ZARZĄDZENIE NR 14/20
WÓJTA GMINY DRAGACZ
z dnia 18 marca 2020 r.

w sprawie organizacji pracy zdalnej na sprzęcie służbowym w Urzędzie Gminy w Dragaczu

Na podstawie art. 3 ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz .U. z 2020 r. poz. 374) zarządzam, co następuje:

§ 1. W przypadku wykonywania pracy zdalnej pracownik Urzędu Gminy w Dragaczu zobowiązany jest do przestrzegania zasad określonych w załączniku Nr 1 do zarządzenia.

§ 2. 1. Praca zdalna wykonywana jest na sprzęcie służbowym będącym w posiadaniu Urzędu Gminy w Dragaczu po uprzednim przygotowaniu go przez informatyka.
2. Zadania dla informatyka określa załącznik Nr 2 do zarządzenia.

§ 3. Zabrania się drukowania oraz skanowania dokumentów w miejscu wykonywania pracy zdalnej.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy

mgr Dorota Krezymon

Załącznik Nr 1 do
Zarządzenia Nr 14/20
z dnia 18 marca 2020 r.

Zasady postępowania dla użytkownika pracującego zdalnie na sprzęcie Urzędu Gminy w Dragaczu:

1. W miejscu pracy zapewnij sobie przestrzeń, która będzie odpowiednia do tego, aby osoby postronne nie miały dostępu do informacji służbowych.
2. Nie pozostawiaj komputera używanego do pracy zdalnej bez nadzoru, a w przypadku krótkotrwałego opuszczania stanowiska pracy zblokuj komputer i zabezpiecz dokumenty.
3. Używaj do logowania się na komputerze haseł zgodnych z polityką haseł przyjętą w Jednostce.
4. Używaj tylko rekomendowanych przez administratora przeglądarek internetowych.
5. Nie zapamiętuj haseł w przeglądarkach internetowych.
6. Nie wykorzystuj komputera do prywatnych celów (np. zakupy, gry, itp.).
7. Nie instaluj żadnego oprogramowania bez uprzedniej akceptacji przez pion informatyki.
8. Nie loguj się komputerem do publicznych sieci Wi-Fi.
9. Łącz się z zasobami Jednostki tylko za pomocą skonfigurowanego przez administratora bezpiecznego łącza.
10. Do celów służbowych korzystaj tylko z służbowej poczty e-mail.
11. Przed wysłaniem wiadomości upewnij się, że wysyłasz ją do właściwego adresata, szczególnie gdy wysyłasz dane osobowe lub inne istotne informacje.
12. Nie otwieraj wiadomości od nieznanych nadawców, a szczególnie załączników niewiadomego pochodzenia oraz nie klikaj w żadne linki lub odnośniki.
13. W przypadku drukowania służbowych dokumentów na prywatnym sprzęcie odpowiednio je zabezpiecz przed dostępem osób trzecich.
13. Wydruki techniczne lub błędne zabezpiecz do momentu powrotu do pracy,a następnie zniszcz w niszczarce chyba, że posiadasz odpowiedni sprzęt w domu.
14.W przypadku wykorzystywania do kontaktów komunikatora internetowego nie używaj w tym samym czasie innych narzędzi do komunikacji.
15.W przypadku przesyłania plików lub dokumentów za pomocą poczty e-mail lub komunikatora internetowego zawsze zabezpieczaj je hasłem. Hasło przekaż innym kanałem kontaktowym(np. wiadomością SMS).
16.W przypadku utraty sprzętu natychmiast skontaktuj się z wyznaczoną osobą do kontaktu i zadbaj, jeżeli masz taką możliwość, o zdalne usunięcie danych z urządzenia.

Załącznik Nr 2 do
Zarządzenia Nr 14 /20
z dnia 18 marca 2020 r.

Zadania dla Informatyka

1. Przygotuj i skonfiguruj komputer aby logował się tylko do zabezpieczonej i odpowiednio skonfigurowanej sieci.
2. Monitoruj ruch sieciowy pod kątem wystąpienia niepożądanego ruchu.
3. Wyłącz możliwość dostępu do BIOS komputera zabezpieczając go hasłem.
4. Wyłącz w BIOS możliwość boot'owania z innych nośników niż dysk twardy komputera.
5. Zaszyfruj dyski twarde, nośniki danych lub karty pamięci, na których będą dane.
6. Zainstaluj i zaktualizuj program antywirusowy oraz skonfiguruj w taki sposób aby bazy wirusów aktualizowały się samoczynnie.
7. Zaktualizuj system operacyjny na komputerze oraz ustaw aktualizacje automatyczne.
8. Zaktualizuj inne oprogramowanie oraz przeglądarki internetowe, które będą wykorzystywane przez pracownika.
9. Zablokuj możliwość instalacji sprzętu zewnętrznego.
10. Włącz i skonfiguruj firewall aby uniemożliwić podłączenie komputera pracownika do niezabezpieczonych sieci Wi-Fi.
11. Wymuś zakaz instalowania innego oprogramowania,jak tylko dopuszczonego przez Jednostkę.
12. Ustaw pracownikom konta dostępu do komputera bez uprawnień administratora.
13. Ustaw hasło do logowania do komputera zgodnie z przyjętą polityką haseł.
14. Ustaw wygaszacz ekranu zabezpieczony hasłem nie dłuższym niż 10 min.
15. W przypadku przekazania przez pracodawcę służbowego punktu dostępowego do Internetu odpowiednio go skonfiguruj (szyfrowana transmisja) i zabezpiecz dostęp hasłem.
16. Wymuś szyfrowanie połączeń z służbową pocztą e-mail.
17. Aktualizuj oprogramowanie serwera poczty e-mail oraz monitoruj ruch na serwerze.
18. W przypadku używania przez pracownika smartfonu do pracy oraz obsługi poczty służbowej odpowiednio go zabezpiecz.
19. W przypadku potrzeby wymiany danych pomiędzy pracownikami załóż wspólny, zabezpieczony katalog mając na uwadze właściwe uprawnienia pracowników
20. Określ maksymalną wielkość pliku, którą można przesłać na wspólny zasób.
21. Ustal zasady oraz punk kontaktowy w przypadku awarii lub innych problemów technicznych.
22. W przypadku korzystania z komunikatora internetowego odpowiednio go skonfiguruj, zabezpiecz hasłem, sprawdź czy posiada właściwą ochronę kryptograficzną oraz sprawdzaj aktualizacje dla serwera i klienta.
23. Zabezpiecz alternatywne połączenie z Jednostką o tych samych parametrach i zabezpieczeniach w przypadku problemów z już istniejącym.
24. Przeprowadź szkolenie pracowników w zakresie pracy zdalnej