Spis treści

Polityka zgłaszania incydentów bezpieczeństwa 2
1. Wstęp 2
2. Definicje 2
3. Zakres 2
4. Cele polityki 2
5. Obowiązki zgłaszającego 3
6. Kanały zgłaszania incydentów 3
7. Informacje wymagane przy zgłoszeniu 3
8. Proces obsługi incydentów 4
9. Kategorie incydentów 4
10. Poufność i ochrona danych 4
11. Szkolenia i podnoszenie świadomości 4
12. Monitorowanie i przegląd polityki 5

Polityka zgłaszania incydentów bezpieczeństwa

1. Wstęp

Niniejsza polityka określa zasady i procedury dotyczące zgłaszania, rejestrowania, analizowania oraz reagowania na incydenty bezpieczeństwa informacji w organizacji iTELade Security Operations Center (SOC). Celem jest szybka identyfikacja zagrożeń, minimalizacja skutków incydentów oraz zapobieganie ich powtórzeniu się, a także ciągłe doskonalenie bezpieczeństwa.

2. Definicje

- **Incydent bezpieczeństwa** – każde zdarzenie, które skutkuje lub może skutkować naruszeniem poufności, integralności lub dostępności informacji, systemów informatycznych bądź usług.
- **Zgłaszający** – osoba, która zauważyła lub podejrzewa wystąpienie incydentu i zgłasza go do SOC.
- **SOC (Security Operations Center)** – jednostka odpowiedzialna za monitorowanie, analizę oraz reagowanie na incydenty bezpieczeństwa w organizacji.
- **Rejestr incydentów** – system lub dokument, w którym zapisywane są wszystkie zgłoszenia incydentów wraz z ich szczegółami i statusem obsługi.

3. Zakres

Polityka dotyczy wszystkich pracowników, współpracowników, podwykonawców oraz użytkowników zasobów iTELade, którzy mają obowiązek niezwłocznie zgłaszać incydenty bezpieczeństwa.

4. Cele polityki

- Zapewnienie skutecznego i szybkiego zgłaszania incydentów.
- Ochrona zasobów organizacji przed zagrożeniami i naruszeniami.
- Minimalizacja negatywnych skutków incydentów.
- Dokumentowanie i analiza incydentów w celu doskonalenia procesów bezpieczeństwa.
- Wzrost świadomości i odpowiedzialności w obszarze bezpieczeństwa informacji.

5. Obowiązki zgłaszającego

Każdy, kto zauważy podejrzane lub nieprawidłowe zdarzenie, powinien:

- Niezwłocznie poinformować SOC.
- Przekazać wszelkie dostępne informacje dotyczące incydentu, w tym opis zdarzenia, czas, miejsce oraz osoby zaangażowane.
- Nie podejmować działań, które mogą zmienić lub zniszczyć dowody incydentu.
- Współpracować z zespołem SOC podczas procesu wyjaśniania i usuwania skutków incydentu.

6. Kanały zgłaszania incydentów

Incydenty należy zgłaszać za pomocą następujących kanałów:

- **E-mail: soc@itelade.pl**
- **Telefony kryzysowe (bezpośrednio do SOC):**
  61 641 98 55
  22 102 16 89
- Telefon ogólny iTELade:
  61 669 86 55

7. Informacje wymagane przy zgłoszeniu

Zgłoszenie incydentu powinno zawierać:

- Szczegółowy opis zdarzenia – co się wydarzyło, objawy, skutki.
- Datę i godzinę wykrycia incydentu.
- Miejsce wystąpienia incydentu (np. system, urządzenie, lokalizacja).
- Dane kontaktowe zgłaszającego.
- Dostępne materiały dowodowe (np. zrzuty ekranu, logi systemowe, wiadomości).
- Informacje o działaniach podjętych przed zgłoszeniem (jeśli dotyczy).

8. Proces obsługi incydentów

1. **Rejestracja zgłoszenia** – każde zgłoszenie jest rejestrowane w systemie SOC i przypisywany jest mu unikalny identyfikator.
2. **Wstępna analiza** – SOC ocenia charakter i wagę incydentu, weryfikuje jego autentyczność oraz określa priorytet.
3. **Reakcja** – podjęcie niezbędnych działań minimalizujących skutki incydentu, np. izolacja zagrożonych systemów, blokada kont, wdrożenie poprawek.
4. **Eskalacja** – w przypadku incydentów wysokiego ryzyka powiadamiane są wyższe szczeble zarządzania, zewnętrzne służby lub partnerzy (np. CERT, organy ścigania).
5. **Raportowanie** – sporządzenie szczegółowego raportu z przebiegu incydentu, jego skutków oraz działań naprawczych i zapobiegawczych.
6. **Zamknięcie incydentu** – po usunięciu zagrożenia i weryfikacji skuteczności działań incydent zostaje formalnie zamknięty.
7. **Analiza powdrożeniowa** – ewaluacja przyczyn incydentu i wprowadzenie usprawnień w procedurach oraz zabezpieczeniach.

9. Kategorie incydentów

- **Incydenty niskiego ryzyka** – drobne błędy, nieistotne zakłócenia działania.
- **Incydenty średniego ryzyka** – próby nieautoryzowanego dostępu, wykryte podatności, podejrzane działania.
- **Incydenty wysokiego ryzyka** – poważne naruszenia, wycieki danych, ataki ransomware, awarie krytycznych systemów.

10. Poufność i ochrona danych

Wszystkie zgłoszenia oraz informacje dotyczące incydentów są traktowane jako poufne i chronione zgodnie z obowiązującymi przepisami o ochronie danych osobowych (RODO). Udostępnianie informacji o incydentach na zewnątrz wymaga zgody uprawnionych osób.

11. Szkolenia i podnoszenie świadomości

Organizacja zobowiązuje się do regularnego szkolenia pracowników i innych zainteresowanych stron w zakresie rozpoznawania i zgłaszania incydentów oraz podnoszenia świadomości dotyczącej bezpieczeństwa informacji.

12. Monitorowanie i przegląd polityki

Polityka będzie podlegać przeglądowi co najmniej raz w roku oraz po każdym poważnym incydencie, aby zapewnić jej aktualność i skuteczność. Zmiany w polityce są komunikowane wszystkim pracownikom i współpracownikom.