

Zarządzenie Nr 67/2025

Wójta Gminy Ustronie Morskie

z dnia 26 maja 2025 r.

zmieniające zarządzenie nr 53/2022 Wójta Gminy Ustronie Morskie z dnia 11 kwietnia 2022 r. w sprawie ustalenia Regulaminu Pracy Urzędu Gminy Ustronie Morskie

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2024 r. poz. 1465 ze zm.), art. 22³ w związku z art. 22² §6-10 oraz art. 104-104³ ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2025 r. poz. 277 t.j.), zarządza się, co następuje:

§ 1. W Regulaminie Pracy Urzędu Gminy Ustronie Morskie przyjętego zarządzeniem nr 53/2022 z dnia 11 kwietnia 2022 r. w sprawie ustalenia Regulaminu Pracy Urzędu Gminy Ustronie Morskie w rozdziale V załącznika do ww. zarządzenia dodaje się § 23¹ o treści:
„Monitoring stanowisk komputerowych w Urzędzie Gminy Ustronie Morskie”

1. Celem stosowania monitoringu stanowisk komputerowych jest zapewnienie zachowania równowagi pomiędzy uzasadnionym interesem pracownika do ochrony jego prywatności, a prawem do ochrony danych i mienia Pracodawcy, a w szczególności:

a) poprawa jakości i zgodności z procedurami wykonywania pracy przez pracowników obowiązującymi w Urzędzie;

b) zabezpieczenie uzasadnionych interesów pracodawcy – zapewnienie organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy;

c) zapewnienie bezpieczeństwa Urzędu w tym bezpieczeństwa przetwarzanych danych osobowych, bezpieczeństwa systemów informatycznych stosowanych w Urzędzie oraz mienia pracodawcy.

2. Cele wskazane w ust. 1 obejmują swoim zakresem:

a) przetwarzanie danych przez pracodawcę w celu dochodzenia roszczeń;

b) przetwarzanie danych przez pracodawcę w celu prowadzenia postępowań dyscyplinarnych wobec pracowników;

c) udostępnienie danych przez pracodawcę organom uprawnionym, w szczególności Policji, prokuraturze lub sądowi, w celu dochodzenia roszczeń lub obrony przed roszczeniami pracowników lub innych osób, na wniosek organów uprawnionych oraz na wniosek pracowników lub tych osób.

3. Dane osobowe pracowników pozyskane w związku z prowadzonym monitoringiem stanowisk komputerowych będą przetwarzane przez pracodawcę wyłącznie w celach określonych w ust. 1 i 2.

4. W przypadku zaistnienia zdarzenia, uzasadniającego wystąpienie przez pracodawcę z roszczeniami wobec pracownika, informacje pozyskane z monitoringu stanowisk komputerowych, mogą stanowić dowód niedozwolonych działań.

5. W związku z monitoringiem treści, zabronione jest wykorzystywanie przez pracownika komputera służbowego dla celów prywatnych. Zabronione jest logowanie się do prywatnej poczty elektronicznej, portali społecznościowych (np. Instagram, Facebook, Twitter itp.) oraz przechowywanie na komputerze innych danych prywatnych (w tym kontaktów prywatnych, zdjęć, informacji tekstowych) do których pracodawca nie powinien mieć dostępu z uwagi na ich prywatny charakter.

6. Korzystanie ze służbowej poczty elektronicznej u pracodawcy do celów innych niż służbowe jest zabronione, całość korespondencji prowadzonej z użyciem służbowej poczty elektronicznej powinna być korespondencją wyłącznie służbową.

7. Zabronione jest instalowanie na komputerze i wykorzystywanie jakiegokolwiek oprogramowania bez wiedzy i udziału osób odpowiedzialnych za tego rodzaju czynności w Urzędzie. Wszelkie działania pracownika w tym zakresie będą monitorowane.

8. Działania pracodawcy zmierzające do poprawy jakości pracy z komputerem polegają w szczególności na eliminowaniu możliwości pobierania określonych danych z Internetu, odciążaniu sieci informatycznej, poprzez ograniczenie możliwości transferu danych z lub do komputera pracownika, usuwaniu nielegalnego oprogramowania, blokowania dostępu do nielegalnej treści oraz kontroli antywirusowej.

9. Monitorowanie pracy pracowników przy wykorzystaniu komputerów służbowych jest prowadzone w następujący sposób:

a) zdalnie poprzez sieć wewnętrzną za pomocą oprogramowania monitorującego pracę komputera będącego własnością pracodawcy, który posiada do niego stosowną licencję i analizę pracy serwerów,

b) poprzez manualną weryfikację całości lub części korespondencji prowadzonej z danego adresu e-mail, przez danego pracownika lub w określonym czasie w przypadku zaistnienia uzasadnionego podejrzenia naruszenia zasad ochrony informacji objętych tajemnicą, w tym danych osobowych, przez określonego pracownika.

10. Zakres monitoringu obejmuje:

- a) kontrolę zdarzeń na komputerze pracownika;
- b) przesyłanie alertów na komputer pracownika przez administratora sieci informatycznej;
- c) monitoring używanych przez pracownika aplikacji;
- d) możliwość blokowania zbędnych aplikacji lub stron internetowych;
- e) monitoring wykonywanych przez pracowników wydruków;
- f) monitoring odwiedzanych przez pracowników stron internetowych;
- g) monitoring ruchu w sieci komputerowej (LAN, WAN) Urzędu;
- h) monitoring legalności oprogramowania;
- i) powiadamianie o monitorowaniu każdego pracownika po uruchomieniu komputera;
- j) monitoring służbowych kont poczty email;

k) monitoring używania przenośnych nośników danych (pendrive, karty pamięci, DVD - ROM, CD - ROM, HDD, telefony, itp.) z możliwością blokowania, jak i odczytania ich treści;

l) monitoring posiadanego sprzętu i oprogramowania w Urzędzie,

m) monitoring zakazów wprowadzonych w niniejszym zarządzeniu.

11. Powiadomienie o monitorowaniu każdego użytkownika komputera następuje w postaci monitu startowego programu monitorującego pracę komputera.

12. Podstawą przetwarzania danych osobowych w związku ze stosowaniem monitoringu jest ustawa z dnia 26 czerwca 1974 r. Kodeks pracy, w związku z realizacją przez pracodawcę spoczywającego na nim obowiązku sprawowania nadzoru nad efektywnym oraz zgodnym z obowiązującym prawem wykorzystaniem zasobów, w tym zasobów informacyjnych.

13. Dostęp do informacji pozyskanych w związku z prowadzonym monitoringiem mają upoważnieni pracownicy Pracodawcy.

14. Jeśli zaistnieje potrzeba podłączenia komputera prywatnego (laptop, tablet, netbook) pracownika do sieci LAN/WAN Urzędu wymaga to akceptacji Informatyka.

15. Zabrania się podejmowania prób wykorzystania obcego konta, uruchamiania aplikacji deszyfrujących hasła, prowadzenia działań mających na celu podsłuchiwanie lub przechwytywanie informacji przepływającej w sieci.

16. Zabrania się uruchamiania aplikacji, które mogą zakłócić i zdestabilizować pracę systemu lub sieci komputerowej, bądź naruszyć prywatność zasobów systemowych.

17. W przypadku naruszenia zasad opisanych w ust. 1 i ust. 2 blokowany jest dostęp do konta użytkownika.

18. W przypadku stwierdzenia, że komputer dołączony jest do sieci LAN/WAN generuje strumień danych zakłócający pracę sieci lub wskazujący na używanie tego komputera jako niezarejestrowanego serwera danych, Administrator Systemów Informatycznych oraz upoważnione do tego osoby mają prawo zablokować dostęp do tego komputera, do czasu wyjaśnienia sprawy.

§ 2. Wzór oświadczenia o zapoznaniu się z treścią zapisów zamieszczonych w Regulaminie Pracy Urzędu Gminy Ustronie Morskie, w tym dotyczących monitoringu stanowisk komputerowych w Urzędzie Gminy Ustronie Morskie, stanowi załącznik nr 1 do niniejszego zarządzenia.

§ 3. Wykonanie zarządzenia powierza się Sekretarzowi Gminy Ustronie Morskie.

§ 4. Zarządzenie wchodzi w życie po upływie 14 dni, od dnia podania go do wiadomości pracowników.

WÓJT GMINY

Grzegorz Czachorowski

OŚWIADCZENIE

Ja niżej podpisany/a informuję, że zapoznałem/am się z zarządzeniem nr/2025 Wójta Gminy Ustronie Morskie z dnia2025 r. i przyjmuję do wiadomości, iż pracownik prowadzący sprawy z zakresu informatyki monitoruje wszelkie czynności wykonywane na komputerze, ruch internetowy oraz wydruki, jak i ma możliwość zdalnego zarządzania komputerem pracownika.

Oświadczam również, że jestem świadomy/a wprowadzonego w Urzędzie Gminy Ustronie Morskie zakazu podłączenia do sieci urzędu wszelkich urządzeń prywatnych, a w tym w szczególności laptopów, smartfonów, tabletów.

Ponadto przyjmuję do wiadomości, że w celu zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, a w szczególności zdalnego zarządzania urządzeniem przez Pracodawcę oraz jego blokady w przypadku kradzieży lub zgubienia przez pracownika, Pracodawca będzie wykorzystywał aplikację zainstalowaną na komputerach służbowych pracowników służącą do zdalnego zarządzania urządzeniem, bezpieczeństwem i aplikacjami zainstalowanymi na urządzeniu. Aplikacja, w przypadkach wynikających z zapewnienia bezpieczeństwa informacji oraz ochrony danych osobowych, umożliwia zdalne zarządzanie komputerem oraz jego zablokowanie w przypadku kradzieży.

Pracodawca będzie prowadził także monitoring służbowej poczty elektronicznej, którego zakresem objęte będą wyłącznie służbowe wiadomości e-mail. Pracownik nie powinien korzystać z poczty służbowej w celach osobistych. Monitoring służbowej poczty elektronicznej będzie polegał na możliwości zapoznania się z treścią wiadomości bez ingerencji w jej treść za pośrednictwem narzędzi informatycznych umożliwiających wgląd do służbowej poczty elektronicznej pracownika.

Monitoring poczty elektronicznej nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika. Pracodawca będzie stosował monitoring poczty elektronicznej w celu zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy.

Monitoring służbowej poczty elektronicznej będzie prowadzony wyłącznie przez Administratora Systemów Informatycznych oraz przez upoważnione do tego osoby.

Sprzęt komputerowy na którym będzie prowadzony monitoring, zostanie oznaczony w odpowiedni sposób przy wykorzystaniu oznaczeń fizycznych w tym graficznych lub informacji wyświetlanych na monitorze komputera.

Dane zarejestrowane przez Pracodawcę są przechowywane przez 30 dni od dnia ich zarejestrowania.

.....
Data i podpis pracownika