

ZARZĄDZENIE NR 53/2025
STAROSTY POWIATU SZTUMSKIEGO

z dnia 17 grudnia 2025 r.

Instrukcja zarządzania uprawnieniami w ramach Krajowego Systemu e-Faktur

Rozdział 1.
Przepisy ogólne

§ 1. Podstawa prawna: rozporządzenie Ministra Finansów z dnia 27 grudnia 2021 r. w sprawie korzystania z Krajowego Systemu e-Faktur (Dz.U. poz. 2481 ze zm.) zarządzam co następuje:

§ 2. Ilekroć w niniejszym dokumencie jest mowa o:

- 1) Powiat Sztumski – należy przez to rozumieć Powiat Sztumski – Starostwo Powiatowe
- 2) administratorze systemu KSeF – należy przez to rozumieć osobę upoważnioną na podstawie zgłoszenia ZAW-FA
- 3) użytkownika systemu – należy przez to rozumieć osobę upoważnioną do:
 - a) wystawiania faktur,
 - b) dostępu do faktur.
 - c) przeglądu faktur.

Rozdział 2.
Procedury nadawania i zmiany uprawnień w ramach KSeF

§ 3. 1. Każdy użytkownik systemu przed uzyskaniem uprawnień do systemu KSeF ma obowiązek zapoznać się z:

- 1) rozporządzeniem Ministra Finansów z dnia 27 grudnia 2021 r. w sprawie korzystania z Krajowego Systemu e-Faktur,
- 2) niniejszą instrukcją.

2. Zapoznanie się z przepisami wymienionymi w ustępie 1 pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik nr 2 do niniejszej instrukcji.

3. Administrator systemu KSeF przyznaje pracownikowi uprawnienia w zakresie dostępu do systemu.

4. Karta ewidencyjna powinna odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień oraz umożliwiać przeglądanie historii zmian uprawnień użytkowników.

5. Wzór karty ewidencyjnej powinien zawierać:

- 1) imię i nazwisko użytkownika systemów informatycznych,
- 2) rodzaj uprawnień,
- 3) datę nadania uprawnień,
- 4) datę odebrania uprawnień,
- 5) przyczynę odebrania uprawnień,
- 6) podpis administratora systemu KSeF.

6. Wzór karty ewidencyjnej uprawnień w zakresie dostępu i obsługi KSeF związanych z dostępem do KSeF stanowi załącznik nr 3 do niniejszej instrukcji.

7. Przyznanie uprawnień w zakresie dostępu do systemu KSeF polega na wprowadzeniu do systemu każdego użytkownika oraz wykazu dostępnych mu danych i operacji.

8. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.

9. Mając na uwadze, że system KSeF jest systemem informatycznym, w ramach którego przetwarzany jest szeroki zakres danych, każdy użytkownik powinien przestrzegać:

- a) zasad bezpiecznego uwierzytelniania się,
- b) regulacji wewnętrznych obowiązujących w danej jednostce organizacyjnej dotyczących bezpiecznej pracy w systemach informatycznych oraz ochrony danych osobowych.

10. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.

11. Wszelkie przekroczenia lub próby przekroczenia przyznaných uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.

12. Pracownik zatrudniony przy pracy w systemie KSeF zobowiązany jest do zachowania tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.

13. W systemie KSeF stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do komputera oraz na poziomie dostępu do aplikacji.

14. Odebranie uprawnień pracownikowi dokonywane jest przez administratora systemu z podaniem daty oraz przyczyny odebrania uprawnień. Odebranie uprawnień pracownikowi równoważne jest z usunięciem konta w systemie KSeF.

15. Identyfikator osoby, która utraciła uprawnienia dostępu do systemu KSeF, należy niezwłocznie zablokować w systemie informatycznym, w którym jest on przetwarzany, oraz unieważnić jej hasło.

16. Administrator systemu KSeF zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym.

Rozdział 3. Zasady posługiwania się hasłami

§ 4. 1. Bezpośredni dostęp do systemu KSeF może mieć miejsce wyłącznie po podaniu identyfikatora i hasła.

2. Hasło powinno być zmieniane przez użytkownika co najmniej raz w miesiącu.

3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu KSeF nie powinien być przydzielany innej osobie.

4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.

5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.

6. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.

7. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.

8. Przy wyborze hasła obowiązują następujące zasady:

- 1) minimalna długość hasła – 8 znaków;
- 2) należy stosować:
 - a) hasła zawierające kombinacje liter i cyfr,
 - b) hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, #, & itp., o ile system informatyczny na to pozwala,
 - c) hasła, które można zapamiętać bez zapisywania,
 - d) hasła łatwe i szybkie do wprowadzenia, po to, by trudniej było podejrzeć je osobom trzecim.

9. Zmiany hasła nie wolno zlecać innym osobom.

10. W systemach, które umożliwiają opcję zapamiętania nazw użytkownika lub jego hasła, nie należy korzystać z tego ułatwienia.

Rozdział 4. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

§ 5. 1. Aby rozpocząć pracę w systemie KSeF, należy zalogować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.

2. W systemie KSeF stosuje się uwierzytelnienie dwustopniowe: na poziomie dostępu do komputera oraz na poziomie dostępu do aplikacji.

3. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wylogować się z systemu (zablokować dostęp) lub – jeżeli taka możliwość nie istnieje – wyjść z programu.

4. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać operację wylogowania z systemu.

5. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i – jeżeli jest to konieczne – wylogować się z sieci komputerowej.

6. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.

Rozdział 5.

Środki ochrony systemu przed złośliwym oprogramowaniem, w tym wirusami komputerowymi

§ 6. 1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe.

2. Każdy e-mail pobierany przez program pocztowy pracowników Starostwa Powiatowego w Sztumie musi być sprawdzony pod kątem występowania wirusów przez program antywirusowy.

3. Definicje wzorców wirusów aktualizowane są w trybie automatycznym kilka razy na dobę.

4. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnika zamierza użyć.

5. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia.

6. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.

7. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.

8. Administrator systemu informatycznego przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach – minimum raz na trzy miesiące.

9. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.

10. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wirusa wykryto.

Rozdział 6.

Postępowanie w sytuacji naruszenia dostępu do KSeF

§ 7. Postępowanie w sytuacji naruszenia dostępu do KSeF określa instrukcja regulująca postępowanie pracowników Starostwa Powiatowego w Sztumie zatrudnionych przy obsłudze KSeF w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych, stanowiąca załącznik nr 4 do niniejszej instrukcji.

Rozdział 7.

Procedury wykonywania przeglądów i konserwacji systemu

§ 8. 1. Awaria systemu KSeF:

- 1) w czasie niedostępności KSeF nie będzie możliwości korzystania z systemu;
- 2) faktury będą mogły być wystawiane wyłącznie w czasie dostępności systemu; w przypadku, gdy data wystawienia zawarta w fakturze (pole P_1) będzie inna niż data przesłania do systemu, fakturę uznaje się za wystawioną w momencie jej przesłania zgodnie z art. 106na ust. 1 ustawy o VAT;
- 3) komunikaty o niedostępności systemu monitoruje pracownik jednostki pod adresem: <https://www.gov.pl/web/kas/komunikaty>.

2. Rejestracja działań konserwacyjnych, awarii oraz napraw:

- 1) administrator systemu KSeF prowadzi „Dziennik systemu informatycznego”; wzór i zakres informacji rejestrowanych w dzienniku określa załącznik nr 5 do niniejszej instrukcji;
- 2) wpisów do dziennika może dokonywać administrator systemu KSeF, administrator systemu lub osoby wyznaczone.

Rozdział 8.

Połączenie do sieci Internet

§ 9. Połączenie lokalnej sieci komputerowej z Internetem jest dopuszczalne wyłącznie po zainstalowaniu mechanizmów ochronnych oraz kompleksowego oprogramowania antywirusowego.

Rozdział 9.
Postanowienia końcowe

§ 10. Na stanowisku pracy obowiązuje bezwzględny zakaz instalowania jakiegokolwiek oprogramowania. Pracownik, chcąc zainstalować aplikację lub program, musi uzyskać pisemną zgodę od administratora systemu informatycznego.

Starosta Powiatu
Sztumskiego

Leszek Sarnowski

Załącznik nr 1
do Instrukcji zarządzania uprawnieniami w ramach KSeF
Upoważnienie dla administratora systemu KSeF

Na podstawie § 3 pkt 3 Instrukcji zarządzania systemem informatycznym z dniem 17 grudnia 2025 roku wyznaczam administratora systemu KSeF, powierzając tę funkcję ~~Panu~~ /Pani Lucynie Bednarskiej posługującemu/ej się numerem [REDACTED]

.....
(podpis administratora systemu KSeF)

Ja, niżej podpisany/a, zobowiązuję się do pełnienia obowiązków administratora systemu KSeF w oparciu o przepisy wewnętrzne obowiązujące w Starostwie Powiatowym w Sztumie.

.....
(podpis administratora systemu KSeF)

**Oświadczenie
do Instrukcji zarządzania uprawnieniami w ramach KSeF**

Oświadczam, że w związku z wykonywaniem obowiązków służbowych przetwarzam dane oraz mam dostęp do systemu KSeF, a także zapoznałem się z:

- 1) rozporządzeniem Ministra Finansów z dnia 27 grudnia 2021 r. w sprawie korzystania z Krajowego Systemu e-Faktur,
- 2) Instrukcją zarządzania uprawnieniami w ramach KSeF w Starostwie Powiatowym w Sztumie

.....
(podpis pracownika)

Załącznik nr 3
do Instrukcji zarządzania uprawnieniami w ramach KSeF

Karta ewidencyjna uprawnień w zakresie dostępu i obsługi KSeF
w Starostwie Powiatowym w Sztumie

Nazwisko i imię użytkownika				
Lp.	Rodzaj uprawnienia	Data nadania uprawnień	Podpis administratora systemu KSeF	Data i przyczyna odebrania uprawnień
1.				
2.				
3.				
4.				
5.				
6.				

Załącznik nr 4

do Instrukcji zarządzania uprawnieniami w ramach KSeF

Instrukcja regulująca postępowanie pracowników

Starostwa Powiatowego w Sztumie

zatrudnionych przy przetwarzaniu danych osobowych

w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych

§ 1

Niniejsza instrukcja reguluje postępowanie pracowników Starostwa Powiatowego w Sztumie zatrudnionych przy obsłudze systemu KSeF w przypadku stwierdzenia naruszenia bezpieczeństwa danych.

§ 2

Celem niniejszej instrukcji jest określenie zadań pracowników zatrudnionych przy obsłudze systemu KSeF w zakresie:

- 1) ochrony danych przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą oraz
- 2) ochrony zasobów technicznych w przypadku stwierdzenia naruszenia ochrony danych lub zabezpieczeń systemu informatycznego.

§ 3

Naruszenie ochrony danych systemu KSeF może zostać stwierdzone na podstawie oceny:

- 1) stanu urządzeń technicznych,
- 2) zawartości zbiorów danych osobowych,
- 3) sposobu działania programu lub jakości komunikacji w sieci teleinformatycznej,
- 4) metod pracy (w tym obiegu dokumentów).

§ 4

W przypadku stwierdzenia naruszenia ochrony danych systemu KSeF należy bezzwłocznie:

- 1) powiadomić administratora systemu KSeF;
- 2) zablokować dostęp do systemu dla użytkowników oraz osób nieupoważnionych;
- 3) podjąć działania mające na celu zminimalizowanie lub całkowite wyeliminowanie powstałego zagrożenia – o ile czynności te nie spowodują przekroczenia uprawnień pracownika;
- 4) zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia bezpieczeństwa systemu.

§ 5

1. Pracownik, który stwierdził naruszenie bezpieczeństwa danych systemu KSeF, jest zobowiązany niezwłocznie powiadomić administratora systemu KSeF.

2. Na stanowisku, na którym stwierdzono naruszenie zabezpieczenia danych, administrator systemu KSeF i osoba przełożona pracownika przejmują nadzór nad pracą w systemie, odsuwając jednocześnie od stanowiska pracownika, który dotychczas na nim pracował, aż do czasu wydania odmiennej decyzji.

§ 6

Administrator systemu KSeF lub osoba przez niego upoważniona podejmuje czynności wyjaśniające, mające na celu ustalenie:

- 1) przyczyn i okoliczności naruszenia bezpieczeństwa danych osobowych;
- 2) osób winnych naruszenia bezpieczeństwa danych osobowych;
- 3) skutków naruszenia.

§ 7

1. Administrator danych zobowiązany jest do powiadomienia o zaistniałej sytuacji Starostę Powiatu Sztumskiego, który podejmuje decyzje o wykonaniu czynności zmierzających do przywrócenia poprawnej pracy systemu oraz o ponownym przystąpieniu do pracy w systemie.

2. Administrator systemu KSeF zobowiązany jest do sporządzenia pisemnego raportu na temat zaistniałej sytuacji, zawierającego co najmniej:

- 1) datę i miejsce wystąpienia naruszenia,
- 2) zakres ujawnionych danych,
- 3) przyczynę ujawnienia, osoby odpowiedzialne oraz stosowne dowody winy,
- 4) sposób rozwiązania problemu,
- 5) przyjęte rozwiązania mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

Załącznik nr 5

do Instrukcji zarządzania uprawnieniami w ramach KSeF

Dziennik systemu informatycznego

w Starostwie Powiatowym w Sztumie

Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu KSeF, a w szczególności:

- 1) w przypadku awarii – opis awarii, przyczyn awarii, szkód wynikłych na skutek awarii, sposobu usunięcia awarii, opis systemu po awarii, wnioski;
- 2) w przypadku konserwacji systemu – opis podjętych działań, wnioski.

Lp.	Data i godzina zdarzenia	Opis zdarzenia	Podjęte działania	Wnioski	Podpis
1.					
2.					
3.					
4.					



DOKUMENT PODPISANY ELEKTRONICZNIE

Dane podpisywanego dokumentu

Typ dokumentu	Zarządzenie
Numer dokumentu	53/2025
Data dokumentu	2025-12-17
Organ wydający	Starosta Powiatu Sztumskiego
Przedmiot regulacji	Instrukcja zarządzania uprawnieniami w ramach Krajowego Systemu e-Faktur
Identyfikator dokumentu	ODA1BE3F-FD00-4C0B-8221-103DBB257D1C

Informacje o złożonych podpisach elektronicznych

Podpis:	
Sygnatura	Signature-1393547995
Numer seryjny	1808CC2D38624E0A72BCF686EB6E18325028ABC4
Osoba podpisująca	Leszek Jan Sarnowski
Kraj	PL
Data złożenia podpisu	17.12.2025 13:43:16
Zakres podpisu	Podpis całego dokumentu
Wystawca certyfikatu	VATPL-5260300517 COPE SZAFIR - Kwalifikowany Krajowa Izba Rozliczeniowa S.A. PL