GMINNE CENTRUM USŁUG WSPÓLNYCH
W RAWICZU
ul. Wały Jarosława Dąbrowskiego 33
63-900 Rawicz
NIP: 6991964675, REGON: 384596682

ZARZĄDZENIE NR 5 /2020

DYREKTORA GMINNEGO CENTRUM USŁUG WSPÓLNYCH W RAWICZU

Z dnia 16 marca 2020 r.

W sprawę wprowadzenia instrukcji bezpieczeństwa podczas wykonywania pracy zdalnej w Gminnym Centrum Usług Wspólnych w Rawiczu

Na podstawie § 7 zarządzenia nr 1/2019 Burmistrza Gminy Rawicz z dnia 4 listopada 2019r. w sprawie wprowadzenia regulaminu organizacyjnego w gminnym Centrum Usług Wspólnych w Rawiczu oraz zarządzenia nr 2/2020 Dyrektora Gminnego Centrum Usług Wspólnych w Rawiczu w sprawie wprowadzenia systemu pracy zdalnej dla pracowników Gminnego Centrum Usług Wspólnych w Rawiczu w związku z pandemią COVID-19 zarządzam co następuje:

§ 1

Wprowadzam instrukcję bezpieczeństwa podczas wykonywania pracy zdalnej w Gminnym Centrum Usług Wspólnych w Rawiczu, stanowiącą załącznik nr 1 do zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem podjęcia.

Dyrektor
Arleta Przydrożna

GMINNE CENTRUM USŁUG WSPÓLNYCH
W RAWICZU
ul.Wały Jarosława Dąbrowskiego 33
63-900 Rawicz
NIP: 6991964675. REGON: 384596682

Załącznik do zarządzenia nr 5/2020
Dyrektora GCUW w Rawiczu
z dnia 16 marca 2020r.

Instrukcja bezpieczeństwa podczas wykonywania pracy zdalnej w Gminnym Centrum Usług Wspólnych w Rawiczu.

I. WSTĘP.

1. Niniejsza instrukcja stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych podczas wykonywania pracy zdalnej na polecenie Dyrektora GCUW, zgodnie z przepisami RODO dla:
   1.1. Pracowników,
   1.2. Współpracowników,
   1.3. Podmiotów trzecich, posiadających dostęp do danych osobowych,
   1.4. Kierownictwa GCUW.
2. Każda osoba zatrudniona w GCUW powinna zapoznać się z poniższą instrukcją, zobowiązać się do jej przestrzegania oraz potwierdzić to własnoręcznym podpisem.
3. Instrukcja określa zasady wykonywania pracy zdalnej zgodnie z zasadami ochrony danych osobowych.
4. Stosowane w Instrukcji pojęcie "Pracownik" należy rozumieć jako osobę zatrudnioną w formie etatu, umowy cywilnoprawej, osobę fizyczną prowadzącą własną działalność gospodarczą z dostępem do zasobów sprzętowych i informacyjnych Pracodawcy. Pojęcie "Pracodawca" należy rozumieć jako Pracodawcę w kontekście Kodeksu pracy oraz Zleceniodawcę usług.

II. ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT PRZEZNACZONEGO DO PRACY ZDALNEJ.

1. Użytkownik odpowiada za zabezpieczenie sprzętu IT (laptop, tablet, smartfon) przed zniszczeniem, uszkodzeniem, utratą oraz kradzieżą.
2. Użytkownik zobowiązany jest do przechowywania danych osobowych związanych z wykonywaniem zadań służbowych na zaszyfrowanych dyskach, partycjach, kartach pamięci zamontowanych w sprzęcie IT.
3. Użytkownik zobowiązany jest do zabezpieczenia dostępu do sprzętu IT, nośników (dysków przenośnych, pendrive, CD, DVD, kart typu flash) oraz danych osobowych na nich zawartych przed osobami postronnymi oraz domownikami.
4. Użytkownik zobowiązany jest do bezpiecznego przewożenia sprzętu IT (np. bagażnik samochodu, torba na laptop).
5. Zakazane jest wynoszenie niezaszyfrowanych nośników z zapisanymi danymi osobowymi poza siedzibę GCUW.
6. Dane osobowe przechowywane na nośnikach (dyskach przenośnych, pendrive, CD, DVD, kartach typu flash) poza siedzibą GCUW muszą być zaszyfrowane.
7. Zakazane jest kopiowanie/zapisywanie danych osobowych związanych z wykonywaniem zadań służbowych na niezabezpieczone prywatne nośniki zewnętrzne.
8. Pliki z danym osobowymi przechowywane na niezabezpieczonych nośnikach na sprzęcie IT firmowym lub prywatnym powinny być zabezpieczone hasłem (hasłowanie plików typu office, hasłowanie plików spakowanych w formatach 7zip, Winrar, Winzip) .
9. Przy wykorzystaniu sieci publicznej, użytkownik zobowiązuje się do stosowania zabezpieczonego przed podsłuchem połączenia zdalnego (VPN, SSL).

10. W przypadku pracy terminalowej, użytkownik zobowiązany jest do pracy z użyciem pulpitu zdalnego.
11. Dostęp do domowej sieci WiFi powinien być zabezpieczony hasłem z użyciem szyfrowania w standardzie WPA/WPA2. Nie dopuszcza się stosowania szyfrowania w stdardzie WEP.
12. Rekomendowana jest zmiana hasła i loginu dostępowego do routera.
13. Sprzęt IT powinien być zabezpieczony aktywnym firewallem.
14. Aktywny program antywirusowy.
15. Automatyczne blokowanie sprzętu IT po dłuższym braku aktywności.
16. Praca na koncie z uprawnieniami niższymi niż administracyjne.
17. Aplikacje do transferu danych powinny być uzgodnione z informatykiem a dostęp do nich poprzez uwierzytelnienie.
18. Hasło użytkownika musi składać się z minimum 8 znaków, np. zawierać małe oraz duże litera, cyfry lub znak specjalny. W haśle nie może być zawarte imię, nazwisko użytkownika.

III. ZARZĄDZANIE URAWNIENIAMI.

1. Każdy użytkownik programów i systemu operacyjnego zobowiązany jest do pracy na własnym koncie.
2. Zabronione jest udostępnianie konta innemu użytkownikowi.
3. Użytkownik nie może zmieniać swoich uprawnień bez konsultacji z przełożonym.
4. Użytkownik komputera oraz programów rozpoczyna i kończy pracę logowaniem i wylogowaniem się.
5. Użytkownik przed tymczasowym odejściem od komputera musi włączyć wygaszacz ekranu lub wylogować się z systemu bądź z programu.
6. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana jako pracownik (działu informatyki, przełożony). Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie hiperlinku.
7. Po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego oraz zabezpieczyć nośniki elektroniczne, magnetyczne i optyczne na których znajdują się dane osobowe.

IV. ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI.

1. Pracownik jest zobowiązany do przechowywania dokumentacji papierowej zawierającej dane osobowe w sposób uniemożliwiający dostęp osobom postronnym, nieupoważnionym, domownikom, np. przechowując je w zamykanych na klucz szafach, biurkach itp.
2. Zabrania się pozostawiania dokumentów w miejscach dostępnych dla osób postronnych do których mogłyby mieć wgląd.
3. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik.
4. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej np. w teczkach, aktówkach, plecakach w celu zabezpieczenia ich przed zagubieniem i kradzieżą.

V. ZASADY KORZYSTANIA Z INTERNETU.

1. Zabrania się instalowania na sprzęcie IT programów i aplikacji (pobieranych z internetu lub instalowanych z nośników) bez konsultacji z dyrektorem GCUW i informatykiem.
2. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez samowolną instalację oprogramowania.
3. Zabrania się wchodzenia na strony z nielegalnym oprogramowaniem, pobierania i instalacji takiego oprogramowania.
4. W przypadku pracy w aplikacjach webowych zabrania się użycia opcji autouzupełniania formularzy i zapamiętywania haseł.

VI. ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ.

1. Pliki zawierające dane osobowe (np. w formacie Word, Excel, Pdf lub spakowane np. w formacie zip, rar) przed wysłaniem ich do osób trzecich powinny być zabezpieczone hasłem, które powinno być przekazane do odbiorcy np. telefonicznie lub SMS.
2. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: np. duże i małe litery i cyfry lub znaki specjalne
3. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy poczty.
4. WAŻNE: Nie otwierać załączników poczty pochodzącej z egzotycznych/ nietypowych domen.
5. WAŻNE: Nie wolno „klikać" na hiperlinki w podejrzanej poczcie, gdyż grozi to zainfekowaniem komputera a nawet całej sieci.
6. WAŻNE: Nie wolno wprowadzać loginów i haseł do formularzy zawartych w poczcie, gdyż mogą to być próby wyłudzenia danych dostępowych, czyli tzw. phishingu (mail przesłany rzekomo z naszego banku z opcją zalogowania się, mail przesłany rzekomo przez Google z komunikatem o próbie włamania do naszej poczty i sugestią do zalogowania się do panelu umieszczonego w treści maila).
7. Należy zgłaszać informatykowi przypadki podejrzanych maili, plików w mailach, prób wyłudzeń, kontaktów podejrzanych osób w kontekście dostępu do danych.
8. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości"!
9. Użytkownicy powinni okresowo usuwać niepotrzebne maile lub przenosić do archiwizacji
10. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.

VII. SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH.

1. Każdy pracownik zobowiązany jest do powiadomienia dyrektora GCUW w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Do incydentów wymagających powiadomienia, należą:
   2.1. zdarzenia losowe zewnętrzne (utrata zasilania, utrata łączności),
   2.2. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki użytkowników, utrata / zagubienie danych),
   2.3. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, nieświadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania),
   2.4. telefoniczne próby wyłudzenia danych osobowych,
   2.5. kradzież, zagubienie komputerów lub CD, DVD, dysków przenośnych, pendrive z danymi osobowymi,
   2.6. maile zachęcające do ujawnienia identyfikatora i/lub hasła,
   2.7. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów.

VIII. OBOIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH.

1. Każdy Pracownik dopuszczony do pracy zdalnej jest zobowiązany do jej wykonywania w miejscu zamieszkania lub innym uzgodnionym miejscu z Pracodawcą.
2. Pracownik jest zobowiązany do wykonywania pracy zgodnie z zakresem obowiązków oraz przetwarzania danych osobowych wyłącznie w celu i zakresie powierzonych jej zadań.
3. Pracownik jest zobowiązany do potwierdzania obecności w pracy w sposób określony przez Pracodawcę.

4. Pracownik jest zobowiązany do zachowania w tajemnicy danych osobowych do których ma dostęp.
5. Pracownik jest zobowiązany do niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych jej zadań.
6. Pracownik jest zobowiązany do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych.
7. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podejrzanym o fałszowanie tożsamości.
8. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się podstawą prawną do dostępu do takich danych.
9. Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana do zabezpieczenia danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.
10. Zabrania się pracy zdalnej w miejscach publicznych, stwarzających ryzyko wglądu w dane osobowe przez osoby postronne.
11. Pracując w domu należy zapewnić, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera oraz smartfona, a także zapewnienie pracy z dokumentami w sposób uniemożliwiający wgląd.

XI. POSTANOWIENIA KOŃCOWE.

1. Pracownik świadczy pracę zdalną wyłącznie po przekazaniu przez pracodawcę lub bezpośredniego przełożonego pracownika pisemnego lub elektronicznego polecenia wykonywania pracy zdalnej.
2. Czas wykonywania pracy zdalnej powinien jest określony w poleceniu Pracodawcy. Zmiana okresu pracy zdalnej może być zmieniona przez Pracodawcę a Pracownik zostanie o tym powiadomiony.
3. Przed przystąpieniem do wykonywania pracy zdalnej Pracownik zapoznaje się z treścią niniejszego Regulaminu, co potwierdza pisemnym lub elektronicznym oświadczeniem. Wzór oświadczenia stanowi Załącznik nr 1 do Regulaminu.
4. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z Instrukcji pracy zdalnej potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy i może skutkować rozwiązaniem stosunku pracy lub umowy.

Dyrektor
Arleta Przydrożna

Załącznik 1 do instrukcji bezpieczeństwa
podczas wykonywania pracy zdalnej

.....

(imię i nazwisko)

.....

(miejscowość, data)

OŚWIADCZENIE O POUFNOŚCI PRZY WYKONYWANIU PRACY ZDALNEJ

Oświadczam, że zapoznałam się z zasadami wykonywania pracy zdalnej powierzonej mi przez pracodawcę zgodnie z „Instrukcją bezpieczeństwa podczas wykonywania pracy zdalnej".

W szczególności zobowiązuję się do:

1. przetwarzania informacji wyłącznie w zakresie i celu przewidzianym w powierzonych przez pracodawcę zadaniach,
2. zachowania w tajemnicy informacji do których mam lub będę mieć dostęp w związku z wykonywaniem zadań podczas pracy zdalnej,
3. niewykorzystywania informacji w celach niezgodnych z zakresem i celem powierzonych zadań przez pracodawcę,
4. zachowania w tajemnicy sposobów zabezpieczenia sprzętu IT i systemów informatycznych wykorzystywanych do pracy zdalnej,
5. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem,
6. niedopuszczania do komputera, telefonu i innych nośników przekazanych mi przez Pracodawcę oraz informacji w nich zawartych, w tym danych osobowych, domowników oraz innych osób trzecich,
7. zwrócić powierzone mi nośniki wraz z kompletnymi danymi na każde żądanie Pracodawcy.

Przyjmuję do wiadomości, że postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez pracodawcę za naruszenie przepisów Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r. (RODO) oraz Ustawy o Ochronie Danych Osobowych z 10 maja 2018 r.

.....

podpis oświadczającego

Kilka wskazówek bezpieczeństwa podczas pracy zdalnej

1. Pamiętaj, że odpowiadasz za zabezpieczenie służbowego sprzętu IT przekazanego do pracy zdalnej (laptop, tablet, smartfon) przed zniszczeniem, uszkodzeniem, utratą oraz kradzieżą.
2. Przechowuj dane osobowe związane z wykonywaniem zadań służbowych na zaszyfrowanych dyskach, partycjach, kartach pamięci zamontowanych w sprzęcie IT
3. Zabezpiecz dostępu do sprzętu IT, nośników (dysków przenośnych, pendrive, CD, DVD, kart typu flash) oraz danych osobowych na nich zawartych przed osobami postronnymi oraz domownikami. Bezpiecznie przewoź sprzęt IT (bagażnik samochodu, torba na laptop)
4. Jeśli korzystasz z własnej sieci WIFI zabezpiecz ją hasłem i pamiętaj aby program antywirusowy był aktywny a system aktualizowany na bieżąco.
5. Korzystaj z automatycznej blokady sprzętu IT po dłuższym braku aktywności.
6. Przed tymczasowym odejściem od komputera włącz wygaszacz ekranu zabezpieczony lub wyloguj się z systemu bądź z programu.
7. Po zakończeniu pracy wyloguj się z systemu informatycznego oraz zabezpiecz komputer.
8. Przechowuj dokumenty papierowe zawierające dane osobowe w sposób uniemożliwiający dostęp osobom postronnym, nieupoważnionym, domownikom, np. przechowując je w zamykanych na klucz szafach, biurkach.
9. Nie wyrzucaj niezniszczonych dokumentów do śmietnika.
10. Bezpieczne przewoź dokumenty papierowe np. w teczkach, aktówkach, plecakach w celu zabezpieczenia ich przed zagubieniem i kradzieżą.
11. Nie instaluj na służbowym komputerze programów i aplikacji (pobieranych z Internetu lub instalowanych z nośników) bez konsultacji dyrektorem GCUW.
12. W przypadku pracy w aplikacjach webowych zabrania się użycia opcji autouzupełniania formularzy i zapamiętywania haseł.
13. Pliki zawierające dane osobowe (np. w formacie Word, Excel, Pdf) zapisz z hasłem dostępowym lub spakuj np. w formacie zip, rar i przed wysłaniem ich do osób trzecich zabezpiecz hasłem, hasło przekaż telefonicznie lub SMS
14. Pamiętaj aby hasło zawierało minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne
15. WAŻNE: Nie otwieraj załączników poczty pochodzącej z nieznanych źródeł
16. WAŻNE: Nie klikaj na hiper linki w podejrzanej poczcie, gdyż grozi to zainfekowaniem komputera a nawet całej sieci
17. Zgłaszaj informatykowi przypadki podejrzanych maili, plików w mailach, prób wyłudzeń, kontaktów podejrzanych osób w kontekście dostępu do danych.
18. Nie wysyłaj korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
19. Pamiętaj, że musisz powiadomić dyrektora GCUW w każdym przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
20. Przypadki o których musisz informować to:
    1. zdarzenia losowe, awarie komputerów, twardych dysków, oprogramowania, pomyłki użytkowników, utrata / zagubienie danych),
    2. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, nieświadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania),
    3. telefoniczne próby wyłudzenia danych osobowych,
    4. kradzież, zagubienie komputerów lub CD, DVD, dysków przenośnych, pendrive z danymi osobowymi,
    5. maile zachęcające do ujawnienia identyfikatora i/lub hasła,
    6. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów.
21. Nie wykonuj pracy zdalnej w miejscach publicznych, stwarzasz przez to ryzyko wglądu w dane osobowe osobom postronnym.

22. Pamiętaj, że pracując w domu musisz zapewnić, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera oraz smartfonu, a także zapewnienie pracy z dokumentami w sposób uniemożliwiający wgląd.

Dyrektor
Arleta Przydrożna