ZARZĄDZENIE NR I/353/2020 BURMISTRZA
GMINY TRZCIŃSKO- ZDRÓJ
z dnia 06 listopada 2020 r.

w sprawie wprowadzenia Regulaminu Bezpieczeństwa podczas wykonywania pracy zdalnej w Urzędzie Miejskim w Trzcińsku- Zdroju.

Na podstawie art. 31 i art. 33 ust. 3 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (t.j. Dz.U. 2020 poz. 713) oraz art.3 ustawy z dnia 2 marca 2020 roku o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacjami kryzysowymi (Dz.U. 2020 poz. 374 z późn. zm.) zarządzam, co następuje:

§ 1. W związku z wprowadzeniem pracy zdalnej dla pracowników Urzędu Miejskiego w Trzcińsku- Zdroju wprowadzam „Regulamin Bezpieczeństwa podczas wykonywania pracy zdalnej dla pracowników Urzędu Miejskiego w Trzcińsku- Zdroju", stanowiący załącznik nr 1 do niniejszego zarządzenia.

§ 2. Zarządzenie obowiązuje do odwołania.

§ 3. Wykonanie zarządzenia powierza się Sekretarzowi Gminy.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
Bartłomiej Wróbel

Załącznik Nr 1
do zarządzenia Nr I/353/2020
Burmistrza Gminy Trzcińsko-Zdrój
z dnia 06 listopada 2020 r.

Regulamin Bezpieczeństwa podczas wykonywania pracy zdalnej w Urzędzie Miejskim w Trzcińsku- Zdroju

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych podczas wykonywania pracy zdalnej na polecenie Pracodawcy zgodnie z przepisami RODO dla:

- Pracowników

Każda z w/w osób powinna zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych

SPIS TREŚCI

1. Regulamin określa zasady wykonywania pracy zdalnej zgodnie z zasadami ochrony danych osobowych.

2. Stosowane w Regulaminie pojęcie "Pracownik" należy rozumieć jako Osobę zatrudnioną w formie etatu, kontraktu, umowy cywilnoprawej z dostępem do zasobów sprzętowych i informacyjnych Pracodawcy. Pojęcie "Pracodawca" należy rozumieć jako Pracodawcę w kontekście Kodeksu pracy oraz Zleceniodawcę usług.

1 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 elektronicznych (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 (bagażnik samochodu, torba na laptop).
5. Zakazane jest wynoszenie niezaszyfrowanych nośników elektronicznych z zapisanymi danymi osobowymi poza siedzibę Pracodawcy.
6. Dane osobowe przechowywane na nośnikach (dyskach przenośnych, pendrive, CD, DVD, kartach typu flash) poza siedzibą Pracodawcy 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.
12. Rekomendowana jest zmiana hasła i loginu dostępowego do routera.
13. Sprzęt IT powinien być zabezpieczony aktywnym firewallem.
14. Sprzęt IT powinien posiadać 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.

2 Zarządzanie uprawnieniami

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 zabezpieczony hasłem (np. z użyciem kombinacji klawiszy **WINDOWS + L**) 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.

3 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, sejfach.
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.

4 ZASADY KORZYSTANIA Z INTERNETU

1. Zabrania się instalowania na sprzęcie IT programów i aplikacji (pobieranych z internetu lub instalowanych z nośników) bez konsultacji z 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

5 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 telefonicznie lub SMS.
2. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum (np. 12) znaków: 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.

6 SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każdy pracownik zobowiązany jest do powiadomienia Pracodawcy/bezpośredniego przełożonego/informatyka w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Do incydentów wymagających powiadomienia, należą:
    a. zdarzenia losowe zewnętrzne (utrata zasilania, utrata łączności),
    b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki użytkowników, utrata / zagubienie danych),
    c. 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),
    d. telefoniczne próby wyłudzenia danych osobowych,
    e. kradzież, zagubienie komputerów lub CD, DVD, dysków przenośnych, pendrive z danymi osobowymi,
    f. maile zachęcające do ujawnienia identyfikatora i/lub hasła,
    g. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów.

7 OBOWIĄZEK 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, tabletu oraz smartfona, a także zapewnienie pracy z dokumentami w sposób uniemożliwiający wgląd.

8 POSTANOWIENIA KOŃCOWE

1. Pracownik świadczy pracę zdalną wyłącznie po przekazaniu przez pracodawcę lub bezpośredniego przełożonego pracownika pisemnego lub elektronicznego polecenia wykonywania pracy zdalnej, zgodnie z ZARZĄDZENIEM NR I/346/2020 BURMISTRZA GMINY TRZCIŃSKO- ZDRÓJ z dnia 8 października 2020 r . w sprawie wprowadzenia Regulaminu pracy zdalnej dla pracowników Urzędu Miejskiego w Trzcińsku- Zdroju.
2. 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

ZAŁĄCZNIK 1 - WZÓR OŚWIADCZENIA

....

(imię i nazwisko) *(miejscowość, data)*

OŚWIADCZENIE O POUFNOŚCI PRZY WYKONYWANIU PRACY ZDALNEJ

Oświadczam, iż zapoznałam/em się z zasadami wykonywania pracy zdalnej powierzonej mi przez pracodawcę zgodnie z „Regulaminem Bezpieczeństwa podczas wykonywania pracy zdalnej w Urzędzie Miejskim w Trzcińsku-Zdroju".

W szczególności zobowiązuję się do:

- przetwarzania informacji wyłącznie w zakresie i celu przewidzianym w powierzonych przez pracodawcę zadaniach
- zachowania w tajemnicy informacji do których mam lub będę mieć dostęp w związku z wykonywaniem zadań podczas pracy zdalnej
- niewykorzystywania informacji w celach niezgodnych z zakresem i celem powierzonych zadań przez pracodawcę
- zachowania w tajemnicy sposobów zabezpieczenia sprzętu IT i systemów informatycznych wykorzystywanych do pracy zdalnej
- 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
- 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
- zwrócić powierzone mi nośniki wraz z kompletnymi danymi na każde żądanie Pracodawcy.

Przyjmuję do wiadomości, iż 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.

.....

podpis oświadczającego