Procedura zarządzania incydentami bezpieczeństwa informacji

1. Cel dokumentu

Celem niniejszej procedury jest określenie zasad i trybu postępowania w przypadku wystąpienia incydentów bezpieczeństwa informacji w Instytucie. Procedura ma na celu zapewnienie szybkiego i skutecznego reagowania, ograniczenia skutków incydentów oraz spełnienie wymogów przepisów prawa, takich jak RODO, KRI czy ISO/IEC 27001.

2. Definicje

Incydent bezpieczeństwa informacji – każde zdarzenie, które może skutkować naruszeniem poufności, integralności lub dostępności informacji.

Zgłaszający – osoba, która zauważyła lub podejrzewa incydent.

Koordynator ds. incydentów – osoba odpowiedzialna za przyjęcie zgłoszenia, jego rejestrację i koordynację dalszych działań.

3. Zakres stosowania

Procedura dotyczy wszystkich pracowników, współpracowników oraz innych osób mających dostęp do zasobów informacyjnych Instytutu. Obejmuje wszystkie systemy informatyczne, dane oraz procesy przetwarzania informacji w ramach działalności Instytutu.

4. Proces obsługi incydentów

4.1. Zgłoszenie incydentu

Każdy pracownik Instytutu zobowiązany jest do niezwłocznego zgłoszenia zauważonego lub podejrzewanego incydentu bezpieczeństwa informacji do Koordynatora ds. incydentów lub bezpośredniego przełożonego. Zgłoszenie może być dokonane ustnie, mailowo lub poprzez dedykowany formularz (załącznik nr 1).

4.2. Rejestracja i klasyfikacja

Koordynator ds. incydentów rejestruje zgłoszenie w Rejestrze incydentów oraz dokonuje jego wstępnej klasyfikacji pod względem rodzaju i potencjalnych skutków.

4.3. Ocena skutków i ryzyka

Dokonywana jest ocena wpływu incydentu na działalność Instytutu oraz na dane osobowe. W przypadku naruszenia ochrony danych osobowych, rozważane jest zgłoszenie incydentu do Prezesa UODO w ciągu 72 godzin od jego wykrycia.

Sporządził: J. Maciejski, dnia 12-12-2024

4.4. Reakcja i usuwanie skutków

Zespół techniczny lub inne wyznaczone osoby podejmują działania mające na celu usunięcie skutków incydentu oraz zapobieżenie jego ponownemu wystąpieniu.

4.5. Dokumentacja i analiza

Po zakończeniu działań sporządzany jest raport z incydentu zawierający opis zdarzenia, działania naprawcze oraz zalecenia na przyszłość.

5. Role i odpowiedzialności

5.1. Pracownik – obowiązek zgłoszenia incydentu.
5.2. Koordynator ds. incydentów – rejestracja, klasyfikacja, prowadzenie dokumentacji.
5.3. Kierownictwo Instytutu – podejmowanie decyzji strategicznych, zatwierdzanie działań naprawczych.

6. Rejestr incydentów

Rejestr incydentów prowadzony jest przez Koordynatora ds. incydentów i zawiera co najmniej: numer incydentu, datę zgłoszenia, opis zdarzenia, klasyfikację, podjęte działania, status oraz informacje o ewentualnym zgłoszeniu do UODO.

7. Przegląd procedury

Procedura podlega corocznemu przeglądowi oraz każdorazowej aktualizacji po zaistnieniu incydentu wymagającego modyfikacji zasad reagowania.

Sporządził: J. Maciejski, dnia 12-12-2024

DYREKTOR
Prof. dr hab. Mariusz K. Piskuła
czł. koresp. PAN

FORMULARZ ZGŁASZANIA INCYDENTÓW BEZPIECZEŃSTWA INFORMACJI

CZĘŚĆ A: DANE DZIAŁU/ZESPOŁU	
1. Pełna nazwa jednostki organizacyjnej, w której wystąpił incydent	
2. Miejsce Pracy zgłaszającego	
3. Kierownik lub przełożony zgłaszającego	
CZĘŚĆ 2: DANE OSOBY ZGŁASZAJĄCEJ Z JEDNOSTKI ORGANIZACYJNEJ (uzupełnia osoba zgłaszająca z jednostki organizacyjnej, w której wystąpił incydent)	
6. Imię i nazwisko osoby z jednostki organizacyjnej, zgłaszającej incydent	Dane pracownika
7. Stanowisko służbowe osoby z jednostki organizacyjnej, zgłaszającej incydent *	
8. Numer telefonu służbowego osoby z jednostki organizacyjnej, zgłaszającej incydent *	
9. Adres poczty elektronicznej osoby z jednostki organizacyjnej, zgłaszającej incydent *	
CZĘŚĆ 3: OPIS INCYDENTU (uzupełnia osoba zgłaszająca z jednostki organizacyjnej, w której wystąpił incydent)	
13. Data wystąpienia incydentu * orientacyjny czas trwania incydent	Data: godzina: - Podany czas jest: • dokładny • przybliżony
14. Data wykrycia incydentu * oraz stan incydentu incydent nadal trwa/wygasł/został obsłużony	• nadal trwa • wygasł • został obsłużony
15. Zadanie, na które incydent miał wpływ *	
16. Liczba osób, na które incydent miał wpływ *	• 1 – 50 • 51 – 500 • 501 – 1.000 • 1.000 – 10.000 • > 10.000 • brak danych
17. Zasięg geograficzny obszaru, którego dotyczy incydent *	• Instytucja • Miasto/Województwo • Polska • Unia Europejska • Świat

	• brak danych
18. Rodzaj działania * Celowe-świadome / Niecelowe-nieświadome	• Celowe • Niecelowe
19. Kategoria zdarzenia *	• Podejrzana wiadomość e-mail | np. podejrzane załączniki, phishing, szantaż • Zbieranie informacji | np. skanowanie, podsłuch, SPAM, inżynieria społeczna • Treści obraźliwe | np. obrażanie, pornografia dziecięca, przemoc i inne nielegalne treści (informacje dla zespołu Dyzurnet.pl) • Oprogramowanie złośliwe | np. wirus, trojan, ransomware, dialer, botnet • Próby włamania | np. próby wykorzystania znanych błędów, próby logowania • Włamanie | np. włamanie na konto, do aplikacji, do systemu, do infrastruktury • Utrata dostępności usługi | np. DoS, DDoS, sabotaż, awaria, zaniedbanie, prace techniczne • Bezpieczeństwo informacji | np. nieuprawniony dostęp do informacji, nieuprawniona zmiana informacji lub jej skasowanie • Oszustwo | np. nieuprawnione wykorzystanie zasobów, Naruszenie praw autorski, podszywanie się, kradzież tożsamości • Podatność | np. błędna konfiguracja, wykrycie podatności • Cyberterroryzm | zdarzenie o charakterze terrorystycznym popełnione w cyberprzestrzeni • Inne | zdarzenia niemieszczące się w powyższych kategoriach • Test | kategoria ćwiczebna
20. Skutki oddziaływania incydentu na systemy informacyjne Instytucji *	• utrata dostępności danych / usługi • utrata poufności danych / usługi • utrata integralności danych / usługi • próba infekcji oprogramowaniem złośliwym • próba uzyskania nieuprawnionego dostępu • inne
dodatkowe informacje	
21. Przebieg incydentu oraz możliwa przyczyna jego wystąpienia *	
22. Podjęte działania zapobiegawcze *	

23. Podjęte działania naprawcze*	
24. Inne istotne informacje *	
25. Pola stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa (podaj nr pól po przecinku lub w przedziale np. 16. - 24.)	
Pola oznaczone * są polami wymaganymi. **Wypełniony formularz należy niezwłocznie przekazać do Administrator Systemu Informatycznego**	
Jeśli pojawią się nowe informacje dotyczące incydentu należy niezwłocznie je przekazać do Administratora Sieci Informatycznej.	