

WÓJT GMINY POCZESNA
ul. Wolności 2
42-262 Poczesna

Zarządzenie nr URO.0050.576.2023.R.S
Wójta Gminy Poczesna
z dnia 28 września 2023 r.

w sprawie: wprowadzenia R e g u l a m i n u korzystania z komputerów służbowych oraz zasobów informatycznych w Urzędzie Gminy w Poczesnej.

Na podstawie art.33 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2023 r. poz. 40 z późn. zm.).

z a r z ą d z a m:

§ 1

Ustalam Regulamin dotyczący korzystania z komputerów służbowych oraz zasobów informatycznych w Urzędzie Gminy w Poczesnej, stanowiący załącznik do zarządzenia.

§ 2

Wykonanie zarządzenia powierza się informatykowi zatrudnionemu w Urzędzie Gminy w Poczesnej.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT

mgr inż. Krzysztof Ujma

RADCA PRAWNY

Wiesław Rodak
nr wpisu: OP-C-2/84

[Signature]
Inspektor ochrony danych
Kazimierz Ślusarczyk

Regulamin

korzystania z komputerów służbowych oraz zasobów informatycznych w Urzędzie Gminy w Poczesnej

I. Postanowienia ogólne

§ 1

1. Niniejszy Regulamin ustala zasady:
 - a) korzystania z komputerów służbowych,
 - b) korzystania z oprogramowania,
 - c) korzystania z zasobów informatycznych sieci komputerowej,
 - d) wysyłania służbowej poczty elektronicznej,
 - e) monitorowania pracy Pracowników przy wykorzystaniu komputerów służbowych,
 - f) korzystania z gniazł prądowych typu "Data" (czerwone gniazda prądowe).

II. Zasady korzystania z komputerów służbowych

§ 2

1. Komputer powierzony Pracownikowi stanowi własność Urzędu i jako narzędzie pracy powinien być do niej wykorzystywany.
2. Osobą uprawnioną do korzystania z komputera jest wyłącznie Pracownik Urzędu, z wyjątkiem uprawnionego serwisanta za zgodą ASI.
3. Urząd może powierzyć Pracownikowi komputer do korzystania w miejscu pracy lub poza miejscem pracy. W tym drugim przypadku komputer powierzony jest na podstawie protokołu zdawczo-odbiorczego.
4. Pracodawca udostępnia Pracownikom komputery z zainstalowanym oprogramowaniem, w tym elektroniczną skrzynką pocztową, oraz zapoznaje Pracownika z obowiązującymi w Urzędzie zasadami korzystania z takiego sprzętu.
5. Korzystanie z komputerów, Internetu i programów użytkowych ma służyć Pracownikom wyłącznie do celów służbowych, informacyjnych i administracyjnych, związanych z wykonywaniem zadań i obowiązków służbowych.
6. W Urzędzie Pracownikowi zabrania się korzystania ze sprzętu komputerowego, do którego Pracownik nie jest uprawniony.
7. Zabrania się dokonywania, bez autoryzacji ASI, zmian w ustawieniach systemowych komputerów, w szczególności ustawień BIOS-u, ustawień systemu operacyjnego (w tym instalowania urządzeń), ustawień sieci teleinformatycznej.
8. Zabrania się samodzielnego otwierania obudowy komputera oraz innych części komputerowych (np. monitorów, drukarek, myszy).
9. Wszelkie zewnętrzne nośniki danych będą blokowane z wyjątkiem pkt. 10 niniejszego §2.
10. Korzystanie z nośników danych typu pendrive dopuszczalne jest wyłącznie po wcześniejszym zarejestrowaniu w systemie monitorującym i sprawdzeniu programem antywirusowym.
11. Pracownik może bez wiedzy i zgody ASI:
 - a) wymienić toner, tusz, taśmę i inne materiały eksploatacyjne,
 - b) usunąć zakleszczony papier.
12. Zezwala się Pracownikom na korzystanie z przenośnego komputera służbowego poza miejscem pracy, na zasadach wymienionych w odrębnych przepisach wewnętrznych.
13. Administratorem firmowego sprzętu komputerowego jest Administrator Systemu Informatycznego

§ 3

1. Pracownik jest zobowiązany właściwie eksploatować i dbać o powierzony mu komputer oraz utrzymać go w stanie nie gorszym, niż wynika to ze zwykłego zużycia eksploatacyjnego.
2. Pracownik zobowiązany jest zabezpieczyć dostęp do komputera w sposób uniemożliwiający zalogowanie się do systemu osobom nieuprawnionym.
3. Pracownik jest odpowiedzialny za właściwe zabezpieczenie danych przechowywanych w komputerze.
4. Wszystkie dane zapisane w komputerze (dokumenty służbowe tworzone i przechowywane w pamięci komputera, pliki oraz inne posiadane informacje i dane) związane z wykonywanymi zadaniami służbowymi są własnością Urzędu.
5. W przypadku używania firmowych zewnętrznych nośników danych typu pendrive, zarejestrowanych w systemie monitorującym, na stacji roboczej Pracownik zobowiązany jest wcześniej wykonać skanowanie programem antywirusowym wszystkich danych na nośniku.
6. Zabrania się używania prywatnych nośników danych.
7. Zabrania się podłączenia nośników firmowych do sprzętu prywatnego.

§ 4

1. Pracownik korzystający z komputera może użytkować go poza miejscem pracy do celów służbowych, jedynie za zgodą przełożonego, zachowując obowiązujące w Urzędzie zasady korzystania z oprogramowania.
2. W przypadku nieobecności w pracy przekraczającej jeden miesiąc, Pracownik zobowiązany jest zwrócić komputer do miejsca pracy.

§ 5

1. Pracownik jest zobowiązany zabezpieczyć sprzęt przed kradzieżą, uszkodzeniem lub zniszczeniem.
2. W przypadku kradzieży komputera, Pracownik zobowiązany jest niezwłocznie powiadomić o tym przełożonego wyjaśniając wszystkie okoliczności zdarzenia.
3. W przypadku utraty komputera lub jego uszkodzenia z winy Pracownika, wszelkie koszty związane z jego naprawą lub zakupem nowego ponosi Pracownik.
4. W szczególnych przypadkach Wójt Gminy, na podstawie pisemnego wniosku zainteresowanego, może zdecydować o odstąpieniu od egzekwowania zobowiązania, o którym mowa w punkcie poprzedzającym.

§ 6

1. Zabrania się wykorzystywania sprzętu komputerowego:
 - a) do celów nie związanych z działalnością Urzędu,
 - b) do prowadzenia działalności mającej na celu naruszenie bezpieczeństwa systemów komputerowych, zarówno wewnętrznych, jak i zewnętrznych,
 - c) posługiwania się fałszywymi informacjami w celu uzyskania dostępu do zasobów komputerowych,
 - d) do zakłócania i blokowania pracy innych użytkowników, nieuprawnionego niszczenia cudzych danych, itp.
 - e) prowadzenia jakiejkolwiek działalności naruszającej dobre imię Urzędu,
 - f) w czasie pracy do odwiedzania popularnych serwisów i wszystkich innych stron, które nie zawierają treści pomocnych przy wykonywaniu obowiązków służbowych,
 - g) w czasie pracy grania w popularne gry, które znajdują się w standardowym oprogramowaniu, np. pasjans lub dostępnych w Internecie.

III. Zasady korzystania z oprogramowania

§ 7



1. Urząd ma obowiązek posiadania i przechowywania dowodów legalności oprogramowania, zainstalowanego na komputerach, będących na jej stanie, zgodnie z obowiązującymi uregulowaniami prawnymi dot. ochrony własności intelektualnej wyrażonej w ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych oraz przepisami Kodeksu karnego.
2. Dokumenty potwierdzające legalność oprogramowania muszą być przechowywane w sposób zapewniający zabezpieczenie ich przed nieupoważnionym dostępem, zniszczeniem lub uszkodzeniem.
3. Pracownikom zabrania się:
 - a) instalowania na służbowym komputerze jakiegokolwiek oprogramowania bez wymaganej licencji i niezgodnego z potrzebami służbowymi,
 - b) instalowania komunikatorów internetowych oraz korzystania z serwisów społecznościowych, które nie są pomocne przy wykonywaniu obowiązków służbowych,

IV. Zasady korzystania z sieci LAN

§ 8

1. Pracownicy mogą korzystać z sieci LAN w czasie pracy tylko i wyłącznie w celach służbowych :
 - a) poszukiwanie wyjaśnień i interpretacji przepisów prawnych,
 - b) komunikacja i pozyskiwanie informacji z urzędów administracji rządowej i samorządowej, wynikające z wykonywanych obowiązków służbowych,
 - c) przeglądanie stron - Biuletynów Informacji Publicznej,
 - d) kopiowanie danych wykorzystywanych wyłącznie do celów służbowych, o ile nie jest to sprzeczne z prawem autorskim.
2. Zabrania się:
 - a) wykorzystywania sieci LAN w sposób, który mógłby narazić Urząd na utratę dobrego imienia,
 - b) pobierania oprogramowania (w tym w wersjach darmowych), niezwiązanego z wykonywanymi obowiązkami służbowymi,
 - c) podłączania sieci LAN do fizycznie odseparowanych sieci,
 - d) udostępniania łącza internetowego dostarczonego przez Urząd innym osobom bez zgody Wójta Gminy,
 - e) instalowania urządzeń udostępniających Internet na sprzęcie Urzędu bez zgody Wójta Gminy,
 - f) działania na szkodę innych użytkowników Internetu,
 - g) wykonania czynności naruszających prawa autorskie.
3. Zobowiązuje się Pracowników do uważnego czytania i nie ignorowania komunikatów i ostrzeżeń pojawiających się w przeglądarce dotyczących „alertów bezpieczeństwa”.
4. Zabrania się samowolnego podłączania do sieci komputerów lub innych urządzeń.
5. O rozdziale adresów IP decyduje ASI.
6. Zabrania się wykorzystywania gniazd elektrycznych sieci teleinformatycznej do zasilania innych urządzeń niż komputery i peryferia komputerowe.
7. W celu zapewnienia bezpieczeństwa mechanizmom sieci teleinformatycznej Urzędu oraz dla jej użytkowników Pracownikowi zabrania się dokonywania na niej działań o charakterze nielegalnym, a w szczególności:
 - a) umieszczania lub uruchamiania programów i innych obiektów niebezpiecznych, w tym „koni trojańskich”, czy innych programów realizujących niepożądane lub wrogie działania,
 - b) skanowania sieci teleinformatycznej Urzędu,
 - c) prowadzenia ataków, włamań, itp., innych czynności związanych z ingerencją w działanie lub zasoby sieci teleinformatycznej Urzędu, lub Internetu,
 - d) naruszania w jakikolwiek sposób bezpieczeństwa serwerów i ich bezawaryjnej pracy, a zwłaszcza logowania się do serwerów, jeżeli zakres obowiązków tego nie wymaga,
 - e) anonimowego wysyłania poczty elektronicznej z sieci teleinformatycznej Urzędu,
 - f) gromadzenia na stanowisku pracy, tj. stacji roboczej lub na zasobie dyskowym udostępnionym w sieci LAN, w dowolnej, cyfrowej formie materiałów lub treści niezgodnych z obowiązującym prawem lub naruszających dobre obyczaje,
 - g) uruchamiania programów komputerowych z nośników zewnętrznych, tj. z płyt CD/DVD lub nośników typu pendrive, itp.,

- h) rozpowszechnia nielegalnych plików do Internetu, tj. przesyłania zdjęć, filmów, tekstów, czy innych formatów plików.
8. Pracownikowi zakazuje się umożliwiania osobom postronnym dostępu do sieci teleinformatycznej Urzędu, np. umożliwienia pracy na identyfikatorach i hasłach Pracownika.
9. Zabrania się Pracownikom Urzędu wykonywania następujących czynności przy użyciu sprzętu i oprogramowania należącego do Pracodawcy :
- a) korzystania z komputera służbowego do celów prywatnych.
- ⑩ używania poczty elektronicznej Urzędu do celów innych niż służbowe,
 - ⑩ wykorzystywania połączenia z siecią internet do celów innych niż służbowe,
 - ⑩ wysyłania wiadomości pocztowych (e-mail), typu reklamy, „łańcuszki szczęścia”, pornograficznych, itp.,
 - ⑩ logowania się w celach prywatnych lub komercyjnych na stronach WWW, czy uczestniczenia w portalach o charakterze społecznościowym, zwłaszcza towarzyskim, komercyjnych, itp.,
 - ⑩ używania w celach prywatnych lub komercyjnych komunikatorów internetowych w rodzaju Skype, Gadu- Gadu, Tlen, itp.,
 - ⑩ korzystania z serwisów internetowych niezwiązanych z obowiązkami Pracownika, np. oferujących gry internetowe i losowe, hazard, prywatne aukcje, rozrywkę, prywatne listy dyskusyjne., itp.,
 - ⑩ przetwarzania na komputerach materiałów, do których Pracodawca nie posiada praw autorskich,
 - ⑩ korzystania z serwisów internetowych zawierających treści niecenzuralne lub jakiegokolwiek łamiące prawo obowiązujące na terenie Rzeczypospolitej Polskiej,
 - ⑩ instalowania i wykorzystywania jakiegokolwiek oprogramowania bez wiedzy i udziału osób odpowiedzialnych za tego rodzaju czynności w Urzędzie.
 - ⑩ zapisywania, przechowywania na dyskach lokalnych lub zasobach sieciowych wszelkich plików multimedialnych niezwiązanych z wykonywaniem czynności służbowych,
 - ⑩ samodzielnej zmiany konfiguracji sprzętowej zestawu i jego ustawień systemowych bez zgody ASI,
 - ⑩ udostępniania innym użytkownikom haseł dostępowych i ich przechowywanie w łatwo dostępnych lub widocznych miejscach,
 - ⑩ używania nośników danych nieznanego pochodzenia oraz nośników wymiany pamięci wcześniej nie zgłoszonych do ASI.
10. O każdej usterce sprzętu należy powiadomić ASI. Za dane i wykonywanie kopii danych przechowywanych na dyskach lokalnych odpowiada użytkownik zestawu komputerowego.

V. Zasady korzystania ze służbowej poczty elektronicznej

§ 9

1. Nadzór i opiekę techniczną nad systemem poczty elektronicznej Urzędu sprawuje Administrator Sieci Informatycznej (Administrator Poczty).
2. Poczta elektroniczna może być wykorzystywana tylko do celów służbowych.
3. Korespondencja, którą przechowuje i dostarcza system pocztowy jest własnością Urzędu.
4. Pracownik zobowiązany jest do okresowej archiwizacji wiadomości (skrzynki pocztowe posiadają ograniczoną wielkość) oraz kasowania wiadomości.
5. Użytkownikom poczty zabrania się:
 - a) otwierania linków oraz załączników poczty elektronicznej ze źródeł niewiadomego pochodzenia,
 - b) przesyłania i udostępniania danych naruszających prawo, powszechnie uznanych za obsceniczne lub obraźliwe oraz oszczerstw i treści obrażającej uczucia innych,
 - c) rozpowszechniania materiałów o treści pornograficznej, propagujących przemoc, nawołujących do nietolerancji i nienawiści itp., lub naruszających obowiązujące prawo,
 - d) uprawiania hazardu,
 - e) rozpowszechniania niechcianych wiadomości e-mail (spam-u),
 - f) prowadzenia działalności komercyjnej nie związanej z działalnością Urzędu,

- g) rozsyłania listów, które wykorzystując elementy socjotechniki generują niepożądany ruch na serwerach poczty elektronicznej oraz treści prawem chronionych bez odpowiedniego zabezpieczenia np. Szyfrowania,
 - h) przesyłania i udostępniania treści niezgodnych z prawem lub będących przedmiotem ochrony własności intelektualnej lub mogących naruszyć czyjekolwiek prawa osobiste,
 - i) rozpowszechniania wirusów komputerowych i innych programów mogących uszkodzić komputery innych użytkowników Internetu.
6. Niedopuszczalne są próby włamań na konta innych użytkowników.
7. Urząd w celach dowodowych oraz bezpieczeństwa systemów ma prawo do kontroli służbowych skrzynek pocztowych Pracowników, informując ich o kontroli i jej wynikach.

VI. Zasady monitorowania pracy Pracowników przy wykorzystaniu komputerów służbowych

§ 10

Wszelkie czynności pracownika w zakresie działań pracodawcy zmierzających do poprawy jakości pracy z komputerem polegające, w szczególności na eliminowaniu możliwości pobierania określonych danych z Internetu, odciążeniu sieci informatycznej, poprzez ograniczenie możliwości transferu danych z lub do komputera pracownika, usuwaniu nielegalnego oprogramowania, blokowania dostępu do nielegalnych treści oraz kontroli antywirusowej związane są bezpośrednio z bezpieczeństwem Urzędu i ochroną danych osobowych, będą monitorowane.

1. Urząd ma prawo wglądu do zapisanych na służbowym komputerze informacji służbowych. Jeżeli Pracownik zabezpieczył je hasłem, na żądanie przełożonego zobowiązany jest je udostępnić
2. Urząd zastrzega sobie prawo do instalacji na sprzęcie komputerowym oprogramowania do monitorowania legalności programów zainstalowanych na komputerach.
3. Monitorowanie pracy pracowników przy wykorzystaniu komputerów służbowych będzie przeprowadzone na bazie dedykowanego oprogramowania, będącego własnością Pracodawcy, który posiada do niego stosowaną licencję.
4. Zakresem monitoringu w Urzędzie objęte są:
 - a) kontrola zdarzeń na komputerze użytkownika,
 - 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) możliwość podglądu on-line ekranu każdego komputera w Urzędzie,
 - h) monitoring ruchu w sieci informatycznej (LAN, WAN) Urzędu,
 - i) monitoring legalności oprogramowania,
 - j) powiadamianie o monitorowaniu każdego użytkownika po uruchomieniu komputera,
 - k) monitoring służbowych kont poczty e-mail. Pracodawca zastrzega sobie prawo do kontroli treści wysłanych i otrzymanych e-maili z konta służbowego,
 - l) monitoring używania przenośnych nośników danych (pendrive, karty pamięci, CD-ROM, HDD, itp.) z możliwością blokowania, jak i odczytania ich treści,
 - m) monitoring podłączonego sprzętu w Urzędzie.
5. Ruch w sieci teleinformatycznej Urzędu, generowany przez Pracownika, podlega monitoringowi z automatycznym zapisem dostępu do stron WWW.

VII. Zasada korzystania w gniazd prądowych typu Data

§ 11

Zabrania się podłączenia do gniazd prądowych typu "Data" (czerwone gniazda prądowe) innych urządzeń niż urządzenia komputerowe.

VIII. Postanowienia końcowe

§ 12

1. Pracownik zobowiązany jest zwrócić Urzędowi służbowy komputer w stanie nie pogorszonym poza zużycie wynikające z normalnej eksploatacji:
 - a) w dniu ustania stosunku pracy,
 - b) na każde żądanie Wójta Gminy.
2. Kończąc świadczenie pracy dla Urzędu, Pracownik jest zobowiązany przekazać wszystkie dane zapisane w komputerze (dokumenty służbowe tworzone i przechowywane w pamięci komputera, pliki oraz inne posiadane informacje) związane z wykonywanymi zadaniami służbowymi przełożonemu.

§ 13

Za nieprzestrzeganie postanowień niniejszego Regulaminu, wobec Pracownika mogą zostać podjęte odpowiednie sankcje dyscyplinarne lub też, w przypadku podejrzenia naruszenia prawa –Wójt Gminy może dokonać zgłoszenia tego faktu właściwym organom ścigania, bądź też wystąpić z powództwem cywilnym o naprawienie szkody.

