Zarządzenie nr 243/2024
REKTORA
Państwowej Akademii Nauk Stosowanych
im. ks. Bronisława Markiewicza
w Jarosławiu
z dnia 24 października 2024 r.

w sprawie Polityki zarządzania incydentami w zakresie cyberbezpieczeństwa w PANS w Jarosławiu

Na podstawie art. 23 ust. 1 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz.U. z 2023 r. poz. 742 z późn. zm.) zarządzam, co następuje:

§1

Wprowadza się Politykę zarządzania indcydentami w zakresie cyberbezpieczeństwa w PANS w Jarosławiu stanowiącą załącznik do zarządzenia.

§2

Wszyscy pracownicy oraz osoby współpracujące z PANS w Jarosławiu zobowiązani są do zapoznania się z postanowieniami polityki, o której mowa w §1 oraz ich stosowania.

§3

Zarządzenie wchodzi w życie z dniem podpisania.

Rektor
PANS w Jarosławiu
dr Beata Rejman

Sporządził
KANCLERZ
.....
Mariusz Dudek

Zatwierdzam pod względem formalno-prawnym
.....
Adam Rymkiewicz
Nr rej. Rz/P/47

Zatwierdzam pod względem merytorycznym
KANCLERZ
.....
Mariusz Dudek

+48 16 624 46 20
uczelnia@pansjar.edu.pl
Państwowa Akademia Nauk Stosowanych
im. ks. Bronisława Markiewicza w Jarosławiu
ul. Czarnieckiego 16
37-500 Jarosław

załącznik do Zarządzenia nr 242/2024
Rektora PANS w Jarosławiu
z dnia 24.10.2024 r.

Polityka zarządzania incydentami w zakresie cyberbezpieczeństwa w PANS w Jarosławiu

§1

1. Polityka określa zasady zarządzania incydentami bezpieczeństwa informacji w zakresie cyberbezpieczeństwa w celu zaplanowania i przygotowania Państwowej Akademii Nauk Stosowanych im. ks. Bronisława Markiewicza w Jarosławiu zwanej dalej „PANS" do zarządzania incydentami bezpieczeństwa, aby zminimalizować ich wpływ na działalność, zapewnić szybkie i skuteczne reagowanie, wyjaśnianie przyczyn powstania incydentu oraz zapobieganie wystąpieniu przyszłych incydentów. Polityka ustanawia standardy i zasady dotyczące zarządzania incydentami związanymi z bezpieczeństwem informacji w zakresie cyberbezpieczeństwa.
2. Polityka obejmuje wszystkie obszary działalności PANS, w których przetwarzane są informacje oraz dotyczy wszystkich pracowników, studentów, kontrahentów i osób trzecich mających dostęp do zasobów informacyjnych PANS.

§2

Użyte w Polityce określenia oznaczają:

1) zdarzenie bezpieczeństwa - wszystkie nieplanowane zdarzenia w systemie informatycznym, sieci, zasobach informacyjnych lub środowisku operacyjnym, które mają potencjalny wpływ na bezpieczeństwo informacji. Zdarzenia bezpieczeństwa mogą być wynikiem działań ludzkich, awarii systemu, błędów w konfiguracji, naturalnych katastrof, błędów użytkowników, ataków złośliwego oprogramowania, czy innych niezamierzonych zdarzeń, które mogą, ale nie muszą prowadzić do naruszenia bezpieczeństwa informacji;
2) incydent bezpieczeństwa to każde zdarzenie lub seria zdarzeń związanych z bezpieczeństwem informacji, które ma lub mogłoby mieć niekorzystny wpływ na cyberbezpieczeństwo, np. skutkuje lub może skutkować nieautoryzowanym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub utratą informacji. Incydenty bezpieczeństwa mogą mieć bezpośredni wpływ na poufność, integralność, dostępność i autentyczność informacji oraz na ciągłość działania PANS w Jarosławiu;
3) CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;
4) lider zespołu – osoba odpowiedzialna za zarządzanie zespołem ds. reagowania na incydenty, koordynację działań związanych z incydentami (w tym wyznaczanie priorytetów i rozdzielanie zadań, zapewnienie komunikacji z władzami PANS, koordynację raportowania wyników i analizy po incydencie) oraz podejmowanie decyzji operacyjnych, który jest również odpowiedzialny za wdrożenie niniejszej polityki;
5) specjalista ds. incydentów – osoba odpowiedzialna za odbieranie zgłoszeń o zdarzeniach dotyczących bezpieczeństwa informacji, reagowanie na zgłaszane zdarzenia i incydenty bezpieczeństwa, w tym ich identyfikowanie i wstępną analizę, współpracę z ekspertami technicznymi w zakresie dalszej analizy incydentów, podejmowanie działań naprawczych w celu zminimalizowania wpływu zdarzeń na działalność PANS oraz dalszych działań zapobiegawczych, zgłaszanie incydentów bezpieczeństwa do CSIRT NASK, dokumentowanie zdarzeń i działań podjętych w odpowiedzi na zgłoszenia, wyszukiwanie i dostarczanie informacji o nowych technikach ataków i zaleceniach bezpieczeństwa oraz za przeglądy i aktualizacje niniejszej polityki;
6) eksperci techniczni – osoby odpowiedzialne za codzienne monitorowanie systemów i analizowanie danych dotyczących zagrożeń, wykrywanie anomalii i podejrzanych działań w systemach IT, diagnozowanie i naprawę luk w zabezpieczeniach infrastruktury, współpracę w ramach zespołu w zakresie analizy incydentów, wykonywanie natychmiastowych działań obronnych w przypadku wystąpienia incydentu, podejmowanie działań naprawczych oraz zapobiegawczych, rekomendowanie i implementację technicznych rozwiązań zabezpieczających, odbieranie zgłoszeń o zdarzeniach dotyczących bezpieczeństwa informacji podczas nieobecności specjalisty ds. incydentów, zgłaszanie incydentów bezpieczeństwa do CSIRT NASK podczas nieobecności specjalisty ds. incydentów;

7) specjalista ds. zgodności – osoba odpowiedzialna za zapewnienie przestrzegania przepisów prawnych i regulacji związanych z cyberbezpieczeństwem oraz bezpieczeństwem danych osobowych oraz monitorowanie zgodności działań reagowania z przepisami prawa, każdorazowo IOD.

§3

1. Rektor PANS w Jarosławiu powołuje w drodze zarządzenia zespół ds. reagowania na incydenty, odpowiedzialny za koordynację działań związanych z incydentami bezpieczeństwa.
2. W skład zespołu ds. reagowania na incydenty wchodzą:
   1) lider zespołu;
   2) specjalista ds. incydentów;
   3) specjalista ds. zgodności – Inspektor Ochrony Danych;
   4) eksperci techniczni.
3. Zespół ds. reagowania na incydenty wymaga przeszkolenia w zakresie najnowszych technik i metod zarządzania incydentami.
4. Wszyscy pracownicy są zobowiązani do niezwłocznego zgłaszania wszelkich zdarzeń i incydentów bezpieczeństwa zgodnie z niniejszą polityką oraz współpracy z zespołem ds. reagowania na incydenty podczas analizy i rozwiązywania incydentów, w tym w zakresie ustalenia stanu faktycznego, źródła i przebiegu incydentu, gromadzenia dowodów, oceny wpływu incydentu na działalność PANS w Jarosławiu.
5. Wszystkie jednostki organizacyjne PANS w Jarosławiu są zobowiązane do pełnej współpracy z zespołem ds. reagowania na incydenty w zakresie obsługi zidentyfikowanych incydentów.

§4

1. Zdarzenia oraz incydenty bezpieczeństwa informacji w PANS w Jarosławiu są systematycznie identyfikowane i klasyfikowane oraz zarządzane zgodnie z niniejszą procedurą.
2. Zdarzenia i incydenty bezpieczeństwa są identyfikowane i zgłaszane przez systemy monitorujące Uczelni, pracowników lub zewnętrzne źródła.
3. Wszystkie systemy informatyczne i zasoby sieciowe powinny być monitorowane w miarę możliwości w sposób ciągły, w celu wykrywania zdarzeń i incydentów bezpieczeństwa informacji.
4. Monitorowanie, o którym mowa w ust. 3 obejmuje:
   1) serwery i stacje robocze,
   2) sieci i urządzenia sieciowe,
   3) aplikacje i bazy danych,
   4) urządzenia mobilne i zdalny dostęp.
5. Narzędzia do automatycznego monitorowania i wykrywania zdarzeń bezpieczeństwa wdrażane są w PANS na podstawie wyników szacowania i oceny ryzyka bezpieczeństwa informacji.
6. Każdy pracownik PANS w Jarosławiu, który powziął informacje o wystąpieniu zdarzenia dotyczącego bezpieczeństwa informacji lub je spowodował, jest zobowiązany niezwłocznie je zgłosić.
7. Zdarzenia, o których mowa w ust. 6 obejmują w szczególności:
   1) nietypowe zachowanie systemów informatycznych,
   2) fizyczne naruszenia bezpieczeństwa,
   3) utratę danych lub urządzeń zawierających dane firmowe,
   4) przypadkowe ujawnienie danych wrażliwych osobom nieuprawnionym,
   5) otrzymanie podejrzanych wiadomości e-mail lub załączników,
   6) naruszenia procedur bezpieczeństwa.
8. Zgłoszenia, o którym mowa w ust. 6 można dokonać w następujący sposób:
   1) wysłanie wiadomości e-mail na dedykowany adres e-mail przeznaczony do zgłaszania zdarzeń bezpieczeństwa (incydent@pansjar.edu.pl);
   2) zgłoszenie zdarzenia osobiście do specjalisty ds. incydentów;

3) zgłoszenie zdarzenia telefonicznie do specjalisty ds. incydentów.

9. Podczas zgłoszenia zdarzenia, pracownicy powinni podać następujące informacje:
   1) imię i nazwisko zgłaszającego,
   2) opis zdarzenia,
   3) data i godzina wystąpienia zdarzenia,
   4) lokalizację (jeśli dotyczy),
   5) wszelkie inne istotne informacje (takie jak załączniki, zrzuty ekranu).
10. Wszystkie zgłoszenia zdarzeń bezpieczeństwa są traktowane jako poufne.
11. Ze zgłoszenia dokonanego w sposób określony w ust. 8 pkt. 2 i 3 osoba przyjmująca zgłoszenie sporządza pisemną notatkę służbową zawierającą informacje określone w ust. 9.
12. Pracownicy zgłaszający zdarzenia nie mogą podlegać żadnym sankcjom ani represjom związanym z faktem dokonania zgłoszenia.

§5

1. Po otrzymaniu informacji o wystąpieniu zdarzenia dotyczącego bezpieczeństwa informacji, zespół ds. reagowania na incydenty przeprowadza wstępną ocenę zdarzenia w celu określenia jego potencjalnego wpływu na bezpieczeństwo informacji PANS oraz dokonania klasyfikacji zdarzenia jako incydentu lub nie.
2. Analiza, o której mowa w ust. 1 powinna obejmować:
   1) rodzaj zdarzenia;
   2) przyczynę zdarzenia;
   3) zakres i potencjalne skutki.
3. Zdarzenia kwalifikowane jako incydenty bezpieczeństwa mogą obejmować w szczególności:
   1) zdarzenia losowe, w tym pożar, zalanie, które uniemożliwiają prowadzenie przez PANS działalności;
   2) awarie zasilania urządzeń powodujące brak możliwości korzystania z kluczowych elementów infrastruktury IT;
   3) błędy i wady istotnego oprogramowania lub sprzętu, uniemożliwiające korzystanie z niego lub powodujące powstanie podatności znacząco obniżających poziom bezpieczeństwa informacji,
   4) instalację na służbowym sprzęcie oprogramowania niedopuszczonego do użytkowania w PANS w Jarosławiu;
   5) naruszenia poufności, integralności, dostępności lub autentyczności danych osobowych;
   6) próby nieautoryzowanego dostępu;
   7) naruszenia procedur bezpieczeństwa;
   8) wykrycie lub podejrzenie zainstalowania złośliwego oprogramowania, np. typu malware i ransomware;
   9) włamanie do sieci;
   10) phishing.

§6

1. Zespół ds. reagowania na incydenty kwalifikuje zdarzenia zidentyfikowane jako incydenty bezpieczeństwa według rodzaju zagrożenia i potencjalnego wpływu na działalność PANS w Jarosławiu. Do klasyfikacji przyjmuje się kryterium typu, źródła, obszaru wpływu oraz krytyczności.
2. Do klasyfikacji, o której mowa w ust. 1 przyjmuje się następujące kryteria:
   1) typ incydentu bezpieczeństwa w odniesieniu do cech informacji:
      a) poufność: incydenty związane z nieautoryzowanym ujawnieniem lub dostępem do informacji, np. nieautoryzowany dostęp do danych, ujawnienie danych osobowych lub poufnych,
      b) integralność: incydenty związane z nieautoryzowaną modyfikacją lub usunięciem informacji, np. nieautoryzowane modyfikacje danych, usunięcie danych bez odpowiednich uprawnień, zniszczenie danych,

c) dostępność: incydenty związane z niedostępnością informacji lub systemów informatycznych, np. ataki DDoS, awarie systemów informatycznych,
d) autentyczność: incydenty związane z naruszeniem wiarygodności informacji, np. nieautoryzowana zmiana lub manipulacja tożsamością, fałszywe certyfikaty,
e) zgodność: incydenty związane z naruszeniem procedur bezpieczeństwa lub regulacji prawnych dotyczących bezpieczeństwa informacji np. naruszenia przepisów RODO, wewnętrznych regulacji dotyczących bezpieczeństwa informacji;

2) typ incydentu ze względu na źródło:
a) wewnętrzne: incydenty spowodowane przez pracowników PANS, studentów lub wewnętrzne systemy informatyczne,
b) zewnętrzne: incydenty spowodowane przez zewnętrzne podmioty, takie jak hakerzy, dostawcy lub partnerzy biznesowi;

3) Typ incydentu ze względu na obszary wpływu na działalność PANS w Jarosławiu:
a) finansowy: incydenty wpływające na finanse PANS,
b) prawny: incydenty wpływające na zgodność z regulacjami prawnymi,
c) reputacyjny: incydenty wpływające na reputację PANS,
d) operacyjny: incydenty wpływające na operacje biznesowe PANS;

4) typ incydentu ze względu na krytyczność incydentu bezpieczeństwa według pięciostopniowej skali:
a) krytyczny: incydenty, które mają natychmiastowy i poważny wpływ na działalność PANS, mogą prowadzić do znacznych strat finansowych, prawnych lub reputacyjnych ~~Zaliczamy do nich incydenty typu:~~ takie jak: utrata krytycznych danych, wycieki wrażliwych danych osobowych, poważne naruszenia systemów bezpieczeństwa, znaczące ataki ransomware lub malware, incydenty z dużym wpływem finansowym lub prawnym,
b) poważny: incydenty, które mają znaczący wpływ na działalność PANS (np. poważne obniżenie jakości lub przerwanie ciągłości działania) i mogą prowadzić do strat finansowych, prawnych lub reputacyjnych ~~Są to incydenty typu:~~ takie jak: naruszenie danych osobowych, znaczące próby nieautoryzowanego dostępu, ataki typu DDoS, ujawnienie poufnych informacji,
c) średni: incydenty, które mają umiarkowany wpływ na działalność PANS w Jarosławiu, np. mniejsze naruszenia procedur bezpieczeństwa, utrata dostępności mniej krytycznych systemów, incydenty z umiarkowanym wpływem operacyjnym,
d) niski: incydenty, które mają niewielki wpływ na działalność PANS, np. drobne naruszenia procedur bezpieczeństwa, problemy z dostępem do mniej istotnych systemów, incydenty bez znaczącego wpływu na działalność.

3. Na podstawie dokonanej klasyfikacji incydentów bezpieczeństwa informacji zespół reagowania na incydenty dokonuje priorytetyzacji podejmowanych działań mającą na celu skuteczne reagowanie oraz minimalizowanie wpływu incydentów na działalność PANS w Jarosławiu.
4. Incydentom bezpieczeństwa nadawane są następujące priorytety, w zależności od skali oraz skutków incydentu:
1) wysoki: incydenty wymagające natychmiastowego lub pilnego działania;
2) średni: incydenty wymagające działań w określonym czasie;
3) niski: incydenty, które mogą zostać rozwiązane rutynowymi działaniami.
5. Na podstawie klasyfikacji i priorytetyzacji incydentu bezpieczeństwa, zespół ds. reagowania na incydenty podejmuje odpowiednie działania naprawcze, które mają na celu:
1) zminimalizowanie strat i doraźne usunięcie skutków incydentu;
2) ocenę stanu bezpieczeństwa i usunięcie podatności bądź minimalizacja ryzyka związanego z zagrożeniem;
3) zebranie i zabezpieczenie materiału dowodowego na potrzeby dalszej analizy lub działań prawnych;
4) wyciągnięcie konsekwencji wobec sprawcy incydentu.

6. W przypadku gdy sprawcą incydentu bezpieczeństwa jest pracownik, w zależności od wagi zagrożenia dla systemu informacyjnego wynikającego z naruszenia jego bezpieczeństwa, PANS w Jarosławiu może wszcząć postępowanie dyscyplinarne, zgodnie z wewnętrznymi regulacjami.
7. W przypadku, gdy incydent bezpieczeństwa mógł spowodować zagrożenie dla dostępności lub integralności informacji przechowywanych w systemie informacyjnym PANS, przeprowadzana jest procedura odtwarzania z kopii zapasowych zgodnie z obowiązującymi procedurami.

§7

1. Zespół ds. reagowania na incydenty dokonuje analizy każdego incydentu bezpieczeństwa w celu identyfikacji luk, jak również wzorców i trendów, aby na tej podstawie podejmować kroki zmierzające do zapobiegania wystąpienia podobnych zdarzeń w przyszłości. Wnioski z dokonywanej analizy są wykorzystywane do wdrożenia działań korygujących oraz doskonalenia procedur i instrukcji bezpieczeństwa.
2. Zespół ds. reagowania na incydenty tworzy szczegółowe plany reagowania na incydenty poszczególnych rodzajów.
3. Po rozwiązaniu incydentu bezpieczeństwa następuje jego formalne zamknięcie.

§8

1. Informacje o incydentach bezpieczeństwa są traktowane jako poufne. Informacje udostępnia się wyłącznie osobom, dla których są one niezbędne w celu wykonania swoich obowiązków służbowych.
2. Każda osoba uczestnicząca w procesie związanym z obsługą incydentów jest odpowiedzialna za ochronę informacji dotyczącej zdarzeń oraz incydentów bezpieczeństwa.
3. W uzasadnionych przypadkach, PANS w Jarosławiu informuje pracowników, studentów, osoby trzecie lub inne organizacje o wystąpieniu incydentu i/lub o wszelkich istotnych i niezbędnych szczegółach.
4. Informacje o incydentach bezpieczeństwa są przekazywane podmiotom uprawnionym zgodnie z obowiązującymi przepisami.

§9

1. PANS w Jarosławiu dokonuje formalnego zgłoszenia incydentu bezpieczeństwa sklasyfikowanego jako incydent krytyczny lub poważny do CSIRT NASK.
2. Zgłoszenie dokonywane jest nie później niż w ciągu 24 godzin od jego wykrycia.
3. Zgłoszenie dokonywane jest w formie elektronicznej, zgodnie z formularzem dostępnym na stronie CSIRT NASK: www.incydent.cert.pl.
4. W przypadku, gdy incydent bezpieczeństwa dotyczy danych osobowych, wszelkie dodatkowe zgłoszenia dokonywane są zgodnie z funkcjonującą w PANS w Jarosławiu polityką ochrony danych osobowych.

§10

1. Specjalista ds. zgodności – Inspektor Ochrony Danych PANS w Jarosławiu prowadzi rejestr wykrytych incydentów (załącznik nr 1).
2. Dokumentacja incydentów jest tworzona i przechowywana w bezpieczny sposób w systemie EOD przez okres wskazany w przepisach obowiązujących. ustalony zgodnie z wymogami prawnymi.

§11

1. PANS w Jarosławiu przeprowadza regularne, co najmniej raz w roku, testy w zakresie monitorowania i wykrywania zdarzeń bezpieczeństwa oraz realizacji planów reagowania na

incydenty. Testy powinny obejmować symulacje incydentów oraz sprawdzanie skuteczności narzędzi monitorujących.

2. Polityka zarządzania incydentami powinna być regularnie przeglądana i aktualizowana na podstawie wyników testów, zmian w infrastrukturze IT oraz doświadczeń z rzeczywistych incydentów, w celu dostosowania do zmieniających się zagrożeń.

ZAŁĄCZNIKI

Załącznik nr 1 Wzór rejestru incydentów

IDENTYFIKACJA I OCENA					
L.p.	**Data i godzina wykrycia**	**Rodzaj incydentu**	**Opis zdarzenia**	**Przyczyna incydentu**	**Zakres i potencjalne skutki**

KLASYFIKACJA INCYDENTÓW				REAGOWANIE		
Typ incydentu (poufność, integralność, dostępność, autentyczność, zgodność)	**Źródło incydentu**	**Obszar wpływu** (finansowy, prawny, reputacyjny, operacyjny)	**Krytyczność incydentu**	**Priorytet**	**Działania naprawcze**	**Odpowiedzialny zespół/osoba**

ANALIZA PO INCYDENCIE					
Data rozwiązania	**Czas reakcji**	**Czas rozwiązania**	**Wpływ na działalność**	**Działania zapobiegawcze**	**Uwagi / wnioski**