

Zarządzenie Nr 37/2025

STAROSTY ŁOWICKIEGO

z dnia 27 czerwca 2025 r.

**w sprawie wprowadzenia
Procedury ochrony informacji w ramach pracy zdalnej
w Starostwie Powiatowym w Łowiczu**

Na podstawie art. 35 ust. 2 z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2024 r. poz. 107, poz. 1907) oraz art. 67²⁶ ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2025 r. poz. 277; zm. z 2024 r. poz. 1871) zarządzam, co następuje:

§ 1. Wprowadzam *Procedurę ochrony informacji w ramach pracy zdalnej w Starostwie Powiatowym w Łowiczu* stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Nadzór nad wykonaniem zarządzenia powierzam Inspektorowi Ochrony Danych.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA ŁOWICKI

Marcin Kosiorek

Katarzyna Marat

adwokat

Inspektor Ochrony Danych

Martyna Bogucka

Procedura ochrony informacji w ramach pracy zdalnej w Starostwie Powiatowym w Łowiczu

Definicje

§ 1. Ilekroć w niniejszej Procedurze jest mowa o:

- 1) **Procedurze** – rozumie się *Procedurę ochrony informacji w ramach pracy zdalnej w Starostwie Powiatowym w Łowiczu*;
- 2) **Starostwie** - rozumie się przez to Starostwo Powiatowe w Łowiczu;
- 3) **Inspektorze** – rozumie się przez to Inspektora Ochrony Danych w Starostwie Powiatowym w Łowiczu;
- 4) **Rozporządzeniu** – rozumie się przez to rozporządzenie 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. Urz. UE L Nr 119, str. 1);
- 5) **Kierującym komórką organizacyjną** – rozumie się przez to dyrektora wydziału, kierownika biura, przewodniczącego zespołu, osobę na samodzielnym stanowisku w Starostwie Powiatowym w Łowiczu;
- 6) **Pracodawcy** – rozumie się przez to Starostwo Powiatowe w Łowiczu, reprezentowane przez Starostę Łowickiego;
- 7) **Pracy zdalnej** - rozumie się przez to pracę wykonywaną całkowicie lub częściowo w miejscu wskazanym przez pracownika i każdorazowo uzgodnionym z Pracodawcą, w tym pod adresem zamieszkania Pracownika, w szczególności przy wykorzystaniu środków bezpośredniego porozumiewania się na odległość,
- 8) **Pracowniku** – rozumie się przez to zarówno osoby zatrudnione w ramach stosunku pracy, jak i współpracowników na stałe wykonujących zadania w ramach umów cywilnoprawnych, wymagające dostępu do zasobów sprzętowych i informacyjnych Starostwa Powiatowego w Łowiczu;
- 9) **Urządzeniu służbowym** – rozumie się przez to urządzenia, które stanowią własność Starostwa Powiatowego w Łowiczu;
- 10) **Informatyku** – rozumie się przez to osobę odpowiedzialną za infrastrukturę informatyczną Starostwa Powiatowego w Łowiczu, która wykonuje swoje zadania na podstawie umowy o pracę lub umowy cywilnoprawnej;
- 11) **Bezpośrednim przełożonym** – rozumie się przez to Starostę lub kierującego komórką organizacyjną zgodnie z zapisami Regulaminu Organizacyjnego Starostwa Powiatowego w Łowiczu.

Zasady ogólne

§ 2. 1. Procedura została wprowadzona w celu zapewnienia odpowiedniego bezpieczeństwa informacji, w tym danych osobowych, w ramach wykonywania pracy zdalnej, w związku z przepisami Rozporządzenia oraz rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773).

2. Decyzje o możliwości podjęcia pracy zdalnej podejmuje Pracodawca na pisemny wniosek pracownika, z zastrzeżeniem przypadków określonych w art. 67²⁰ § 3 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy.

3. Warunki, zakres oraz harmonogram wykonywanej pracy określa się w odrębnym porozumieniu z pracownikiem.

4. Dla zapewnienia właściwego poziomu bezpieczeństwa informacji pracownik podejmujący pracę zdalną zapewnia odpowiednie warunki techniczne i lokalowe w miejscu wykonywania pracy zdalnej odpowiadające warunkom zawartym w Procedurze.

5. Pracownik w ramach pracy zdalnej przetwarza udostępnione mu informacje wyłącznie w celach służbowych. Zabrania się wykorzystywania danych w jakichkolwiek innych celach.

6. Pracownik przed rozpoczęciem wykonywania pracy zdalnej podpisuje oświadczenie o zapoznaniu się z Procedurą, którego wzór stanowi załącznik do Procedury.

Bezpieczeństwo miejsca świadczenia pracy zdalnej

§ 3. 1. Pracownik wykonuje pracę zdalną pod adresem, który wskazał w porozumieniu, o którym mowa w § 2 ust. 3.

2. Niedozwolone jest podejmowanie pracy w innym miejscu niż te, o którym mowa powyżej, w szczególności w miejscach użytku publicznego.

3. Pracownik realizuje swoje obowiązki służbowe w ustalonych godzinach, zgodnie z harmonogramem ustalonym w porozumieniu, o którym mowa w § 2 ust. 3.

4. Pracownik jest zobowiązany do zabezpieczenia dostępu do posiadanych informacji przed osobami postronnymi, w tym wspólnie z nim zamieszkującymi, przed nieuprawnionym wglądem, zniszczeniem, pobraniem, udostępnieniem lub modyfikacją.

5. Pracownik jest zobowiązany do uniemożliwienia wglądu osobom postronnym, w tym wspólnie z nim zamieszkującym, wglądu w treści wyświetlane na ekranie sprzętu komputerowego poprzez odpowiednie ustawienie ekranu monitora.

6. Pracownik jest zobowiązany do dostosowania polityki czystego ekranu poprzez zastosowanie wygaszacza ekranu wraz z automatyczną blokadą, a przy dłuższej nieobecności ustawionego maksymalnie na okres 5 minut, oraz hasła dostępowego do systemu.

7. Pracownik odchodząc od stanowiska pracy lub kończąc korzystanie ze służbowego telefonu zobowiązany jest upewnić się, że urządzenie zostało zablokowane przed dostępem osób nieuprawnionych.

8. W przypadku pracy na sprzęcie prywatnym, pracownik zobowiązany jest do wydzielania odrębnego konta systemowego, na którym wykonywana będzie praca zdalna. Hasło do konta powinien znać wyłącznie pracownik.

9. Hasła, o których mowa w ust. 6 i 8, powinny odpowiadać zasadom polityki haseł zawartej w instrukcji zarządzania system informatycznym obowiązującej w Starostwie.

10. Pracownik zobowiązany jest do bezpiecznego przechowywania dokumentacji papierowej w miejscach niedostępnych dla osób postronnych, w tym wspólnie z nim zamieszkujących.

11. Prowadzenie służbowych spotkań zdalnych lub rozmów telefonicznych jest realizowane w sposób zapewniający poufność informacji przekazywanych w trakcie rozmowy.

Bezpieczeństwo Internetu

§ 4. 1. Pracownik wykonuje pracę zdalną z wykorzystaniem urządzeń służbowych lub urządzeń prywatnych, w zależności od uzgodnień przyjętych w porozumieniu, o którym mowa w § 2 ust. 3.

2. W przypadku korzystania z domowej sieci WiFi należy zapewnić, aby została ona skonfigurowana w sposób minimalizujący ryzyko włamania, a w szczególności:

- 1) korzystanie z Internetu powinno wymagać uwierzytelnienia poprzez podanie hasła, a połączenie z urządzeniem powinno podlegać szyfrowaniu;
- 2) jeśli jest to możliwe, należy zmienić login do panelu administracyjnego na własny;
- 3) dostęp do panelu administracyjnego routera powinien być możliwy wyłącznie z urządzeń znajdujących się w sieci domowej;
- 4) oprogramowanie urządzenia sieciowego powinno być regularnie aktualizowane.

3. Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udziela informatyk Starostwa.

Bezpieczeństwo urządzeń służących do pracy zdalnej

§ 5. 1. Zabronione jest udostępnianie urządzeń wykorzystywanych do realizowania pracy zdalnej osobom trzecim, w tym wspólnie zamieszkującym.

2. Jeżeli z jakichś względów pracownik nie może wykonywać pracy zdalnej z wykorzystaniem służbowego sprzętu, zgłasza to pracodawcy, który może wydać zgodę na pracę z wykorzystaniem prywatnych urządzeń.

3. Po uzgodnieniu z jakich urządzeń będzie korzystał pracownik, fakt ten powinien zgłosić informatykowi w drodze służbowej wiadomości e-mail.

4. Wydanie urządzeń służbowych pracownikowi następuje po sporządzeniu protokołu.

5. Informatyk odnotowuje, które urządzenia będą wykorzystywane przez pracownika do pracy zdalnej i jeśli jest to niezbędne przeprowadza ich przegląd.

6. W przypadku, gdy przegląd jest niemożliwy, pracownik na żądanie informatyka udostępnia urządzenie zdalnie z wykorzystaniem zaproponowanego narzędzia w celu dokonania jego zdalnego przeglądu.

7. Przegląd urządzeń prywatnych, na których wykorzystanie wyrażono zgodę, jest obowiązkowy.

8. Ustala się następujące minimalne wymagania w zakresie bezpieczeństwa:

- 1) zainstalowanie legalnego oprogramowanie na urządzeniach, które będzie podlegać automatycznym aktualizacją;
- 2) włączenie zapory systemowej;
- 3) zainstalowanie i zapewnienie działania w tle programu antywirusowego;
- 4) zastosowanie uwierzytelnienia przy pomocy indywidualnego loginu i silnego hasła użytkownika przy zalogowaniu do systemu operacyjnego, z zastrzeżeniem stosowania zasad polityki haseł zawartej w instrukcji zarządzania system informatycznym obowiązującej w Starostwie;
- 5) wyłączenie autouzupełniania i zapamiętywania haseł w przeglądarce internetowej;
- 6) zainstalowanie programu umożliwiającego zaszyfrowanie i odszyfrowanie danych (np. 7-zip);
- 7) ustawienie automatycznego blokowania urządzenia po dłuższym braku aktywności.

9. W porozumieniu, o którym mowa w § 2 ust. 3, można uwzględnić dodatkowe zabezpieczenia, takie jak m.in.

- 1) zaszyfrowanie dysku;
- 2) wyłączenie portów pamięci zewnętrznych;
- 3) zainstalowanie oprogramowania służącego monitorowaniu wykonywania pracy przez pracownika, wykorzystywanego zgodnie z wymaganiami przepisów prawa pracy.

Bezpieczeństwo przekazywanych informacji

§ 6. 1. Pracownik do pracy zdalnej wykorzystuje tylko i wyłącznie służbowe systemy, programy i aplikacje udostępnione mu przez pracodawcę.

2. Wykorzystywanie prywatnej poczty e-mail do celów służbowych jest zabronione.

3. Wykorzystanie prywatnych urządzeń typu pendrive i pamięć masowa do celów służbowych jest zabronione.

4. Przesyłanie informacji o charakterze poufnym, w tym danych osobowych, z wykorzystaniem poczty e-mail, należy przesyłać w załączniku zabezpieczonym hasłem.

5. Hasło powinno zostać przekazane odbiorcy inną drogą komunikacji i powinno być odpowiednio skomplikowane.

6. Dozwolone jest ustalenie stałego hasła na komunikację z jednym odbiorcą, o ile nie będzie wykorzystywane do zabezpieczania plików w komunikacji z innym odbiorcą.

7. Każda wiadomość powinna być wysłana z należytą starannością, polegającą w szczególności na sprawdzeniu, czy jest kierowana do odpowiedniego odbiorcy.

8. W przypadku wysyłania informacji do kilku odbiorców, którzy nie znają się wzajemnie i/lub ich adresy e-mail są adresami prywatnymi, należy skorzystać z opcji „Ukryte do wiadomości” (UDW/BCC).

9. Zapisy z ust. 3-7 stosuje się również w wewnętrznej korespondencji e-mail dokonywanej z innymi pracownikami.

10. Pracownik może przekazywać pliki z informacjami chronionymi z wykorzystaniem udostępnionych serwerów sieciowych lub plików FTP.

11. Wykorzystywanie innych narzędzi do przesyłania i udostępniania plików (weTransfer, Google Drive, DropBox) jest zabronione.

Bezpieczeństwo korzystania z dokumentów w formie papierowej

§ 7. 1. W Starostwie obowiązuje zakaz zabierania dokumentów lub ich kopii poza siedzibę Starostwa.

2. Pracownik wykonujący pracę zdalnie zgłasza do pracodawcy prośbę o możliwość skopiowania dokumentów papierowych oraz zabrania ich do domu na czas wykonywania pracy, o ile jest to niezbędne dla skutecznego wykonywania pracy zdalnej.

3. Po uzyskaniu zgody na piśmie lub w formie służbowej wiadomości e-mail, pracownik jest obowiązany sporządzić kopie niezbędnych dokumentów, a następnie przygotować zestawienie zawierające informację o tym, jakie dokumenty i w jakiej liczbie zostały skopiowane.

4. Niedozwolone jest zabieranie poza siedzibę Starostwa oryginałów dokumentów.

5. Podczas przewożenia dokumentów do miejsca realizowania pracy zdalnej, należy je zabezpieczyć i przenosić w taki sposób, aby były one niewidoczne i niedostępne dla osób trzecich.

6. Podczas pracy zdalnej pracownik zobowiązany jest przechowywać udostępnione dokumenty wyłącznie na okres niezbędny do wykonywania określonych zadań podczas pracy zdalnej. Po tym czasie zobowiązany jest je niezwłocznie zwrócić.

7. Bezpośredni przełożony każdorazowo weryfikuje kompletność dokumentów zwróconych przez pracownika. Kopie dokumentów brakowane są zgodnie z obowiązującymi przepisami prawa.

Naruszenie bezpieczeństwa danych przy pracy zdalnej

§ 8. 1. Pracownik, który stwierdzi lub podejrzewa naruszenie bezpieczeństwa informacji, a w szczególności przetwarzania danych osobowych, zobowiązany jest do niezwłocznego poinformowania o tym fakcie informatyka lub Inspektora.

2. Informację, o której mowa powyżej, powinno się przekazać w formie rozmowy telefonicznej na numer telefonu 46 811 53 12 lub 46 811 53 64 lub wiadomości e-mail na adres inf@powiatlowicki.pl lub iod@powiatlowicki.pl.

3. W przypadku powzięcia informacji o naruszeniu bezpieczeństwa informacji, zostaje wszczęte postępowanie wyjaśniające, którego tryb i przebieg określony został w dokumentacji dot. zgłaszania naruszeń bezpieczeństwa informacji obowiązujących w Starostwie.

Postanowienia końcowe

§ 9. 1. Procedura stanowi wewnętrzną regulację Starostwa Powiatowego w Łowiczu i obowiązuje wszystkich pracowników Starostwa.

2. Procedura obowiązuje od dnia jej wprowadzenia w życie, zgodnie z zarządzeniem Starosty. Wszelkie zmiany w Procedurze obowiązują od dnia ich wprowadzenia w życie, zgodnie z zarządzeniem zmieniającym.

3. Przypadki nieuzasadnionego naruszenia postanowień wynikających z Procedury mogą być kwalifikowane jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.

STAROSTA ŁOWICKI

Marcin Kosiorek

Załącznik
do Procedury ochrony informacji w ramach pracy
zdalnej w Starostwie Powiatowym w Łowiczu
wprowadzonej
Zarządzeniem Nr/2025
Starosty Łowickiego
z dnia 2025 r.
w sprawie wprowadzenia Procedury ochrony
informacji w ramach pracy zdalnej w Starostwie
Powiatowym w Łowiczu

Łowicz, dnia

.....
(imię i nazwisko pracownika)

.....
(stanowisko pracownika)

OŚWIADCZENIE

Oświadczam, że zapoznałem/-am się z regulacjami zawartymi w *Procedurze ochrony informacji w ramach pracy zdalnej w Starostwie Powiatowym w Łowiczu* i przyjąłem/-am je do stosowania.

.....
(podpis pracownika)