PROCEDURA ZARZĄDZANIA INCYDENTAMI CYBERBEZPIECZEŃSTWA

Egzemplarz zatwierdzony: X **TAK** ☐ **NIE**

Podpis:

STAROSTA
/-/ Sławomir Śmieciuch
……

Spis treści

I. INFORMACJE WSTĘPNE

Procedura zarządzania incydentami cyberbezpieczeństwa, zwana dalej „Procedurą" jest dokumentem wewnętrznym **Starostwa Powiatowego w Lipsku**. Opisuje zasady zarządzania incydentem cyberbezpieczeństwa stosowane przez Starostwo Powiatowe w Lipsku, dalej „Starostwo" w celu spełnienia wymagań wynikających w szczególności z:

1) Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U.UE.L.2016.194.1);
2) art. 22 ust. 1 pkt 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r., poz. 1863 z późn. zm.);
3) § 20 ust. 2 pkt 13 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 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. z 2017 r. poz. 2247).

II. TERMINOLOGIA

1. **CSIRT NASK** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy.
2. **Cyberbezpieczeństwo** – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.
3. **Incydent** – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo.
4. **Incydent cyberbezpieczeństwa** – zbiorcza nazwa obejmująca terminy incydent, incydent w podmiocie publicznym, incydent krytyczny.
5. **Incydent w podmiocie publicznym** – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7–15 Ustawy.
6. **Incydent krytyczny** – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT.
7. **Koordynator KSC** – osoba odpowiedzialna za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, o której mowa w art. 21 ust. 1 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r., poz. 1863 z późn. zm.).
8. **Obsługa incydentu** – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie,

klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu.

9. **Podatność** – właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa.
10. **System informacyjny** – system teleinformatyczny, o którym mowa w art. 3 pkt 3 Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023 r. poz. 57), wraz z przetwarzanymi w nim danymi w postaci elektronicznej.
11. **Użytkownik** – osoba posiadająca dostęp do systemu informacyjnego Starostwa służącego do realizacji zadania publicznego.
12. **Ustawa** – Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r., poz. 1863 z późn. zm.).
13. **Zagrożenie cyberbezpieczeństwa** – potencjalna przyczyna wystąpienia incydentu.
14. **Zarządzanie incydentem** – obsługa incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu.

III. OSOBY ODPOWIEDZIALNE ZA CYBERBEZPIECZEŃSTWO STAROSTWA

1. Starosta Powiatu Lipskiego, ponosząc odpowiedzialność w szczególności za:
   1) wyznaczenie osoby odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa - Koordynatora KSC;
   2) przekazanie do CSIRT NASK w terminie 14 dni od dnia wyznaczenia, danych Koordynatora KSC, a także informacji o zmianie tych danych w terminie 14 dni od dnia ich zmiany.
      Przekazanie danych Koordynatora KSC odbywa się w sposób następujący:
      a) za pośrednictwem formularza elektronicznego pod adres e-mail: ksc@cert.pl,
      lub
      b) w formie pisemnej pod adres do korespondencji CSIRT NASK: NASK - Państwowy Instytut Badawczy, ul. Kolska 12, 01-045 Warszawa.
2. Koordynator KSC, który realizuje następujące zadania:
   1) przyjmuje od Użytkowników informacje o zdarzeniach mogących stanowić incydent cyberbezpieczeństwa lub podejrzenie ich wystąpienia w Starostwie;
   2) koordynuje obsługę zgłaszanych incydentów cyberbezpieczeństwa;
   3) przygotowuje zgłoszenie incydentu w podmiocie publicznym do CSIRT NASK, zgodnie ze wzorem stanowiącym załącznik nr 1 do niniejszej Procedury;
   4) dokonuje zgłoszenia incydentu w podmiocie publicznym do CSIRT NASK. Zgłoszenie incydentu odbywa się za pomocą formularza dostępnego na stronie internetowej https://incydent.cert.pl/;
   5) koordynuje wdrażanie działań naprawczych po wystąpieniu incydentu

cyberbezpieczeństwa;

6) szkoli i podnosi świadomość Użytkowników oraz pozostałych pracowników Starostwa w zakresie incydentów cyberbezpieczeństwa, ich zgłaszania, przeciwdziałania i prewencyjnych sposobach zabezpieczenia przed ich występowaniem;
7) koordynuje prace związane z informowaniem osób, na rzecz których zadanie publiczne jest realizowane w zakresie dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowania skutecznych sposobów zabezpieczania się przed tymi zagrożeniami;
8) w przypadku wystąpienia incydentu cyberbezpieczeństwa ściśle współpracuje z Użytkownikami, pracownikami Starostwa, innymi osobami lub podmiotami świadczącymi Starostwu usługi dotyczące obsługi informatycznej, w celu wdrożenia działań naprawczych;
9) wraz z innymi osobami zaangażowanymi przy wystąpieniu zdarzenia, dokonuje oceny danego zdarzenia pod względem możliwości zakwalifikowania go jako incydentu w odniesieniu do przepisów Ustawy, w tym ewentualnej konieczności dokonania zgłoszenia wystąpienia incydentu w podmiocie publicznym do właściwego CSIRT;
10) prowadzi rejestr incydentów cyberbezpieczeństwa.

IV. PRZYCZYNY WYSTĄPIENIA INCYDENTU

Przyczynę wystąpienia incydentu cyberbezpieczeństwa mogą stanowić:

1) klęski żywiołowe;
2) pożary;
3) zakłócenia w dostawie energii elektrycznej;
4) błędy w oprogramowaniu;
5) awaria sprzętu;
6) błędy użytkowników, których wystąpienie może spowodować zniszczenie lub uszkodzenie infrastruktury informatycznej oraz zakłócenie ciągłości pracy systemów informacyjnych;
7) niewłaściwe wykorzystywanie zasobów informatycznych;
8) działanie szkodliwego oprogramowania;
9) próby omijania systemów zabezpieczeń;
10) nieautoryzowany dostęp do systemów informacyjnych i aplikacji;
11) zniszczenia lub kradzież urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
12) zniszczenia lub kradzież nośników danych;
13) próby wyłudzeń informacji;
14) ataki socjotechniczne.

V. ZGŁASZANIE ZDARZEŃ PRZEZ UŻYTKOWNIKÓW ORAZ OBSŁUGA INCYDENTU CYBERBEZPIECZEŃSTWA

1. Każdy Użytkownik i/lub pracownik Starostwa, który zaobserwuje zdarzenie mogące stanowić incydent cyberbezpieczeństwa lub podejrzewa, iż wystąpił incydent cyberbezpieczeństwa w Starostwie - w tym, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez Starostwo – zobowiązany jest poinformować o w/w okolicznościach Koordynatora KSC.
2. Poinformowanie Koordynatora KSC, o którym mowa w ust. 1, winno nastąpić niezwłocznie, jednak nie później niż w terminie 2 godzin od wystąpienia zdarzenia lub podejrzenia jego wystąpienia oraz winno być potwierdzone w formie pisemnej za pośrednictwem poczty elektronicznej e-mail.
3. W przypadku nieobecności w pracy Koordynatora KSC informacje, o których mowa w ust. 1 należy przekazać do osoby wyznaczonej w zastępstwie do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Odpowiednio mają zastosowanie postanowienia ust. 2.
4. Koordynator KSC lub osoba, o której mowa w ust. 3 we współpracy z Koordynatorem KSC dokonuje wstępnej weryfikacji otrzymanych informacji pod względem przesłanek identyfikujących zaistnienie incydentu cyberbezpieczeństwa, w tym czy stanowi on incydent w podmiocie publicznym podlegający zgłoszeniu do CSIRT NASK.
5. Przy ocenie istoty zdarzenia, o którym mowa w pkt 1, uwzględnia się następujące czynniki:
   1) wpływ zdarzenia na działanie systemów informacyjnych;
   2) wpływ zdarzenia na ciągłość realizacji zadań publicznych z wykorzystaniem systemów informacyjnych;
   3) wpływ zdarzenia na dostępność, integralność, poufność oraz autentyczność danych wykorzystywanych do realizacji zadań publicznych.
6. Koordynator KSC wspólnie z osobami zaangażowanymi w zarządzanie i obsługę incydentu cyberbezpieczeństwa weryfikują zgromadzone o zdarzeniu informacje, w tym w szczególności informacje:
   1) opisujące wpływ incydentu w podmiocie publicznym na realizowane zadanie publiczne, w tym:
      a) wskazanie zadania publicznego, na które incydent cyberbezpieczeństwa miał wpływ,
      b) liczbę osób, na które incydent miał wpływ,
      c) moment wystąpienia i wykrycia incydentu cyberbezpieczeństwa oraz czas jego trwania,
      d) zasięg geograficzny obszaru, którego dotyczy incydent,
      e) przyczynę zaistnienia incydentu i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne podmiotu publicznego;
   2) informacje o przyczynie i źródle incydentu;
   3) informacje o podjętych działaniach zapobiegawczych.

7. Na podstawie informacji, o których mowa w ust. 6 dokonywana jest ostateczna ocena incydentu cyberbezpieczeństwa pod względem przesłanek stanowiących o zaistnieniu incydentu w podmiocie publicznym podlegającemu zgłoszeniu do CSIRT NASK.
8. Ustalenia dotyczące incydentu cyberbezpieczeństwa winny zostać odnotowane w dokumencie „Raport incydentu cyberbezpieczeństwa", stanowiącym załącznik nr 1 do niniejszej Procedury.
9. Po sporządzeniu Raportu incydentu cyberbezpieczeństwa – w przypadku gdy zdarzenie zakwalifikowano jako incydent w podmiocie publicznym – Starostwo zobowiązane jest do dokonania zgłoszenia do właściwego CSIRT.
10. Incydent cyberbezpieczeństwa, każdorazowo należy odnotować w „Rejestrze incydentów cyberbezpieczeństwa", stanowiącym załącznik nr 2 do niniejszej Procedury.
11. Koordynator KSC niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia zdarzenia, dokonuje zgłoszenia incydentu w podmiocie publicznym do CSIRT NASK zgodnie z dyspozycją przepisu art. 23 Ustawy.
12. Dokonując zgłoszenia incydentu w podmiocie publicznym zgodnie z ust. 11, dla wiadomości CSIRT NASK należy uwzględnić oznaczenie wszystkich informacji prawnie chronionych, w tym stanowiących tajemnicę przedsiębiorstwa jeśli takie informacje są zostaną zawarte w zgłoszeniu.
13. Po dokonaniu zgłoszenia o incydencie do CSIRT NASK, Koordynator KSC gromadzi dodatkowe informacje o incydencie cyberbezpieczeństwa na podstawie analizy systemów monitorujących, systemów zabezpieczeń, urządzeń sieciowych, logów oraz baz wiedzy (szczególnie z uwzględnieniem przesłanek i powiązań z wcześniejszymi analogicznymi zdarzeniami lub incydentami cyberbezpieczeństwa, o ile takie występowały).
14. W przypadku powzięcia nowych informacji dotyczących obsługiwanego incydentu cyberbezpieczeństwa, Koordynator KSC informuje o tych okolicznościach CSIRT NASK, uzupełniając wcześniejsze zgłoszenie. Sposób informowana na zasadach określonych w ust. 11.
15. Koordynator KSC wdraża działania naprawcze i zabezpieczające mające na celu ograniczenie skutków incydentu cyberbezpieczeństwa, w szczególności incydentu w podmiocie publicznym, polegające w szczególności na:
    1) przywróceniu pełnej funkcjonalności systemu informacyjnego;
    2) zapewnienie bezpieczeństwa dla systemu informacyjnego np. zmiana haseł, wzmacnianie bezpieczeństwa instalacji i ustawień systemów (hardening), włączanie innych, wymaganych zabezpieczeń (na przykład zabezpieczeń firewall, dodatkowej kontroli dostępu, zmiany reguł w systemach IPS itp.);
    3) usunięcie z systemów śladów incydentów cyberbezpieczeństwa (min. poprzez usunięcie szkodliwego oprogramowania, odblokowanie kont użytkowników zablokowanych wskutek wystąpienia incydentu itp.);
    4) przeglądu, aktualizacji lub wdrożenia planów ciągłości działania, wpływających na realizację zadania publicznego;

5) przeglądu oraz aktualizacji procedur i/lub polityk związanych z bezpieczeństwem informacji oraz danych osobowych;
6) analizie incydentów cyberbezpieczeństwa, które wystąpiły w Starostwie lub jednostkach o podobnym profilu działania;
7) po zakończeniu obsługi incydentu cyberbezpieczeństwa, w terminie nieprzekraczającym 21 dni od zakończenia obsługi incydentu, Koordynator KSC przeprowadza szkolenie dla wszystkich Użytkowników;
8) w przypadku gdy do incydentu doszło z winy umyślnej Użytkownika, przechodzi on szkolenie indywidualne z zakresu cyberbezpieczeństwa zakończone testem wiedzy.

16. W celu potwierdzenia skuteczności przeprowadzonych w Starostwie działań naprawczych i zapobiegawczych incydentom cyberbezpieczeństwa, mogą zostać przeprowadzone dodatkowe działania weryfikacyjne do których należą: przeprowadzenie testów podatności systemu IT, jeżeli incydent spowodowany został podatnością tego systemu lub inne czynności analityczne i sprawdzające.

VI. NARUSZENIE DANYCH OSOBOWYCH W ZWIĄZKU Z INCYDENTEM

W przypadku, gdy incydent w podmiocie publicznym spowoduje naruszenie ochrony danych osobowych wówczas należy postępować zgodnie z art. 33-34 Rozporządzenia 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 - RODO) (Dz. Urz. UE L 119 z dnia 05 kwietnia 2016 r.) oraz z wewnętrzną procedurą stanowiącą art. 23 Polityki Ochrony Danych Osobowych - Naruszenia ochrony danych osobowych - instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych.

VII. SZKOLENIA

1. Każdy Użytkownik i pracownik Starostwa winien zostać przeszkolony z zakresu Ustawy oraz informacji o zagrożeniach cyberbezpieczeństwa.
2. Koordynator KSC z własnej inicjatywy lub na wniosek Starosty Powiatu Lipskiego przeprowadza wewnętrzne szkolenia, o których mowa w ust. 1.
3. Dodatkowo szkolenia winny zostać przeprowadzane w przypadku każdej istotnej zmiany zasad lub przepisów dotyczących Ustawy w zakresie odnoszącym się do podmiotu publicznego. Przepis ust. 2 stosuje się odpowiednio.
4. W przypadku zaistnienia incydentu cyberbezpieczeństwa - po zakończeniu obsługi tego incydentu - Koordynator KSC winien przeprowadzić w terminie 21 dni od zakończenia obsługi incydentu szkolenie dla pracowników Starostwa, mające na celu przekazanie informacji o zaistniałym incydencie cyberbezpieczeństwa i prewencyjnych sposobach zabezpieczenia

Starostwa przed podobnymi incydentami.

5. Każde szkolenie wewnętrzne powinno być udokumentowane poprzez sporządzenie dokumentów potwierdzających uczestnictwo w takim szkoleniu przez jego uczestników (lista obecności lub zaświadczenie/certyfikat imienny dla osoby uczestniczącej w szkoleniu).

VIII. DYSTRYBUCJA ORAZ AKTUALIZACJA PROCEDURY

1. Niniejsza Procedura podlega regularnym (nie rzadziej niż raz na rok) przeglądom dokonywanym przez Koordynatora KSC.
2. W zależności od potrzeb mogą zostać przeprowadzone także dodatkowe przeglądy po stwierdzeniu istotnego naruszenia bezpieczeństwa, pojawieniu się zasadniczych zmian w Starostwie, jego strukturze lub jego otoczeniu (nowe zagrożenia, technologie).
3. Każdy Użytkownik, który wykorzystuje system informacyjny do realizacji zadań publicznych pozostających w jego zakresie obowiązków, jest zobowiązany do zapoznania się z obowiązkami związanymi z przepisami wynikającymi z Ustawy.
4. Starosta Powiatu Lipskiego zapewnia dostęp do niniejszej Procedury każdemu Użytkownikowi i pracownikowi Starostwa.
5. Każdy Użytkownik oraz pracownik Starostwa zobowiązany jest zapoznać się z niniejszą Procedurą potwierdzając tę okoliczność własnoręcznym podpisem w dokumencie „Wykaz osób zapoznanych z Procedurą zarządzania incydentami cyberbezpieczeństwa”, stanowiącym załącznik nr 3 do niniejszej Procedury.

IX. WYKAZ ZAŁĄCZNIKÓW

Załącznik nr 1 – Wzór raportu incydentu cyberbezpieczeństwa.
Załącznik nr 2 – Rejestr incydentów cyberbezpieczeństwa.
Załącznik nr 3 – Wykaz osób zapoznanych z Procedurą zarządzania incydentami cyberbezpieczeństwa.