ZARZĄDZENIE NR 120/5/2023
WÓJTA GMINY BOJSZOWY

z dnia 10 stycznia 2023 r.

w sprawie wprowadzenia Regulaminu Bezpieczeństwa podczas wykonywania pracy zdalnej w Urzędzie Gminy Bojszowy

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2023 r. poz. 40), art. 24 ust. 1 i 2 Rozporządzenia Parlamentu 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 (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L. z 2016 r., Nr 119, str. 1)

zarządzam, co następuje:

§ 1. Wprowadza się Regulamin Bezpieczeństwa podczas wykonywania pracy zdalnej w Urzędzie Gminy Bojszowy, który stanowi załącznik do niniejszego zarządzania.

§ 2. Wykonanie Zarządzenia powierza się Sekretarz Gminy wraz z Inspektorem Ochrony Danych.

§ 3. Zarządzenie wchodzi w życie z dniem podjęcia.

Wójt Gminy Bojszowy

Adam Duczmal

Załącznik do zarządzenia Nr 120/5/2023
Wójta Gminy Bojszowy
z dnia 10 stycznia 2023 r.

Regulamin Bezpieczeństwa podczas wykonywania pracy zdalnej w Urzędzie Gminy Bojszowy

43-220 Bojszowy ul. Gaikowa 35

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

- Pracowników upoważnionych

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

…… *(podpis IOD)*

…… *(podpis Administratora)*

v.02/2022

1 SPIS TREŚCI

1. Regulamin określa zasady wykonywania pracy zdalnej zgodnie z zasadami ochrony danych osobowych zawartymi w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
2. Stosowane w Regulaminie pojęcie "Pracownik" należy rozumieć jako Osobę zatrudnioną w formie etatu, kontraktu, umowy cywilnoprawej, umowy zlecenia, umowy o dzieło, osobę fizyczną prowadzącą własną działalność gospodarczą z dostępem do zasobów sprzętowych i informacyjnych Administratora. Pojęcie "Pracodawca" należy rozumieć jako Pracodawcę w kontekście Kodeksu pracy oraz Zleceniodawcę usług.

2 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 (bagażnik samochodu, torba na laptop),
5. Zakazane jest wynoszenie niezaszyfrowanych nośników z zapisanymi danymi osobowymi poza siedzibę organizacji,
6. Dane osobowe przechowywane na nośnikach (dyskach przenośnych, pendrive, CD, DVD, kartach typu flash) poza siedzibą organizacji 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. Hasła powinny składać się z minimum 8 znaków,
10. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne),
11. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty,
12. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie,
13. W przypadku ujawnienia hasła – należy natychmiast go zmienić,
14. Hasła muszą być zmieniane co 30 dni,
15. Przy wykorzystaniu sieci publicznej, użytkownik zobowiązuje się do stosowania zabezpieczonego przed podsłuchem połączenia zdalnego (VPN, SSL),
16. W przypadku pracy terminalowej, użytkownik zobowiązany jest do pracy z użyciem pulpitu zdalnego
17. Dostęp do domowej sieci WiFi powinien być zabezpieczony hasłem,
18. Rekomendowana jest zmiana hasła i loginu dostępowego do routera,
19. Sprzęt IT powinien być zabezpieczony aktywnym firewallem,
20. Aktywny program antywirusowy,
21. Automatyczne blokowanie sprzętu IT po dłuższym braku aktywności,
22. Praca na koncie z uprawnieniami niższymi niż administracyjne,
23. Na prywatnym sprzęcie IT używanym do celów służbowych, należy utworzyć indywidualne konto „PRACA”,
24. Aplikacje do transferu danych powinny być uzgodnione z informatykiem a dostęp do ich poprzez uwierzytelnienie.

3 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 Administratorem,
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.

4 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.

5 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 / Administratorem,
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.

6 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 (8) 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

7 SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każdy pracownik zobowiązany jest do powiadomienia Administratora/bezpośredniego przełożonego/IOD/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.

8 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 Administratorem
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 Administratora,
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.

9 POSTANOWIENIA KOŃCOWE

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

Załącznik nr 1

Zlecenie modyfikacji uprawnień
PRACA ZDALNA

Nowy użytkownik	**X** Modyfikacja uprawnień	Odebranie uprawnień

Imię i nazwisko użytkownika:	Referat :
Upoważnienie nr: **……. PZ**	Stanowisko:
Opis zakresu uprawnień użytkownika w systemie informatycznym: T – Tworzenie; M – Modyfikacja; U- Usuwanie; A – Archiwizacja; ASI – Administracja Systemami Informatycznymi; O- Odczyt	

Uprawnienia	T	M	U	A	ASI	O

Programy / Dokumenty :

Dokumenty wersja papierowa i elektroniczna						
Pendrive służbowy						
Komputer służbowy						
Komputer prywatny z wydzielonym zahasłowanym kontem						

Inne

Praca zdalna (VPN, strona internetowa)						

Uwagi: Upoważnienie obowiązuje od : **……**

Do : **Odwołania**

Data i podpis osoby upoważnionej:	Data i podpis Administratora:
Data i podpis bezpośredniego przełożonego:	Data i podpis IOD:

Załącznik nr 2

…….. ……
(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 pracy zdalnej".

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 Administratora

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)

Załącznik nr 3

Wykaz pobranych dokumentów

……
Imię nazwisko

LP	Dokument wydany	Data wydania	Podpis odbierającego /przełożonego	Data zwrotu	Podpis przyjmującego / przełożonego