Jeżeli zaistnieje taka konieczność ASI nadaje Pracownikowi odpowiednie dane uwierzytelniające niezbędne do wykonywania pracy w trybie zdalnym.
3. Jeżeli praca zdalna wymaga pracy z oprogramowaniem zainstalowanym fizycznie w Urzędzie Miejskim w Pyrzycach, ASI sprawdza czy istnieje możliwość bezpiecznego zdalnego podłączenia komputera klienckiego z zasobami w Urzędzie przy pomocy sieci Internet. Po dokonaniu takiej analizy ASI przekazuje Pracownikowi Instrukcję bezpiecznego podłączenia wraz z danymi uwierzytelniającymi.
4. Narzędzia i materiały potrzebne do wykonywania pracy zdalnej oraz obsługę logistyczną pracy zdalnej zapewnia Pracodawca. Przy wykonywaniu pracy zdalnej pracownik może używać narzędzi lub materiałów niezapewnionych przez Pracodawcę pod warunkiem, że umożliwia to poszanowanie i ochronę informacji poufnych i innych tajemnic prawnie chronionych, w tym tajemnicy przedsiębiorstwa lub danych osobowych, a także informacji, których ujawnienie mogłoby narazić Pracodawcę na szkodę.
5. Przed przystąpieniem do pracy zdalnej, ASI wydaje sprzęt służbowy jednocześnie odnotowując



w szczególności w Rejestrze wymiennych nośników danych oraz Rejestrze urzędów mających dostęp do sieci numer i symbol/model powierzonego. Co do zasady korzystać należy z poczty służbowej (e-mail służbowy).

6. W każdym wypadku zabrania się wykorzystania zasobów prywatnych, w tym poczty prywatnej do przetwarzania, w szczególności przesyłania danych osobowych.
7. Kierując się potrzebą zapewnienia ciągłości działania organu administracji publicznej, w szczególności uzasadnionych przypadkach ASI, po uzyskaniu opinii IOD, może wyrazić zgodę na wykorzystanie prywatnych urzędów do wykonywania pracy zdalnej, zapewniając niezbędny poziom zabezpieczeń, w szczególności przy wykorzystaniu środków ochrony kryptograficznej.

Rozdział 4

Ogólne warunki wykonywania pracy zdalnej

§ 6

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.
2. 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.
3. W trakcie wykonywania pracy zdalnej Pracownik pracuje w systemie czasu pracy wynikającym z regulaminu pracy lub obowiązującej go umowy o pracę.
4. Praca w trybie zdalnym powinna być wykonywana w godzinach i w dniach normalnej pracy, w których dany Pracownik pracował w miejscu stałego jej wykonywania. Dni wykonywania pracy zdalnej są dniami świadczenia pracy.
5. Uzyskanie prawa do zasiłku opiekuńczego lub dodatkowego zasiłku opiekuńczego z powodu sprawowania opieki nad dzieckiem wyklucza wykonywanie jakiejkolwiek pracy, w tym pracę w trybie zdalnym (na podstawie przepisów prawa). W przypadku korzystania z prawa do zasiłku opiekuńczego lub dodatkowego zasiłku opiekuńczego z powodu sprawowania opieki nad dzieckiem, Pracownik niezwłocznie poinformuje o tym fakcie Pracodawcę.

Rozdział 5

Prawa i obowiązki Pracodawcy

§ 7

1. Pracodawca zobowiązuje się do przekazywania Pracownikowi zadań do wykonania, udzielania informacji merytorycznych oraz organizowania procesu pracy w sposób umożliwiający Pracownikowi pracę w trybie zdalnym.
2. Pracodawca wydaje stosowne polecenia i zgody określone w §3 wobec zaistnienia podstaw do ich wydania.
3. Pracodawca zapoznaje Pracownika z **Załącznikiem nr 3**.



4. Pracodawca zapewnia Pracownikowi w dostępnej w stosunku do faktycznych okoliczności formie, przeprowadzenie szkolenia przygotowawczego przez IOD (**Załącznik nr 4**). Szkolenie dotyczy będzie bezpiecznej pracy z urządzeniami wykorzystywanymi do wykonywania pracy zdalnej oraz dokumentacją papierową, właściwego korzystania z poczty mailowej i zasobów Internetu, zasad komunikowania się poza siedzibą Pracodawcy, niebezpieczeństw związanych z phishingiem.
5. Pracodawca ma prawo:
 - a) powierzyć określone zadania, które powinny być wykonane podczas pracy zdalnej;
 - b) monitorowania wyników pracy (w szczególności za pośrednictwem przyjętego środka komunikacji);
 - c) kontrolować i weryfikować wykonywanie powierzonych zadań, w tym również żądać od Pracownika informacji o ich wynikach, potwierdzenia ich wykonania. Pracodawca może polecić wykonywanie takiej kontroli bezpośrednio przełożonemu pracownikowi, a następnie zobowiązać go do przekazania jej wyników.
6. Pracodawca wykona ocenę ryzyka występujących przy przetwarzaniu danych oraz odnotowuje czynności wykonywane podczas pracy zdalnej w rejestrze czynności przetwarzania danych.

Rozdział 6

Prawa i obowiązki Pracownika

§ 8

1. Pracownik jest zobowiązany do wykonywania pracy zgodnie z treścią umowy łączącej go z Pracodawcą oraz zakresem obowiązków.
2. Obowiązkiem Pracownika jest zastosowanie się do niniejszego Regulaminu pracy zdalnej.
3. Pracownik zobowiązuje się do:
 - a) 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;
 - b) bieżącego informowania o wynikach swojej pracy oraz przedstawiania Pracodawcy wyników swojej pracy, przy pomocy środków komunikacji elektronicznej takich jak: wiadomości e-mail, rozmowy i wiadomości telefoniczne, telekonferencje, a także prowadząc rejestr pracy zdalnej zgodnie z **Załącznikiem nr 5**;
 - c) dbania o powierzony sprzęt, w tym chronienia udostępnionych urządzeń przed zalaniem, zniszczeniem lub kradzieżą,
 - d) korzystania z urządzeń oraz oprogramowania dostarczonego przez Pracodawcę;
 - e) korzystania z poczty służbowej w celu wykonywania swoich obowiązków służbowych.
4. Pracownik po otrzymaniu odpowiedniego polecenia, zostaje zapoznany z **Załącznikiem nr 3**, co potwierdza własnoręcznym podpisem.
5. Obowiązki wykonywane w ramach pracy zdalnej podlegają raportowaniu, w każdym dniu pracy po zakończeniu wykonywania obowiązków, do bezpośredniego przełożonego (**Załącznik nr 5**). Raport należy przesłać na adres e-mail bezpośredniego przełożonego.
6. Bezpośredni przełożony Pracownika wykonującego pracę zdalną zobowiązany jest po zakończeniu okresu świadczenia pracy zdalnej przedłożyć komplet otrzymanych raportów Pracodawcy.



7. Pracownikowi nie przysługuje zwrot kosztów za media i sprzęt wykorzystywany do wykonywania pracy zdalnej w jego miejscu zamieszkania, o ile świadczenia takie nie wynikają z przepisów powszechnie obowiązujących.
8. Pracownik jest zobowiązany do zabezpieczenia urządzeń przed dostępem osób trzecich w trakcie pracy jak i po jej zakończeniu.
9. Jeżeli Pracownikowi powierzone zostaną dokumenty papierowe to ma on obowiązek wydzielenia odrębnego miejsca do ich przechowania, tak aby dokumenty nie uległy uszkodzeniu, zgubieniu bądź zniszczeniu.
10. 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.

§ 9

1. Pracownik ma prawo do wsparcia technicznego ze strony Pracodawcy. W przypadku problemów technicznych Pracownik korzysta z pomocy informatyka Urzędu.
2. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie Pracodawcy.
3. Pracownik zobowiązuje się do stosowania wszystkich znanych mu zasad Ochrony Danych Osobowych stosowanych w miejscu pracy, a w szczególności do wszystkich wytycznych określonych w Regulaminie pracy zdalnej.
4. Pracownik kontaktuje się z IOD w sprawach dotyczących przetwarzania danych osobowych, w szczególności jeżeli pojawiają się jakiegokolwiek wątpliwości w obszarach dotyczących przetwarzania.
5. W przypadku zaistnienia incydentu niebezpieczeństwa, Pracownik natychmiast kontaktuje się z IOD i następnie informuje Pracodawcę. Obowiązują w tym zakresie wszystkie zasady wskazane w Polityce Ochrony Danych.
6. Niewłaściwe przetwarzanie danych, naruszające bezpieczeństwo osób, których dane są przetwarzane, może skutkować wyciągnięciem wobec Pracownika konsekwencji przewidzianych w Kodeksie pracy oraz określonych innymi przepisami prawa.
7. W przypadku gdy niezbędne okaże się wysłanie wiadomości, która zawierać będzie dane osobowe lub tajemnice Pracodawcy/jednostki, taka wiadomość winna zostać zaszyfrowana. Hasło powinno zawierać 8 znaków, w tym: duża i mała litera, cyfra i znak specjalny. Hasło należy wysyłać innym środkiem komunikacji np. SMS lub po dokonaniu wcześniejszej identyfikacji podać osobie, do której kierowana jest korespondencja.
8. Pracownik pracujący zdalnie na sprzętach, stosuje politykę haseł wynikającą z Polityki Ochrony Danych. Jeżeli system nie wymusza zmiany hasła to Pracownik zobowiązany jest do systematycznej zmiany hasła stosując zasady tworzenia haseł opisane w ust. 7.
9. Dokumenty, nośniki pamięci i inne sprzęty wykorzystywane przy pracy, należy zabezpieczyć, a po ustaniu pracy zdalnej, w sposób bezpieczny dostarczyć do miejsca pracy i oddać Pracodawcy.



Rozdział 7

Bezpieczeństwo i higiena pracy

§ 10

1. Pracownik zobowiązany jest:
 - a. zapoznać się z wymogami organizacji stanowiska pracy na zajmowanym stanowisku;
 - b. zorganizować w miejscu wykonywania pracy stanowisko pracy stosownie do wymogów bezpieczeństwa i higieny pracy oraz zapewnić możliwość skontrolowania spełnienia ww. wymogów przez Pracodawcę – przy zachowaniu prywatności Pracownika i osób przebywających w miejscu świadczenia pracy zdalnej;
 - c. przestrzegać przepisów bezpieczeństwa i higieny pracy w miejscu wykonywania pracy zdalnej.
2. W razie wypadku przy wykonywaniu pracy zdalnej, Pracownik jest zobowiązany niezwłocznie poinformować o tym 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.

Rozdział 8

Postanowienia końcowe

§ 11

1. Każdy z Pracowników ma obowiązek zapoznania się z regulaminem.
2. W sprawach nieuregulowanych 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, w szczególności Politykę Ochrony Danych Osobowych.

Załączniki:

- 1) Załącznik nr 1 – Polecenie pracy zdalnej
- 2) Załącznik nr 2- Zgoda na świadczenie pracy w trybie zdalnym
- 3) Załącznik nr 3 – Zasady pracy w trybie zdalnym przy użyciu sprzętu prywatnego lub służbowego
- 4) Załącznik nr 4 – Szkolenie praca zdalna
- 5) Załącznik nr 5 – Rejestr z pracy zdalnej
- 6) Załącznik nr 6- Procedura postępowania z dokumentacją tradycyjną w ramach pracy w trybie zdalnym

Bez zastrzeżeń i za zgodą rad prawnym
Przemysław Szlowski

ADWOKAT

Dyppok

Pyrzyce, r.

.....
Imię i nazwisko pracownika

.....
Wydział – stanowisko

**POLECENIE PRACODAWCY
wykonywania pracy zdalnej**

Na podstawie art. 3 ustawy z dnia 2 marca 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.), w celu przeciwdziałania COVID-19, polecam Pani/Panu^{1*} wykonywanie pracy określonej w zawartej z Panią/Panem* umowie o pracę oraz zadań wynikających z zakresu obowiązków służbowych, poza miejscem jej stałego wykonywania, czyli w trybie pracy zdalnej w miejscu zamieszkania Pracownika, w okresie od do

Pracodawca może w każdym czasie odwołać Pracownika z tej formy wykonywania pracy i powrócić do umownych warunków pracy.

W związku z powyższym, informuję, że:

- 1) w okresie wykonywania pracy zdalnej nie ulegają zmianie obowiązujące Panią/Pana* godziny rozpoczynania, kończenia pracy oraz dotychczasowe zasady korzystania z przerw w pracy;
- 2) podczas wykonywania pracy zdalnej jest Pani/Pan zobowiązana/y do przestrzegania przepisów o ochronie danych osobowych wynikających z rozporządzenia Parlamentu

^{1*} Niepotrzebne skreślić

Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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 (ogólnego rozporządzenia o ochronie danych osobowych - RODO) oraz innych przepisów szczegółowych odnoszących się do ochrony danych osobowych;

3) ma Pani/Pan* obowiązek:

- a. przestrzegania regulacji wewnętrznych (w szczególności tych zawartych w regulaminie pracy) oraz innych przepisów, przestrzeganie których było wymagane przed poleceniem pracy zdalnej,
- b. wykonywania pracy przy zachowaniu bezpiecznych i higienicznych warunków pracy,
- c. świadczenia pracy w godzinach nadliczbowych wyłącznie na polecenie przełożonego,
- d. dbania o bezpieczne przetwarzanie powierzonych Pani/Panu danych osobowych,
- e. ewidencjonowania wykonanych w trybie pracy zdalnej czynności,
- f. pozostawania w kontakcie z Pracodawcą pod telefonem oraz mailem w ustalonych godzinach pracy.

.....
podpis pracodawcy

.....
data i czytelny podpis pracownika

Bez zastrzeżeń i bezpodległym prawnym
Przemysław Słozowski

ADWOKAT

Kujak

Znak: Pyrzyce, dnia

I. Zgoda na świadczenie pracy w trybie zdalnym

Na podstawie art.
.....

Wyrażam zgodę na świadczenie pracy w trybie zdalnym Pani/Panu

.....
(imię i nazwisko pracownika)

.....
(zajmowane stanowisko)

w godzinach pracy Urzędu , na warunkach określonych w umowie o pracę, w zakresie czynności oraz Regulaminie pracy zdalnej.

Jednocześnie w sytuacji wymagającej Pana/Pani obecności w pracy jest Pan/Pani zobowiązany/zobowiązana do niezwłocznego stawienia się w Urzędzie.

Okres obowiązywania zgody: od dnia do dnia

.....
(Podpis ADO/pracodawcy)

II. Uwagi o wycofaniu zgody i zablokowaniu konta w systemie informatycznym

Zgodę wycofano w dniu z powodu

W dniu zostało zablokowane konto w systemie informatycznym utworzone ze względu na wykonywanie pracy zdalnej.

.....
(Miejscowość i data)

.....
(Podpis osoby wycofującej zgodę)

Otrzymują:

1. IOD
2. Informatycy
3. ASI
4.

Bez zastrzeżeń i uwag zгідem prawnym
Przemysław Szozowski

ADWOKAT

Dyja

Zasady pracy w trybie zdalnym przy użyciu sprzętu służbowego

- I. Administrator danych osobowych (ADO), w związku z wykonywaniem pracy w trybie zdalnym, przypomina i poleca stosować najważniejsze zasady mające na celu zgodne z prawem przetwarzanie danych osobowych.
- II. Każdy kto przetwarza dane osobowe posiadane przez ADO poza miejscem pracy (w trybie pracy zdalnej w miejscu do tego wyznaczonym), zobowiązany jest do stosowania przy przetwarzaniu danych osobowych postanowień zawartych poniżej:
 - 1) Pracownik wykonując pracę zdalną z wykorzystaniem urządzeń służbowych, tzn. otrzymanych od Pracodawcy.
 - 2) Wykorzystanie innych urządzeń może nastąpić wyłącznie po uzyskaniu uprzedniej zgody ASI, zgodnie z postanowieniami § 5 ust. 7 Regulaminu pracy zdalnej.
 - 3) Podczas korzystania z Internetu należy:
 - a) dysponować bezpieczną siecią domową - należy upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania, w szczególności korzystanie z Internetu z sieci WiFi powinno wymagać szyfrowania WPA2.
 - b) nie korzystać z niezabezpieczonych (otwartych) sieci WiFi;
 - c) nie stosować mediów społecznościowych jako środka komunikacji służbowej, w szczególności do przekazywania danych osobowych;
 - d) zachować 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, PIN-u, numeru kart płatniczych przez Internet. Szczególnie dotyczy to żądania podania takich informacji przez rzekomy bank;
 - e) wyłączyć autouzupełnianie i zapamiętywanie hasła w przeglądarce internetowej;
 - f) zachować szczególne warunki bezpieczeństwa i poufności w zakresie korespondencji służbowej i ochrony danych osobowych;
 - g) niezwłocznie zakończyć pracę, w tym zerwać połączenie, w przypadku ujawnienia się przesłanek mogących świadczyć o naruszeniu bezpieczeństwa zasobów;
 - h) nie zapisywać haseł w przeglądarkach internetowych.
 - 4) W razie wątpliwości co do sposobów zabezpieczenia sieci domowej należy skontaktować się z ASI i postępować zgodnie z przekazanymi przez ASI instrukcjami.
 - 5) Pracownik jest zobowiązany przestrzegać w trybie pracy zdalnej Polityki haseł, Polityki czystego ekranu i biurka – zgodnie z zasadami wskazanymi w Polityce Ochrony Danych.
 - 6) Pracownik wykonując czynności zawodowe w domu powinien zadbać o należyte zabezpieczenie dostępu do informacji przed nieautoryzowanym dostępem osób trzecich (m.in. uniemożliwienie podglądu monitora osobom postronnym).

- 7) Niedozwolone jest podejmowanie pracy w trybie zdalnym w miejscach publicznych, takich jak kawiarnie, restauracje, galerie handlowe, gdzie osoby postronne mogłyby usłyszeć fragmenty służbowych rozmów lub zapoznać się z fragmentami wykonywanej pracy.
- 8) Odchodząc od komputera lub kończąc korzystanie z innego sprzętu elektronicznego należy upewnić się, że urządzenie zostało zablokowane oraz, że zostały schowane i zabezpieczone dokumenty przed dostępem osób trzecich.
- 9) Pracownik jest zobowiązany chronić dokumenty przed uszkodzeniem, zniszczeniem lub zagubieniem. 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).
- 10) W przypadku stwierdzenia pojawienia się złośliwego oprogramowania i braku możliwości usunięcia go przez program antywirusowy, Pracownik powinien niezwłocznie skontaktować się z Administratorem Systemów Informatycznych (ASI).
- 11) Na Pracowniku ciąży obowiązek niezwłocznego powiadomienia ASI oraz IOD o okolicznościach mogących świadczyć o utracie poufności, integralności lub dostępności do aktywów lub zasobów.
- 12) Pracownik wykonując czynności zawodowe w trybie pracy zdalnej obowiązany jest do przestrzegania zasad BHP.
- 13) W razie wypadku przy wykonywaniu pracy w trybie zdalnym Pracownik jest zobowiązany niezwłocznie poinformować o tym telefonicznie Pracodawcę. 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.
- 14) Pracownik wykonując czynności zawodowe w trybie pracy zdalnej ma obowiązek pozostawania w stałym kontakcie z Pracodawcą.
- 15) Pracownikowi nie przysługuje zwrot kosztów z tytułu mediów i sprzętu zużytych do wykonywania pracy zdalnej ani inne dodatkowe wynagrodzenie, chyba że świadczenia takie wynikają z powszechnie obowiązujących przepisów prawa.
- 16) Pracodawca nie ponosi odpowiedzialności za jakiegokolwiek szkody powstałe w mieniu Pracownika oraz osób trzecich w godzinach pracy w związku z wykonywaniem przez Pracownika pracy zdalnej.
- 17) Przypadki nie stosowania się do niniejszych zasad stanowią ciężkie naruszenie obowiązków pracowniczych.
- 18) Pracownik pozostaje w stałym kontakcie z ASI oraz Inspektorem Ochrony Danych (IOD).
- 19) W przypadku wystąpienia jakichkolwiek wątpliwości w obszarach przetwarzania danych, wymagany jest natychmiastowy kontakt z IOD.
- 20) Podczas pracy zdalnej Pracownik obowiązany jest do zachowania szczególnej ostrożności i dbałości o przetwarzanie danych.



- 21) Niedozwolone jest samodzielne niszczenie dokumentów służbowych w miejscu realizowania pracy zdalnej, w szczególności wyrzucanie dokumentów do zwykłych śmietników w stopniu zniszczenia umożliwiającym ich odczytanie.
- 22) Po zakończeniu pracy zdalnej Pracownik jest obowiązany usunąć z pamięci sprzętu elektronicznego będącego jego własnością wszelkie dane związane z pracą wykonywaną w trybie zdalnym.
- 23) Przed przystąpieniem do pracy w trybie zdalnym Pracownik odbywa szkolenie stanowiące **Załącznik nr 4.**
- 24) Szkolenie zostanie przekazane Pracownikowi drogą elektroniczną przez e-mail lub w formie papierowej przez bezpośredniego przełożonego.

OŚWIADCZENIE

Ja, niżej podpisany/a zapoznałem/łam się z Regulaminem pracy zdalnej oraz z powyższymi zasadami pracy w trybie zdalnym przy użyciu sprzętu służbowego i zobowiązuję się do ich przestrzegania.

.....

(data i czytelny podpis pracownika)

Bez zastrzeżeń pod względem prawnym

Przemysław Słozowski

ADWOKAT

Ryjak

SZKOLENIE – PRACA ZDALNA

Załącznik nr 4 Regulaminu pracy zdalnej

SZKOLENIE – PRACA ZDALNA

Pracowniku,

Pamiętaj, że 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** przestregania zasad określonych w obowiązującej u Pracodawcy dokumentacji z zakresu ochrony danych osobowych i bezpieczeństwa informacji, w tym w szczególności w Polityce ochrony danych osobowych

SZKOLENIE – PRACA ZDALNA

Miejsce wykonywania pracy zdalnej

- ✓ 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 fragmentem wykonywanej pracy.
- ✓ Pracując w miejscu zamieszkania, Pracownik powinien zapewnić, aby osoby nieupoważnione, w tym domownicy lub współlokatorzy, miały wgląd w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera, a także organizowanie pracy dokumentami w sposób uniemożliwiający wgląd.

SZKOLENIE – PRACA ZDALNA

Miejsce wykonywania pracy zdalnej

- ✓ Odchodząc od komputera należy upewnić się, że urządzenie zostało zablokowane.
- ✓ Odchodząc od stanowiska pracy Pracownik jest zobowiązany skorzystać z zabezpieczeń dokumenty przed dostępem osób trzecich.
- ✓ Pracownik jest zobowiązany chronić dokumenty przed uszkodzeniem, zniszczeniem lub zagubieniem.
- ✓ 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).

SZKOLENIE – PRACA ZDALNA

Urządzenia do wykonywania pracy zdalnej

- ✓ Jeżeli do świadczenia pracy zdalnej zostały Pracownik udostępnione urządzenia służbowe np. laptop to Pracownik zobowiązany jest do wykonywania obowiązków służbowych wyłączeni z wykorzystaniem sprzętu otrzymanego od Pracodawcy.
- ✓ Jeżeli nie jest możliwe wykonywanie przez Pracownika pracy zdalnej wykorzystaniem służbowego sprzętu, informuje on o tym Pracodawcę
- ✓ Zabronione jest udostępnianie służbowych urządzeń wykorzystywanych do realizowania pracy zdalnej innym osobom nieupoważnionym, np. domownikom, współlokatorom.

SZKOLENIE – PRACA ZDALNA

Urządzenia do wykonywania pracy zdalnej

Korzystając ze sprzętu służbowego należy pamiętać o tym, że:

- ✚ urządzenia i oprogramowanie przekazane przez pracodawcę do pracy zdalnej służy wykonywaniu obowiązków służbowych;
- ✚ nie wolno na nich instalować dodatkowych aplikacji i oprogramowania niezgodny z Polityką ochrony danych osobowych;
- ✚ należy korzystać tylko ze swojego konta użytkownika - nie wolno go udostępniać in osobom;
- ✚ trzeba stosować na bieżąco aktualizowane oprogramowanie antywirusowe;
- ✚ odchodząc od stanowiska pracy każdorazowo trzeba blokować urządzenie, na które pracujemy i zabezpieczać dokumenty;
- ✚ konieczne jest zabezpieczenie komputera przez używanie silnych haseł dostępu. Pozwól na ograniczenia dostępu do urządzenia, a jednocześnie na ograniczenie ryzyka utraty danych w przypadku kradzieży lub zgubienia urządzenia.

SZKOLENIE – PRACA ZDALNA

Ogólne zasady dotyczące haseł czyli Polityka haseł są następujące:

- ❖ hasła nie mogą być ujawniane innym osobom;
- ❖ hasła nie mogą być zapisywane, chyba że w bezpieczny sposób, zaakceptowany przez Inform: oraz Inspektora Ochrony Danych;
- ❖ hasło musi zostać natychmiast zmienione jeżeli istnieje podejrzenie, że hasło lub sy informatyczny mógł zostać naruszony; jeżeli Pracownik nie może zmienić hasła musi niezwłto poinformować o tym Informatyka;
- ❖ hasła muszą spełniać następujące wymagania: zawierać co najmniej 8 znaków, zawierać co najr 1 cyfrę, zawierać co najmniej 1 znak specjalny i hasło musi być odmienne od 3 wcześniejszych h
- ❖ hasła muszą być zmieniane stosowanie do okoliczności, jednak nie rzadziej niż raz na 3 miesiące
- ❖ hasło musi być zmienione przy pierwszym logowaniu do sytemu;
- ❖ hasło nie może być zapamiętywane w aplikacjach lub przeglądarkach internetowych;
- ❖ hasła do urządzeń i systemów informatycznych muszą się różnić.

SZKOLENIE – PRACA ZDALNA

Internet w pracy zdalnej

W przypadku korzystania z domowej sieci Wi-Fi, Pracownik zobowiązany jest upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania, w szczególności:

- ✓ korzystanie z Internetu powinno wymagać uwierzytelnienia, poprzez hasło;
- ✓ hasło dostępu powinno spełniać wymogi wskazane w Polityce hasła

SZKOLENIE – PRACA ZDALNA

Internet w pracy zdalnej

- nie należy korzystać z niezabezpieczonych (otwartych) sieci WiFi;
- powinno się unikać mediów społecznościowych jako środka komunikacji służbowej, w szczególności do przekazywania danych osobowych;
- o ile to możliwe, trzeba stosować oprogramowanie pozwalające na podłączenie wirtualnej sieci prywatnej VPN (dotyczy zapewnienia bezpieczeństwa transferowanych danych oraz możliwości dostępu do zasobów danych Pracodawcy);
- należy zachować szczególną ostrożność w przypadku podejrzanego żądania próby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego sklepu, poczty mailowej) lub podania loginu, hasła, PIN-u, numeru płatniczych przez Internet. Szczególnie dotyczy to żądania podania takich informacji przez rzekomy bank.

SZKOLENIE – PRACA ZDALNA

Przekazywanie danych w pracy zdalnej

- Do pracy zdalnej Pracownik powinien wykorzystywać tylko i wyłącznie służbowe programy udostępnione mu przez Pracodawcę.
- Jeżeli niezbędne jest przesłanie, w tym przekazywanie z wykorzystaniem poczty elektronicznej (mail), informacji o charakterze poufnych, w szczególności danych osobowych, to powinny zostać udostępnione w załączniku zabezpieczonym hasłem.
- Zabezpieczeniu powinny podlegać wszelkiego rodzaju dane osobowe, niezależnie od charakteru, nawet jeżeli są to jedynie imiona, nazwiska, czy adresy e-mail pozwalając na identyfikację osoby fizycznej.
- Hasło powinno zostać przekazane odbiorcy inną drogą komunikacji niż dostarczono dane.
- Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą.
- Rekomendowane metody zabezpieczania hasłem to nadanie hasła do pliku, w którym znajdują dane osobowe lub zabezpieczenie pliku lub plików poprzez kompresję z zabezpieczonego archiwum wynikowego hasłem.

SZKOLENIE – PRACA ZDALNA

E-mail w pracy zdalnej

- Prywatna poczta elektroniczna nie powinna być wykorzystywana do celów służbowych. O możliwe, należy korzystać w tym celu jedynie ze służbowego konta e-mail.
- Przed wystaniem maila trzeba upewnić się, że wysłany jest do właściwego adresata – koniecznie jest zachowanie szczególnej ostrożności, zwłaszcza jeśli wiadomość zawiera dane osobowe i informacje poufne.
- Zawsze trzeba dokładnie sprawdzać nadawcę maila. Nie należy otwierać wiadomości nieznanym adresatom, a zwłaszcza załączników oraz nie wolno klikać w link zawarty w wiadomości. To może być atak phishingowy. Otwierając załączniki od nieznanego nadawcy (zwłaszcza typu: .zip, .xls, .pdf, .exe) lub klikając na hiperlink w mailu od nieznanego nadawcy, można zainfekować komputer oraz inne komputery w sieci. Takie zachowania to wysokie ryzyko bezpowrotnej utraty danych.
- Bezwzględnie należy korzystać z funkcji poczty elektronicznej, umożliwiającej wysłanie wiadomości do wielu odbiorców naraz czyli stosować opcję: „ukryte do wiadomości” (w skrócie: „UDW”, „BCC”), zamiast opcji: „do wiadomości” (w skrócie: „DW”, ang.: „CC”). Pole „UDW” pozwala wysłać wiadomości w taki sposób, że odbiorcy nie widzą wzajemnie swoich adresów

SZKOLENIE – PRACA ZDALNA

E-mail w pracy zdalnej

Przy wysyłaniu e-maili istotne są skróty DO, DW i UDW:

DO (TO)

Do odbiorcy. Wpisanie adresatów w to pole powoduje, że każdy, kto otrzymał wiadomość, zobaczy również pozostałych adresatów, do których została wysłana ta wiadomość.

DW (CC)

Do wiadomości. Wpisanie adresata w to pole, oznacza mu, że nie jest głównym adresater wiadomości. Ma wiedzieć, że ten e-mail został wysłany. Adresaci z pola DW są również widoczni pozostałym odbiorców tej wiadomości. Może oczywiście odpowiedzieć na ten e-mail.

UDW (BCC)

Ukryj do wiadomości. Pole to pełni zblizoną funkcję co DW, z tym, że osoby wpisane w to pole niewidoczni dla pozostałych odbiorców. Osobom, które zostały wpisane w to pole, nie zalecać odpowiadania na tą wiadomość. Aby wysłać wiadomość do wielu adresatów z poszanowaniem danych osobowych należy **wyłącznie** stosować funkcję UDW.

SZKOLENIE – PRACA ZDALNA

E-mail w pracy zdalnej

Phishing to jeden z najpopularniejszych typów ataków opartych o wiadomości e-mail. Wykorzystuje technikę polegającą na tym, że przestępca internetowi próbują oszukać, aby odbiorca maila podjął działania zgodnie z ich zamiarem. Cyberprzestępca podszuwając się m.in. pod firmy kurierskie, urzędy, operatory telekomunikacyjnych, czy nawet znajomych, starają się wyłudzić dane do logowania na konta bankowych lub używanych kont społecznościowych, czy systemów.

Wiadomości phishingowe są tak przygotowywane przez cyberprzestępców, aby wyglądały autentycznie, ale w rzeczywistości są fałszywe. Mogą próbować skłonić odbiorcę do ujawnienia poufnych informacji, zawierając link do strony internetowej rozpraszającej szkoc oprogramowanie (często przestępca używają podobnych do autentycznych nazw witryn, które mają zainfekowany załącznik).

Aby uniknąć tego typu ataku należy stosować określone na następnych slajdach d praktyki.

SZKOLENIE – PRACA ZDALNA

E-mail w pracy zdalnej – fałszywe maile

Dobre praktyki:

! trzeba zwracać uwagę na poprawność gramatyczną i sensowność treści. Wiele masowych ataków pochodzi z zagranicy. Tekst tych maili jest tłumaczony na polski za pomocą Google Translator. Na pierwszy rzut oka tekst jest poprawny, a dogłębnie go przeanalizować, to okazuje się, że nie do końca brzmi sensownie. Podobnie z ortografią - niebezpiecznych maili często zawiera błędy ortograficzne, których nie spodziewamy się po korespondencji współpracownika, banku, czy urzędzie;

! należy weryfikować nadawców maili. Atakujący często korzystają z darmowych skrzynek pocztowych i nawet nie się tego zamaskować. Urząd skarbowy, operator telekomunikacyjny, czy inna instytucja nie wysyłają wiadomości gmaila. Posiadanie własnej domeny i korzystanie z kont email w tej domenie jest standardem. Wiadomości z darm. kont powinny być traktowane jako szczególnie podejrzane;

! prawidłowy adres email nadawcy nie powinien jednak usypiać czujności. Atakujący potrafią spreparować wiadomość, która wygląda ona jak wysłana z zupełnie innego konta niż w rzeczywistości – dlatego tak ważne jest zachowanie ostrożności;

SZKOLENIE – PRACA ZDALNA

E-mail w pracy zdalnej – fałszywe maile

Dobre praktyki (c.d.):

! maile związane z kwestiami finansowymi jak faktury, zmiana numeru konta, konieczność dopłaty ci drobnych sum, zablokowanie konta bankowego, czy inne kwestie związane z logowaniem się do konta, egze komornicze, nadpłaty czy niedopłaty w urzędzie skarbowym – to wszystko są kwestie, które szczególnie ci wykorzystują atakujący. Takie maile, choć oczywiście nie tylko takie, mogą zawierać odnośniki do klikni należy sprawdzić, czy one rzeczywiście prowadzą do bezpiecznego miejsca. Oczywiście jeśli tylko pojawia jakiegokolwiek wątpliwości nie należy w nie klikać. Pracownik przynajmniej powinien w przypadku zadzw potwierdzić fakt wystania maila;

! : jeśli w korespondencji mailowej przesyłane są dane osobowe trzeba upewnić się, że:

- nie są przesyłane w nadmiernym zakresie (często wystarczy imię i nazwisko bez nr PESEL czy daty urodzenia
- prawidłowo jest określany krąg adresatów (należy zachować ostrożność przy autouzupelnianiu - zawsze t sprawdzić do kogo kierujemy wiadomość),
- załączniki są właściwie zabezpieczone poprzez np. szyfrowanie (pakowanie i hasłowanie wysyłanych plików)
- nie używamy danych osobowych lub poufnych informacji w temacie wiadomości.

SZKOLENIE – PRACA ZDALNA

Szyfrowanie załączników

WAŻNE!

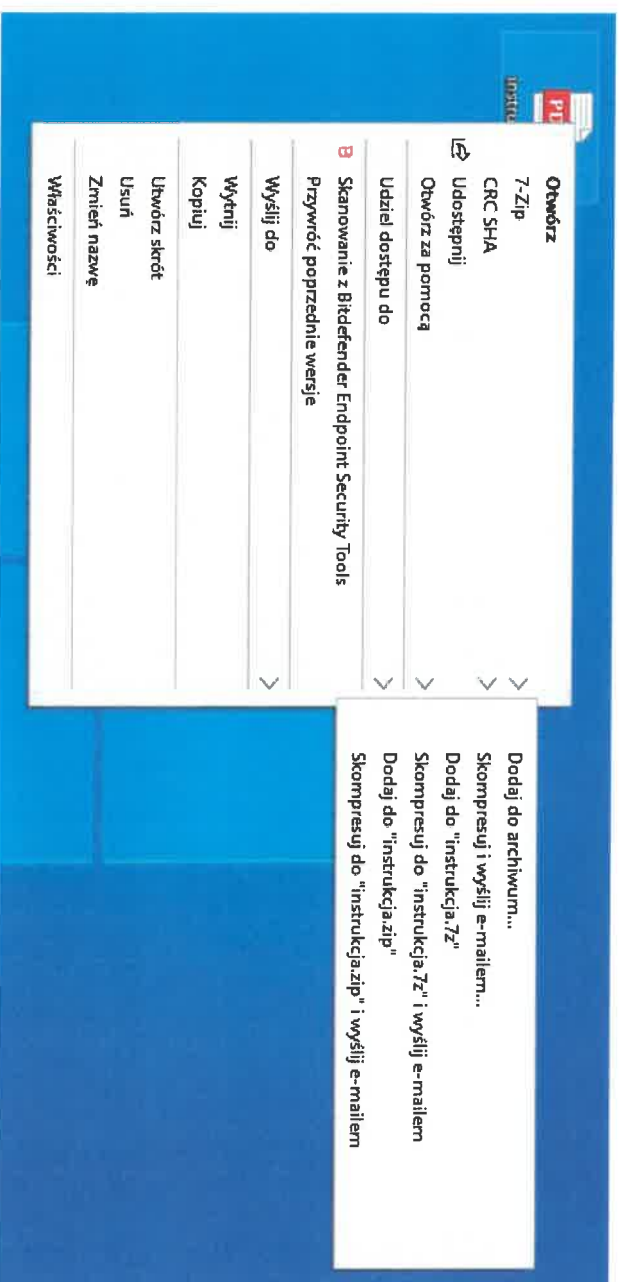
Wszelkie materiały i dokumenty służbowe należy przesłać elektronicznie w formie zaszyfrowanej (w dalszej części instrukcji szyfrowania i odszyfrowania przy użyciu oprogramowania 7ZIP) lub formie zanonimizowanej tj. uniemożliwiającej identyfikację osób.

SZKOLENIE – PRACA ZDALNA

Szyfrowanie załączników

Instrukcja szyfrowania na przykładzie programu 7-zip

- 1) Wybieramy dokument, który chcemy zaszyfrować. Następnie należy kliknąć prawym przyciskiem myszy na wybrani lub katalog i wybrać opcję „7-Zip” → i w kolejnym etapie „Dodaj do archiwum...” :

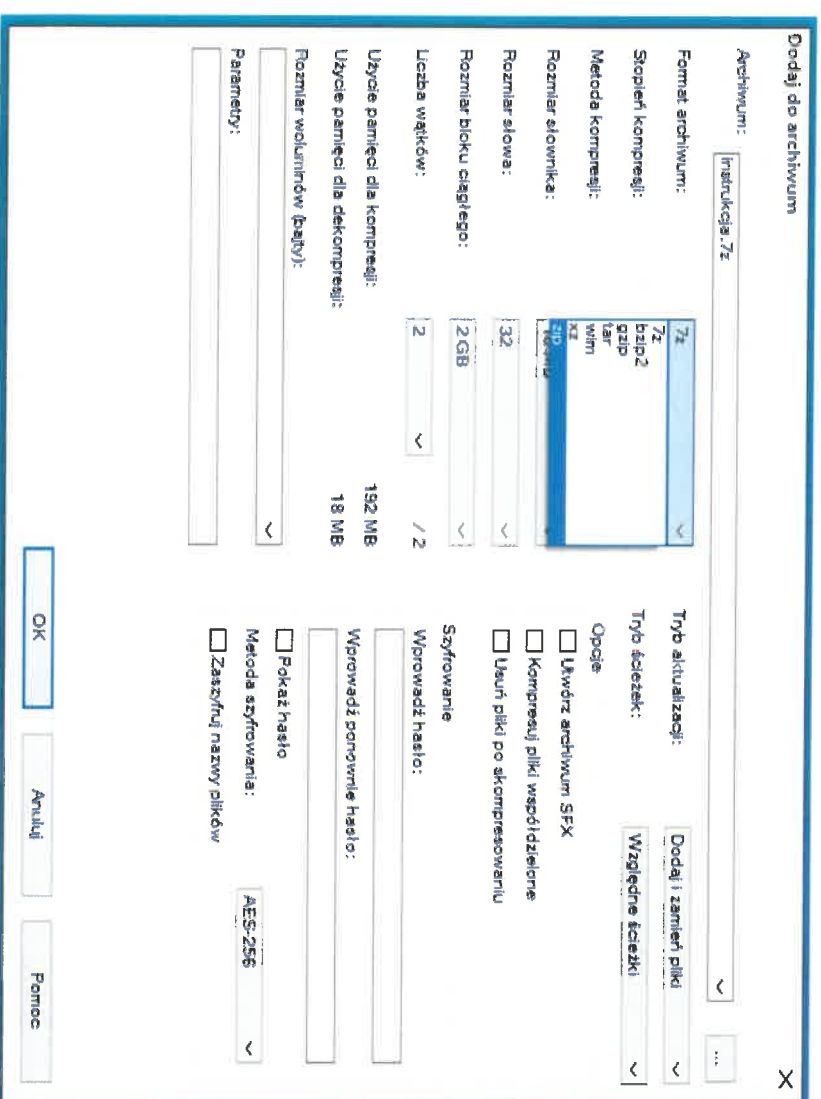


SZKOLENIE – PRACA ZDALNA

Szyfrowanie załączników

Instrukcja szyfrowania na przykładzie programu 7-zip (c.d.)

2) Następnie w otwartym oknie „Dodaj do archiwum...” w polu „Format archiwum:” wybieramy opcję „zip”:

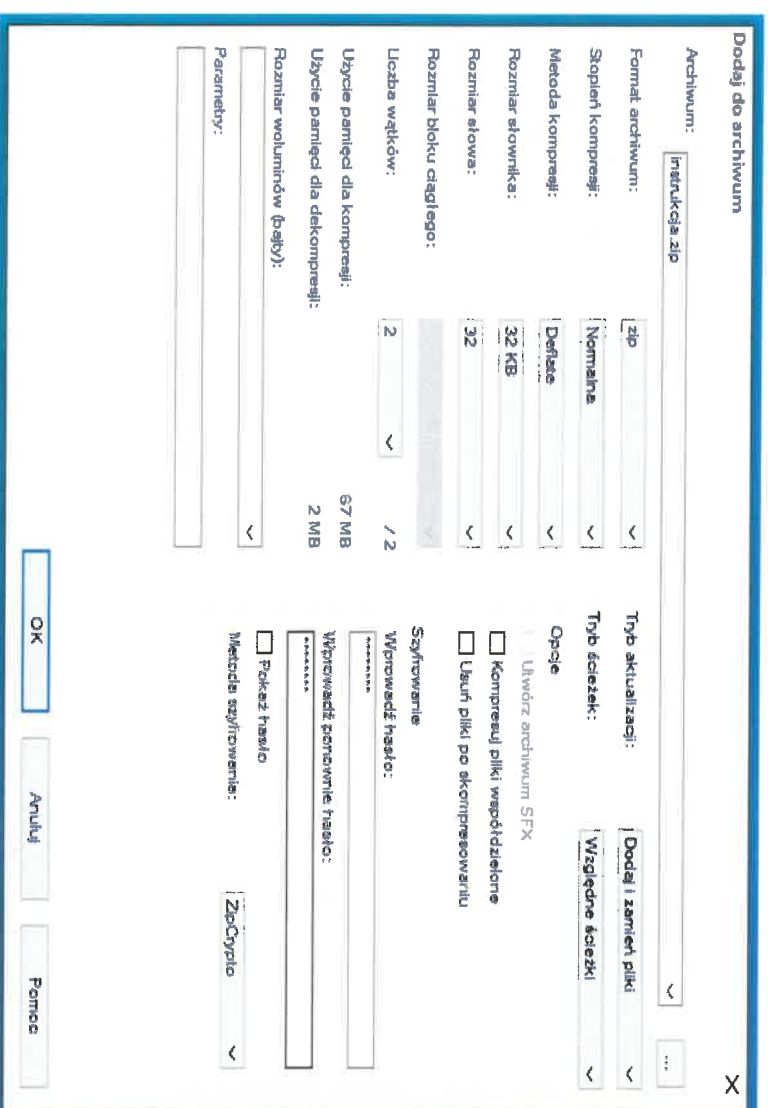


SZKOLENIE – PRACA ZDALNA

Szyfrowanie załączników

Instrukcja szyfrowania na przykładzie programu 7-zip (c.d.)

3) Dalej, nadal w oknie „Dodaj do archiwum...” w polu „Wprowadź hasło:” wpisujemy hasło, którym ma zaszyfrowany plik. W polu „Wprowadź ponownie hasło:” ponownie wpisujemy hasło w celu weryfikacji jego popraw



SZKOLENIE – PRACA ZDALNA

Szyfrowanie załączników

Instrukcja szyfrowania na przykładzie programu 7-zip (c.d.)

4) W wyniku szyfrowania otrzymujemy plik o rozszerzeniu „.zip”, który można bezpiecznie przestać e-mailem jako załącznik.

Instrukcja odszyfrowania pliku/katalogu programem 7-zip

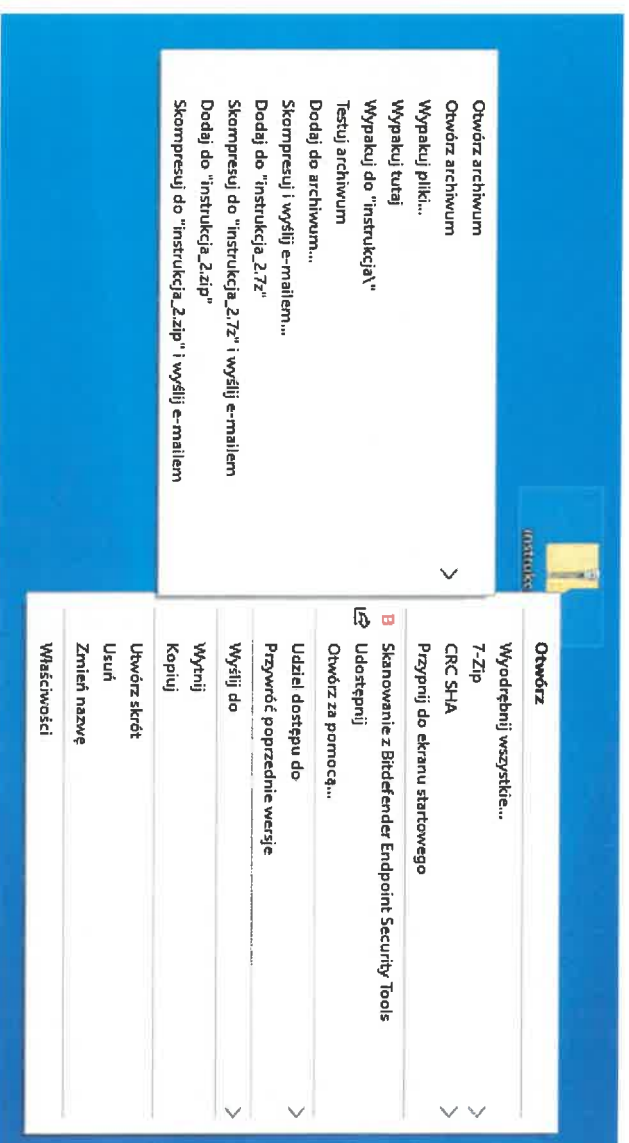
5) Otrzymany od sprawdzonego adresata, zaszyfrowany załącznik w wiadomości e-mail należy zapisać na komputerze.

SZKOLENIE – PRACA ZDALNA

Szyfrowanie załączników

Instrukcja odszyfrowania pliku/katalogu programem 7-zip (c.d.)

2) Na zaszyfrowany plik klikamy prawym przyciskiem myszy i wybieramy opcję „7-Zip” → „Otwórz archiwum”:

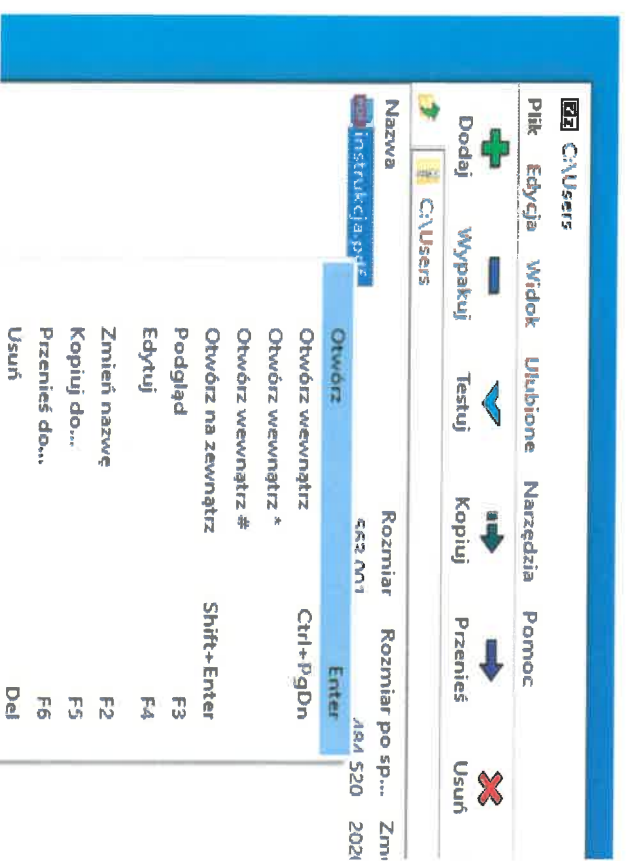


SZKOLENIE – PRACA ZDALNA

Szyfrowanie załączników

Instrukcja odszyfrowania pliku/katalogu programem 7-zip (c.d.)

- 3) Dalej w oknie, które się wyświetli, klikamy prawym przyciskiem myszy plik, który chcemy odszyfrować i wybieramy „Otwórz”:

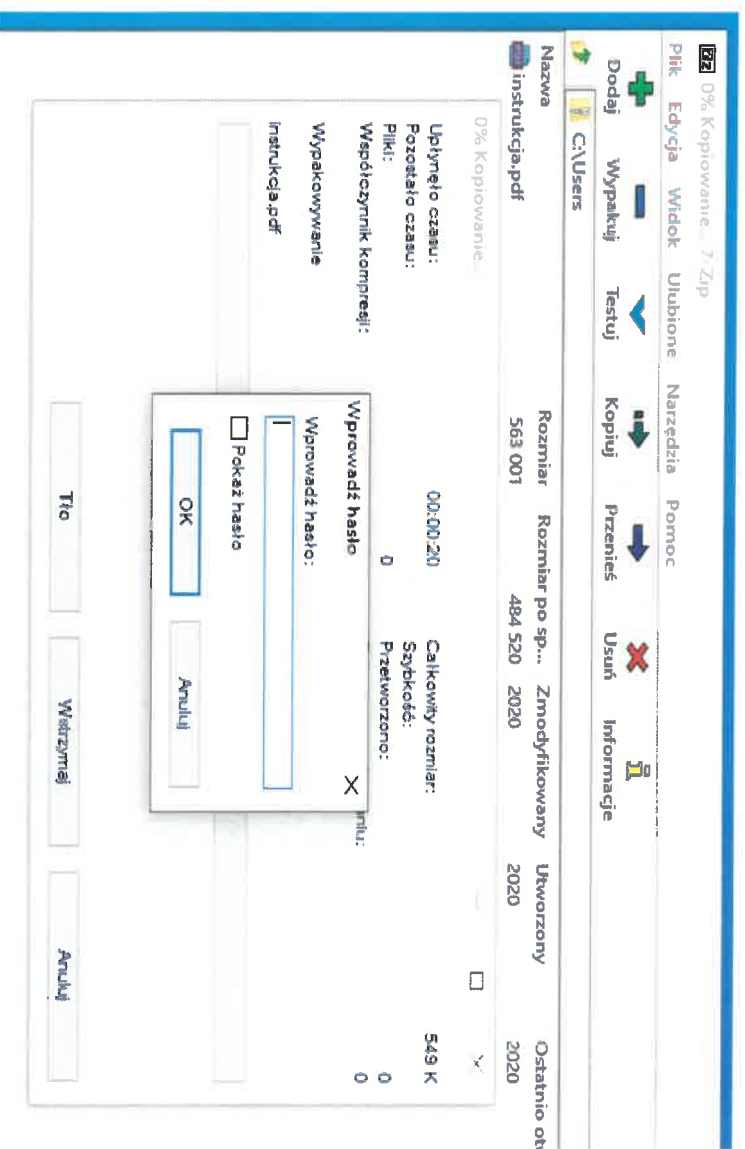


SZKOLENIE – PRACA ZDALNA

Szyfrowanie załączników

Instrukcja odszyfrowania pliku/katalogu programem 7-zip (c.d.)

4) Następnie w oknie, które się wyświetli wpisujemy hasło do archiwum:



SZKOLENIE – PRACA ZDALNA

Dokumenty

- ✓ Należy je chronić przed uszkodzeniem, zniszczeniem lub zagubieniem, a także dostępem nieupoważnionych.
- ✓ Odchodząc od miejsca wykonywania pracy w trybie zdalnym należy pamiętać zabezpieczeniu dokumentów, tak aby osoby nieupoważnione nie miały do nich dostępu.
- ✓ Powinno się unikać fotografowania dokumentacji za pomocą prywatnego telefonu komórkowego, co wiąże się z zapisywaniem danych w jego pamięci.
- ✓ Warto unikać drukowania dokumentów na prywatnych drukarkach – większość druków posiada możliwość łączenia się z siecią i jest podatna na uzyskanie nieautoryzowanego dostępu.

SZKOLENIE – PRACA ZDALNA

Kopowanie i niszczenie dokumentów przy pracy zdalnej

- ✓ Nie należy drukować dokumentów firmowych w ogólnodostępnych punktach ksero.
- ✓ Jeżeli dokumenty, bądź ich kopie okazują się zbędne lub nadmiarowe, należy je podlegają zniszczeniu.
- ✓ Do niszczenia dokumentów należy używać wyłącznie niszczarki.
- ✓ Nie wolno wyrzucać do śmietnika dokumentów i innych informacji jeżeli Pracownik nie ma możliwości wcześniejszego prawidłowego zniszczenia dokumentów, powinien przechowywać je do momentu bezpiecznego zniszczenia w siedzibie Pracodawcy.

SZKOLENIE – PRACA ZDALNA

WAŻNE!

Wszelkie wątpliwości w przypadku zaistnienia sytuacji wskazujących na incydent bezpieczeństwa należy niezwłocznie skonsultować z IOD lub ADO.

Pracownik powinien natychmiast poinformować Pracodawcę o każdej sytuacji która w jego ocenie może być naruszeniem ochrony danych osobowych.

Dane kontaktowe:

1. Katarzyna Jankowska - Inspektor Ochrony Danych (IOD) tel. 698 494 914 e-iod@pyrzyce.um.gov.pl

2. – Administrator Systemów Informatycznych (A
tel..... e-mail

SZKOLENIE – PRACA ZDALNA

DZIĘKUJĘ ZA UWAGĘ!

.....
.....
Pyrzyce, dnia

(Imię i nazwisko pracownika)

.....
(Wydział – stanowisko)

EWIDENCJA WYKONYWANYCH CZYNNOŚCI

Podczas realizowania w dniu pracy zdalnej
wykonałam następujące czynności/zadania*:

.....
.....
.....
.....

Godzina rozpoczęcia i zakończenia pracy:

od do

.....

pracownika)

(czytelny podpis

*uwzględniające w szczególności szczegółowy opis tych czynności/zadań

Dydek

Procedura postępowania z dokumentacją tradycyjną w ramach pracy w trybie zdalnym

1. Jeżeli do pracy zdalnej niezbędny jest dostęp do dokumentów tradycyjnych (papierowych), Pracownik zgłasza do bezpośredniego przełożonego prośbę o możliwość ich zabrania do uzgodnionego miejsca wykonywania pracy zdalnej na czas jej wykonywania.
2. Po otrzymaniu zgody na piśmie lub w formie służbowej wiadomości e-mail, Pracownik sporządza Protokół z przekazania dokumentacji do wykonywania pracy w trybie zdalnym, który stanowi Załącznik nr 1 do niniejszej procedury i zawiera informacje o rodzaju i liczbie pobieranych dokumentów. Każdy pobierany dokument stanowi odrębną pozycję na liście.
3. Bezpośredni przełożony przy wydawaniu dokumentacji Pracownikowi jest zobowiązany zweryfikować ich zgodność z Protokołem, o którym mowa w pkt 2. Kopia Protokołu, o którym mowa w zdaniu poprzednim przekazywana jest Sekretarzowi Gminy niezwłocznie, jednak nie później niż następnego dnia roboczego po jego sporządzeniu.
4. Przed pobraniem dokumentacji powinna zostać zdigitalizowana w sposób ustalony z Informatykiem w celu odtworzenia jej w przypadku utraty.
5. Transport dokumentów może być realizowany wyłącznie w przeznaczonych do tego celu kontenerach transportowych lub kartonach do przechowywania dokumentacji udostępnianych przez pracownika Archiwum. Kontenery transportowe, o którym mowa w zdaniu poprzednim wyposażone są w mechanizm uniemożliwiający ich wielokrotne zamykanie oraz uniemożliwiający dostęp osobom trzecim.
6. Podczas transportowania dokumentów do miejsca realizowania pracy zdalnej, należy zachować szczególną ostrożność, aby ich nie zgubić.
7. Zabronione jest:
 - a) transportowanie dokumentów środkami komunikacji publicznej;
 - b) pozostawianie dokumentów w czasie transportu bez nadzoru (np. w samochodzie).
8. Pracownik jest zobowiązany chronić dokumenty przed uszkodzeniem, zniszczeniem lub zagubieniem, a także dostępem osób nieupoważnionych.
9. Praca z dokumentami nie może być wykonywana w miejscu publicznie dostępnym (w szczególności takim jak kawiarnia, restauracja, galeria handlowa itp.).
10. Odchodząc od stanowiska wykonywania pracy w trybie zdalnym należy schować i zabezpieczyć dokumenty, przy wykorzystaniu kontenera transportowego, tak aby osoby nieupoważnione nie miały do nich wglądu. W ten sam sposób należy zabezpieczyć wszystkie dokumenty robocze odnoszące się wykorzystywanych dokumentów takie jak projekty pism, brudnopisy czy notatki.
11. Z zastrzeżeniem pkt 11, po zakończeniu pracy, wszystkie dokumenty należy zwrócić. Bezpośredni przełożony jest zobowiązany zweryfikować rodzaj i ilość zwracanych dokumentów. Przy zwrocie dokumentacji sporządzany Protokół ze zwrotu dokumentacji, który stanowi Załącznik nr 2 do niniejszej procedury. Kopia Protokołu, o którym mowa w zdaniu poprzednim przekazywana jest Sekretarzowi Gminy niezwłocznie, jednak nie później niż następnego dnia roboczego po jego sporządzeniu.
12. Pobrane dokumenty należy zwrócić najpóźniej w terminie 7 dni od dnia ich pobrania. W szczególnie uzasadnionych przypadkach bezpośredni przełożony może wyrazić zgodę na późniejszy zwrot pobranych dokumentów, informując o tym Sekretarza Gminy. Zgoda o której mowa w zdaniu poprzednim udzielana jest na piśmie lub przy wykorzystaniu służbowej poczty elektronicznej.
13. W każdym przypadku Pracownik jest zobowiązany niezwłocznie zwrócić pobrane dokumenty na żądanie Pracodawcy.

14. Wraz z pobranymi dokumentami należy zwrócić w szczególności wszystkie dokumenty robocze odnoszące się wykorzystywanych dokumentów takie jak projekty pism, brudnopisy czy notatki.
15. W przypadku, gdy występuje rozbieżność między dokumentacją pobieraną, a zwracaną bezpośredni przełożony niezwłocznie informuje o tym fakcie Sekretarza Gminy oraz IOD.
16. Pracownik ponosi bezpośrednią odpowiedzialność za poufność, integralność oraz dostępność pobranej dokumentacji od momentu sporządzenia Protokołu z przekazania dokumentacji do wykonywania pracy w trybie zdalnym, który stanowi Załącznik nr 1 do chwili sporządzenia Protokołu ze zwrotu dokumentacji, który stanowi Załącznik nr 2.
17. W sprawach nieuregulowanych niniejszą Procedurą stosuje się postanowienia Polityki Ochrony Danych Osobowych oraz Regulaminu pracy zdalnej.
- 18.

Protokół przekazania dokumentacji do wykonywania pracy w trybie zdalnym

spisany w dniu

pomiędzy:

.....
(imię i nazwisko, stanowisko oraz komórka organizacyjna)

jako przekazującym dokumentację do wykonywania pracy w trybie zdalnym

a,

.....
(imię i nazwisko, stanowisko oraz komórka organizacyjna)

jako przyjmującym dokumentację do wykonywania pracy w trybie zdalnym.

Dokumentacja została przekazana według poniższego spisu:

Lp.	Nazwa dokumentu i krótki opis sprawy	Liczba stron	Oryginał/kopia	Uwagi

Przekazujący:

Przyjmujący:

.....
 (podpis)

.....
 (podpis)

Protokół ze zwrotu dokumentacji z wykonywania pracy w trybie zdalnym

spisany w dniu

pomiędzy:

.....
(imię i nazwisko, stanowisko oraz komórka organizacyjna)

jako zwracającym dokumentację z wykonywania pracy w trybie zdalnym

a,

.....
(imię i nazwisko, stanowisko oraz komórka organizacyjna)

jako przyjmującym dokumentację z wykonywania pracy w trybie zdalnym.

Dokumentacja została zwrócona według poniższego spisu:

Lp.	Nazwa dokumentu i krótki opis sprawy	Liczba stron	Oryginał/kopia	Uwagi

Zwracający jednocześnie oświadcza, że nie jest w posiadaniu żadnych dokumentów służbowych ani innych materiałów zawierających informacje, z którymi zapoznał się podczas wykonywania obowiązków zawodowych lub innych nośników zawierających inne informacje poufne, w szczególności dane osobowe, jakie sporządził, zebrał, opracował lub otrzymał w czasie wykonywania pracy, włączając w to kopie, odpisy, a także zapisy na innych nośnikach.

Zwracający:

Przyjmujący:

.....
 (podpis)

.....
 (podpis)

