1. O tym dokumencie

1.1. Data ostatniej aktualizacji.

Jest to wersja 1.3, opublikowana w dniu 09.02.2026 roku.

1.2. Lista dystrybucyjna powiadomień.

Obecnie NSOC NASK S.A. nie korzysta z żadnych list dystrybucyjnych do powiadamiania o zmianach w tym dokumencie.

1.3. Miejsca, w których można znaleźć niniejszy dokument.

Aktualna wersja niniejszego dokumentu opisującego NSOC NASK S.A. jest dostępna na stronie internetowej NASK S.A.; jej adres URL to: https://www.nasksa.pl/pliki_do_pobrania Proszę upewnić się, że używasz najnowszej wersji.

1.4. Uwierzytelnianie tego dokumentu.

Dokument ten został podpisany przez klucz PGP NASK S.A. Podpis znajduje się również na naszej stronie internetowej pod adresem: https://www.nasksa.pl/pliki_do_pobrania

2. Dane kontaktowe

2.1. Nazwa zespołu

NSOC NASK S.A.

2.2. Adres

NASK S.A. ul. 11 Listopada 23, 03-446 Warszawa

2.3. Strefa czasowa

Europe/Warsaw (CET/CEST)

2.4. Numer telefonu

+48 22 380 86 07

2.5. Adres poczty elektronicznej

NSOC@nasksa.pl

2.6. Klucze publiczne

NASK S.A. posiada klucz PGP, szyfrowanie RSA, o identyfikatorze 02B4FA6103D0F00E oraz odcisku palca CABCE1A26E00EFF709BEA57802B4FA6103D0F00E.

2.7. Inne informacje Ogólne

Informacje o NSOC NASK S.A., a także linki do różnych zalecanych zasobów bezpieczeństwa, można znaleźć na stronie: https://www.nasksa.pl/nsoc

2.8. Punkty kontaktowe

Dla klientów preferowana metoda kontaktu z NSOC NASK S.A. jest e-mail na adres

NSOC@nasksa.pl; wiadomość wysłana na ten adres będzie obsługiwana przez odpowiedniego operatora. Zachęcamy, aby klienci używali szyfrowania PGP podczas wysyłania jakichkolwiek informacji wrażliwych dla NASK S.A. Jeśli nie ma możliwości skorzystania z poczty elektronicznej, z NSOC NASK S.A. można skontaktować się telefonicznie. NSOC NASK S.A. działa 24 godziny na dobę.

3. Statut

3.1. Misja organizacji

Misja NSOC NASK S.A. jest identyfikowanie, analizowanie i łagodzenie zagrożeń skierowanych na swoich klientów. Jako zasadnicza część krajowego systemu bezpieczeństwa cybernetycznego, NSOC NASK S.A. przyczynia się do zapewnienia bezpieczeństwa cybernetycznego na poziomie krajowym.

3.2. Obszar działania

Obszar działania NSOC NASK S.A. obejmuje wszystkich użytkowników systemów i sieci

teleinformatycznych NASK S.A., w tym jej spółek zależnych i innych zewnętrznych podmiotów korzystających z infrastruktury sieciowej i platform usługowych NASK S.A., dla których świadczone są usługi.

### 3.3. Finansowanie i/lub przynależność

NSOC NASK S.A. jest finansowo utrzymywany przez NASK S.A.

### 3.4. Organ NSOC NASK S.A.

Działa pod nadzorem delegowanym przez kierownictwo Pionu Cyberbezpieczeństwa NASK S.A.

## 4. Regulamin

### 4.1. Rodzaje incydentów i poziom wsparcia

NSOC NASK S.A. jest upoważniony do rozwiązywania wszelkiego rodzaju incydentów związanych z bezpieczeństwem komputerów i sieci, które mogą wystąpić w NASK S.A. (w zakresie świadczonych usług). NSOC NASK S.A. priorytetowo traktuje zdarzenia według ich wagi, zasięgu i znaczenia.

Incydenty są obsługiwane zgodnie z priorytetem. Poziom wsparcia zapewnianego przez NSOC NASK S.A. będzie się różnić w zależności od wagi i rodzaju problemu, a także innych okoliczności istotnych dla sprawy.

### 4.2. Współpraca, interakcja i ujawnianie informacji

Wszystkie informacje przekazywane do NSOC NASK S.A. w związku z obsługą incydentów cyberbezpieczeństwa są traktowane jako poufne i wykorzystywane wyłącznie w celu identyfikacji, analizy, ograniczenia skutków oraz zapobiegania dalszym incydentom. Przetwarzanie informacji odbywa się zgodnie z obowiązującymi przepisami prawa polskiego i UE, w tym przepisami dotyczącymi ochrony danych osobowych, oraz zgodnie z wewnętrznymi regulacjami bezpieczeństwa.

Zasady współpracy i wymiany informacji:

NSOC NASK S.A. współpracuje w zakresie niezbędnym do obsługi incydentu z podmiotami zaangażowanymi w jego obsługę, w szczególności z: administratorami dotkniętych systemów, dostawcami usług ICT, operatorami infrastruktury, producentami oprogramowania oraz innymi zespołami CSIRT/CERT.

Informacje mogą być przekazywane stronom trzecim wyłącznie na zasadzie need-to-know oraz w zakresie minimalnym koniecznym do identyfikacji źródła, ograniczenia zagrożenia, usunięcia skutków lub koordynacji działań naprawczych.

Tam, gdzie to możliwe, NSOC NASK S.A. stosuje klasyfikację informacji w celu określenia dopuszczalnego kręgu odbiorców i warunków dalszego udostępniania.

Dane wrażliwe i dane osobowe:

NSOC NASK S.A. minimalizuje zakres przetwarzanych danych wrażliwych (np. konfiguracje, logi, próbki) i danych osobowych do poziomu koniecznego do realizacji celu obsługi incydentu.

Dane osobowe nie są udostępniane stronom trzecim, chyba że istnieje ku temu jednoznaczna podstawa prawna albo uprzednie, wyraźne upoważnienie/zgoda klienta lub osoby, której dane dotyczą (w zakresie dopuszczalnym przepisami).

W przypadku konieczności przekazania informacji wrażliwych do podmiotów zewnętrznych, NSOC NASK S.A. ogranicza zakres przekazywanych danych, a gdy to zasadne — stosuje pseudonimizację lub anonimizację.

Ujawnianie informacji i komunikacja zewnętrzna:

NSOC NASK S.A. nie publikuje informacji o incydentach ani nie przekazuje ich podmiotom niezaangażowanym w obsługę incydentu bez uzasadnionej potrzeby operacyjnej lub bez wymaganej podstawy prawnej.

Informacje mogą zostać przekazane właściwym organom publicznym, nadzorczym lub organom ścigania wyłącznie w zakresie wymaganym obowiązującymi przepisami lub na podstawie prawnie wiążącego żądania.

Retencja i dowodowość:

Dane i artefakty z obsługi incydentów (np. zgłoszenia, korespondencja, logi, wskaźniki) są przechowywane przez okres niezbędny do realizacji celu obsługi incydentu oraz zgodnie z wewnętrzną polityką retencji i obowiązkami wynikającymi z przepisów prawa.

### 4.3. Komunikacja i uwierzytelnianie

NSOC NASK S.A. jest zobowiązany do przestrzegania przepisów i zasad obowiązujących w Polsce i UE dotyczących przetwarzania poufnych informacji.

Wszelka komunikacja e-mailowa powinna być oznaczona przy użyciu standardów TLP 2.0. Dane o niskiej czułości mogą zostać wysłane za pomocą niezaszyfrowanej wiadomości e-mail, jednak nie jest to uważane za bezpieczne. Szyfrowanie PGP jest zalecane, szczególnie w przypadku wrażliwych danych.

## 5. Usługi

### 5.1. Wykrywanie i analiza incydentów

Ustalenie autentyczności incydentu. Ustalenie pierwotnej przyczyny incydentu. Określenie odpowiedniej reakcji. Ocena dotkliwości incydentu.

### 5.2. Ograniczenie ryzyka i plany naprawcze

Przygotowanie strategii naprawczej post factum. Przygotowywanie zaleceń dotyczących ulepszeń bezpieczeństwa dla administratorów systemu. Opracowanie procedur obsługi różnych rodzajów incydentów związanych z bezpieczeństwem cybernetycznym.

### 5.3. Ocena incydentów

Korelacja incydentów na podstawie zebranych danych. Ciągłe poszukiwanie sposobów na poprawę wydajności zespołów.

### 5.4. Zapobieganie incydentom

Koordynacja reagowania na zagrożenia.  Zbieranie danych o zagrożeniach bezpieczeństwa i znanych wskaźnikach naruszenia bezpieczeństwa z różnych źródeł. Obserwacja aktualnych zagrożeń technologicznych i bezpieczeństwa. Opracowywanie i ulepszanie istniejących narzędzi i mechanizmów bezpieczeństwa w celu ciągłego podnoszenia poziomu bezpieczeństwa.

### 5.5. Aktywne działania

Współtworzenie ogłoszeń o nowych zagrożeniach dla swoich klientów

Szkolenia i inne działania (takie jak symulacje prawdziwych incydentów) w celu poprawy wydajności zespołu zgłaszanie incydentów.

Przypadki naruszenia bezpieczeństwa należy zgłaszać za pomocą zaszyfrowanej wiadomości e-mail na adres: NSOC@nasksa.pl

## 6. Zastrzeżenia

Pomimo, iż przy przygotowaniu informacji, powiadomień i alertów zostały podjęte wszelkie środki ostrożności, NSOC NASK S.A. (jak również NASK S.A.) nie ponosi odpowiedzialności za błędy lub przeoczenia, ani za szkody wynikające z wykorzystania zawartych w nich informacji.

# 1. About this document

## 1.1. Date of last update

This is version 1.3, published on 09 February 2026.

## 1.2. Distribution list for notifications

Currently, NSOC NASK S.A. does not use any distribution lists to notify about changes to this document.

## 1.3. Locations where this document can be found

The current version of this document describing NSOC NASK S.A. is available on the NASK S.A. website; its URL is: https://www.nasksa.pl/pliki_do_pobrania

Please ensure that you are using the latest version.

## 1.4. Authentication of this document

This document has been signed with the NASK S.A. PGP key. The signature is also available on our website at: https://www.nasksa.pl/pliki_do_pobrania

# 2. Contact information

## 2.1. Team name

NSOC NASK S.A.

## 2.2. Address

NASK S.A., ul. 11 Listopada 23, 03-446 Warsaw

## 2.3. Time zone

Europe/Warsaw (CET/CEST)

2.4. Telephone number

+48 22 380 86 07

2.5. E-mail address

NSOC@nasksa.pl

2.6. Public keys

NASK S.A. holds a PGP key (RSA encryption) with the identifier 02B4FA6103D0F00E and the fingerprint CABCE1A26E00EFF709BEA57802B4FA6103D0F00E.

2.7. Other general information

Information about NSOC NASK S.A., as well as links to various recommended security resources, can be found at: https://www.nasksa.pl/nsoc

2.8. Points of contact

For customers, the preferred method of contacting NSOC NASK S.A. is e-mail sent to NSOC@nasksa.pl ; messages sent to this address will be handled by the appropriate operator. We encourage customers to use PGP encryption when sending any sensitive information to NASK S.A. If it is not possible to use e-mail, NSOC NASK S.A. can be contacted by phone. NSOC NASK S.A. operates 24 hours a day.

3. Charter

3.1. Mission statement

The mission of NSOC NASK S.A. is to identify, analyze, and mitigate threats directed at its customers. As an integral part of the national cybersecurity system, NSOC NASK S.A. contributes to ensuring cybersecurity at the national level.

3.2. Constituency

The constituency of NSOC NASK S.A. includes all users of NASK S.A. ICT systems and networks, including its subsidiaries and other external entities using NASK S.A. network infrastructure and service platforms for which services are provided.

### 3.3. Sponsorship and/or affiliation

NSOC NASK S.A. is financially supported by NASK S.A.

### 3.4. Authority

NSOC NASK S.A. operates under supervision delegated by the management of the Cybersecurity Division of NASK S.A.

## 4. Policies

### 4.1. Types of incidents and level of support

NSOC NASK S.A. is authorized to handle all types of computer and network security incidents that may occur within NASK S.A. (within the scope of services provided). NSOC NASK S.A. prioritizes events based on their severity, scope, and significance.

Incidents are handled according to their priority. The level of support provided by NSOC NASK S.A. may vary depending on the severity and type of the issue, as well as other circumstances relevant to the case.

### 4.2. Cooperation, interaction and disclosure of information

All information provided to NSOC NASK S.A. in connection with the handling of cybersecurity incidents is treated as confidential and used solely for the purpose of identification, analysis, impact mitigation, and prevention of further incidents. Information is processed in accordance with applicable Polish and EU law, including personal data protection regulations, and in line with internal security regulations.

Rules for cooperation and information sharing:

NSOC NASK S.A. cooperates, to the extent necessary to handle an incident, with entities involved in incident handling, in particular: administrators of affected systems, ICT service providers, infrastructure operators, software vendors, and other CSIRT/CERT teams.

Information may be shared with third parties only on a need-to-know basis and only to the minimum extent necessary to identify the source, contain the threat, remediate the impact, or coordinate corrective actions.

Where possible, NSOC NASK S.A. applies information classification to define the permitted audience and conditions for further sharing.

Sensitive data and personal data:

NSOC NASK S.A. minimizes the scope of processed sensitive information (e.g., configurations, logs, samples) and personal data to what is necessary to achieve the purpose of incident handling.

Personal data is not shared with third parties unless there is a clear legal basis for doing so or prior explicit authorization/consent from the customer or the data subject (within the limits permitted by law).

Where it is necessary to transfer sensitive information to external entities, NSOC NASK S.A. limits the scope of data shared and, where appropriate, applies pseudonymization or anonymization.

Disclosure and external communication:

NSOC NASK S.A. does not publish incident information or share it with entities not involved in incident handling unless there is a justified operational need or a required legal basis.

Information may be provided to competent public authorities, supervisory authorities, or law enforcement only to the extent required by applicable law or pursuant to a legally binding request.

Retention and evidentiary integrity:

Incident-handling data and artifacts (e.g., reports, correspondence, logs, indicators) are retained for the period necessary to achieve the purpose of incident handling and in accordance with the internal retention policy and obligations under applicable law.

### 4.3. Communication and authentication

NSOC NASK S.A. is required to comply with laws and rules applicable in Poland and the EU regarding the processing of confidential information.

All e-mail communication should be marked using the TLP 2.0 standard. Low-sensitivity data may be sent via unencrypted e-mail; however, this is not considered secure. PGP encryption is recommended, especially for sensitive data.

## 5. Services

### 5.1. Incident detection and analysis

Determining the authenticity of the incident. Determining the root cause of the incident. Determining the appropriate response. Assessing the severity of the incident.

### 5.2. Risk mitigation and remediation plans

Preparing a post-incident remediation strategy. Preparing recommendations for security improvements for system administrators. Developing procedures for handling various types of cybersecurity incidents.

### 5.3. Incident assessment

Correlating incidents based on collected data. Continuously seeking ways to improve team performance.

### 5.4. Incident prevention

Coordinating responses to threats. Collecting threat intelligence and known indicators of compromise from various sources. Monitoring current technology and security threats. Developing and improving existing security tools and mechanisms to continuously raise the level of security.

### 5.5. Proactive activities

Co-creating notifications about new threats for customers.

Training and other activities (such as simulations of real incidents) aimed at improving the effectiveness of the team and the quality of incident reporting.

Security breaches should be reported via an encrypted e-mail message to: NSOC@nasksa.pl

## 6. Disclaimer

Despite all due care taken in preparing information, notifications, and alerts, NSOC NASK S.A. (as well as NASK S.A.) accepts no liability for errors or omissions, nor for any damages resulting from the use of the information contained therein.