Procedura Zarządzania Incydentami Cyberbezpieczeństwa w Hotelu Pory Roku

Wstęp

1. Procedura zarządzania incydentami związanymi z cyberbezpieczeństwem ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych na działalność **Hotelu Pory Roku.**
2. Podstawą prawną do opracowania i wdrożenia niniejszej Procedury jest art. 22 ust. 1. pkt. 1 Ustawy o krajowym systemie cyberbezpieczeństwa z dnia 05 lipca 2018 r. (Dz. U. z 2018. poz. 1560 ze zm.).

Definicje

1. Incydent w podmiocie publicznym- incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.
2. Incydent krytyczny – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku prawnego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw lub wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT NASK.
3. Osoba pełniąca funkcję odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa – osoba wyznaczona przez Administratora Danych Osobowych.
4. Inspektor Ochrony Danych – osoba wyznaczona przez Administratora Danych Osobowych zwana dalej „IOD".
5. Administrator Systemów Informatycznych – osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych zwana dalej „ASI".
6. Administrator Danych Osobowych „ADO"- Dyrektor.
7. Jednostka – **Hotel Pory Roku**

Kategorie Incydentów

1. Incydent cyberbezpieczeństwa to zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych oraz, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.
2. Przyczyną powstania incydentu cyberbezpieczeństwa może być:

a) zdarzenia losowe zewnętrzne (np. klęski żywiołowe, pożary, zakłócenia w dostawie energii elektrycznej itp.), którego wystąpienie może spowodować zniszczenie lub uszkodzenie infrastruktury informatycznej albo dokumentacji papierowej oraz zakłócenia ciągłości pracy systemów nie powodując naruszenia poufności danych;
b) zdarzenie losowe wewnętrzne (np. błędy w oprogramowaniu, awarie sprzętu itp.), które mogą powodować zakłócenia ciągłości pracy systemów, a także prowadzić do zniszczenia lub utraty danych;
c) świadome i celowe działania mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych.

3. Incydentami cyberbezpieczeństwa w szczególności są działania takie jak:

a) naruszenie poufności, tj. ujawnienie informacji niepowołanym osobom;
b) naruszenie integralności, tj. zniszczenie, uszkodzenie lub przekłamanie informacji;
c) naruszenie dostępności, tj. braku dostępu do danych przez uprawnionych użytkowników.

4. Przyczyny incydentów cyberbezpieczeństwa mogą dotyczyć:

a) niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwe postępowanie z dokumentacją papierową;
b) działania szkodliwego oprogramowania;
c) próby omijania systemów zabezpieczeń;
d) nieautoryzowanego dostępu do systemów, aplikacji i dokumentów;
e)zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
f) zniszczenia lub kradzieży nośników danych;
g) próby wyłudzeń informacji;
h) ataków socjotechnicznych, ataków z wykorzystaniem technik zagrażających poufności;
i) integralności lub dostępności informacji;
j) nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych;

5. k) naruszenia zasad obowiązujących w **Hotelu Pory Roku** dotyczących bezpieczeństwa informacji, w tym danych osobowych.
6. O możliwości zaistnienia przypadku naruszenia cyberbezpieczeństwa mogą świadczyć:

a) nadmierne, w stosunku do wykonywanych zadań (zakresu upoważnienia), uprawnienia użytkownika do zasobów systemu;
b) niestabilna praca systemu teleinformatycznego;
c) korzystanie z zasobów systemu poza godzinami pracy bez zgody (przełożonego);
d) nowe „podejrzane" (nieznane) konta użytkowników;
e) wysoka aktywność kont, które długo pozostawały niewykorzystane;
f) zanotowanie w krótkim czasie dużej liczby nieudanych prób logowania;
g) anomalnie w pracy systemu lub programu (świadczące np. o obecności wirusa komputerowego);

7. h) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w których następuje przetwarzanie informacji w **Hotelu Pory Roku** (uszkodzone zamki, okna, drzwi, naruszone plomby, itp.).

Zakres Obowiązywania Procedury Zarządzania Incydentami Związanymi z Bezpieczeństwem Informacji oraz Cyberbezpieczeństwem

Procedura zarządzania incydentami związanymi z cyberbezpieczeństwem obowiązuje w **Hotelu Pory Roku.**

Zgłaszanie Incydentów Związanych z Bezpieczeństwem Informacji oraz Cyberbezpieczeństwem

1. W przypadku ujawnienia incydentu pracownik niezwłocznie powiadamia o tym fakcie Osobę pełniącą funkcję osoby odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, Inspektora Ochrony Danych oraz Administratora Systemów Informatycznych (w sytuacji gdy, incydent dotyczy bezpośrednio systemów komputerowych). Zgłoszenie następuje telefonicznie lub mailowo. Dane kontaktowe Osoby pełniącej funkcję odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, IOD oraz ASI znajdują się w klauzuli informacyjnej na stronie internetowej dps-wabrzezno.rbip.mojregion.info .Telefoniczne zgłoszenie należy potwierdzić notatką służbową, którą przekazuje się IOD poprzez swojego bezpośredniego przełożonego

lub bezpośrednio do IOD w przypadku pracowników zatrudnionych na samodzielnych stanowiskach.

2. Notatka musi zawierać następujące informację:

a) imię i nazwisko osoby zgłaszającej;
b) stanowisko oraz komórka organizacyjna;
c) dokładne miejsce oraz datę i godzinę wystąpienia incydentu;
d) opis incydentu wykonany w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego;
e) informacje o zgromadzonych materiałach dowodowych;
f) informacje dotyczące sposobu postępowania z incydentem.

3. Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.
4. W przypadku dłuższej nieobecności Osoby pełniącej funkcję odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz IOD incydent należy zgłosić do ASI w sposób określony w pkt. 1.

Podejmowanie Działań w Związku ze Zgłaszanymi Incydentami Związanymi z Bezpieczeństwem Informacji oraz Cyberbezpieczeństwem

1. Zgłoszenie incydentu rejestrowane jest przez IOD i przechowywane z dokumentacją pod nazwą „Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem". Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy (np. zrzut ekranu monitora, zdjęcie niezabezpieczonych materiałów zawierających dane osobowe itp.). Działania związane z obsługą zdarzenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia. W przypadku, kiedy zgłoszenie zostało zakwalifikowane jako incydent bezpieczeństwa informacji lub cyberbezpieczeństwa, dokonywana jest jego ocena istotności. Powyższe działania – ocena istotności – wykonuje osoba pełniąca funkcję odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa lub IOD w porozumieniu z ASI.
2. Przy ocenie istotności incydentu pod uwagę są brane następujące czynniki:

a) powstałe szkody będące wynikiem incydentu;
b) wpływ incydentu na działanie systemów;
c) wpływ incydentu na ciągłość działania **Hotelu**;
d) koszty usunięcia skutków incydentu;
e) szacowany czas naprawy skutków incydentu;
f) oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.

3. Zakwalifikowane zgłoszenia incydentu jako „fałszywy alarm" kończy postępowanie, o czym osoba pełniąca funkcję odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa lub IOD informuje zgłaszającego.
4. W przypadku zakwalifikowania zdarzenia jako incydent związany z bezpieczeństwem informacji lub cyberbezpieczeństwem, osoba pełniąca funkcję odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa lub IOD wspólnie z ASI podejmuje działania naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
5. Osoba pełniąca funkcję odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa lub IOD informuje ADO o wynikach analizy incydentu oraz podjętych działaniach naprawczych.
6. W przypadku stwierdzenia incydentu w podmiocie publicznym lub incydentu krytycznego osoba pełniąca funkcję osoby odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa lub IOD nie później niż w ciągu 24 godzin od momentu wykrycia zgłasza incydent do właściwego CSIRT NASK (Naukowa i Akademicka Sieć Komputerowa – Państwowego Instytutu Badawczego ul. Kolska 12, 01-045 Warszawa).
7. Zgłoszenia do CSIRT NASK przekazywane są w sposób elektroniczny. Procedura zgłoszeń

opisana jest pod adresem internetowym https://incydent.cert.pl/#!/lang=pl W przypadku braku możliwości przekazania go w sposób elektroniczny można zgłaszać przy użyciu innych dostępnych środków komunikacji (np. pod nr telefonu 223808274).

8. W zgłoszeniu przekazuje się informacje zgodnie z formularzem oraz zgodnie z treścią art. 23 ust.1 Ustawy o krajowym systemie cyberbezpieczeństwa z dnia 05 lipca 2018 r. (Dz. U. Z 2018r. poz. 1560 ze zm.).
9. W przypadku stwierdzenia działań zamierzonych , przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa informacji oraz cyberbezpieczeństwa ADO podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie, w zależności od wagi incydentu mogą zostać powiadomione organy ścigania.

Podejmowanie Działań w Związku ze Zgłaszanymi Incydentami Naruszenia Bezpieczeństwa Przetwarzania Danych Osobowych

1. W przypadku naruszenia ochrony danych osobowych mają zastosowanie przepisy ar. 33-34 Rozporządzenia Parlamentu Europejskiego i Rady (ue) 2016/679 z dnia 27 kwietnia 2016r. 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. ze zm.).
2. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie ochrony danych osobowych tj.:

a) przypadkowe lub niezgodne z prawem zniszczenie danych;
b) przypadkowa lub niezgodna z prawem utrata danych;
c) przypadkowa lub niezgodna z prawem modyfikacja danych;
d) nieuprawnione ujawnienie danych;
e) nieuprawniony dostęp do danych osobowych.

3. Każdy pracownik zatrudniony przy przetwarzaniu danych osobowych (pracownik, stażysta, praktykant itp.) jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie swojego bezpośredniego przełożonego oraz Inspektora Ochrony Danych i Administratora Systemów Informatycznych (jeżeli naruszenie ma związek z systemami informatycznymi).
4. Fakt naruszenia lub podejrzenia naruszenia ochrony danych osobowych należy potwierdzić pisemnie poprzez niezwłoczne sporządzenie notatki służbowej, w której umieszcza się informację o dacie, czasie, miejscu, okolicznościach zdarzenia. Notatkę przekazuję się do IOD za pośrednictwem swojego przełożonego lub bezpośrednio w przypadku osób zatrudnionych na samodzielnych stanowiskach. O zdarzeniu IOD niezwłocznie powiadamia ADO.
5. Zgłoszenia są rejestrowane w „Rejestrze naruszeń ochrony danych osobowych" prowadzonym zgodnie z art. 33 ust. 5 RODO.
6. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:

a) charakter naruszenia ochrony danych osobowych;
b) kategorię i przybliżoną liczbę osób których dane dotyczą;
c) kategorię i przybliżoną liczbę wpisów danych osobowych, których dotyczą.

….....
(podpis ADO)