Polityka Bezpieczeństwa Informacji

1. Wprowadzenie

1.1 Cel dokumentu

Celem niniejszej Polityki Bezpieczeństwa Informacji jest ustanowienie zasad i procedur zapewniających ochronę informacji w [NAZWA ORGANIZACJI].

1.2 Zakres

Niniejsza polityka ma zastosowanie do wszystkich pracowników, współpracowników, kontrahentów oraz innych osób mających dostęp do informacji [NAZWA ORGANIZACJI].

1.3 Definicje

[WYMIEŃ ISTOTNE DEFINICJE]

przykład:

- Informacja: Wszelkie dane przetwarzane przez organizację, niezależnie od formy i sposobu ich przechowywania.
- Bezpieczeństwo informacji: Zachowanie poufności, integralności i dostępności informacji.
- Incydent bezpieczeństwa: Zdarzenie, które może prowadzić do naruszenia bezpieczeństwa informacji.
- SZBI: System Zarządzania Bezpieczeństwem Informacji.

2. Organizacja bezpieczeństwa informacji

2.1 Role i odpowiedzialności

[WYMIEŃ ROLE I OPISZ ODPOWIEDZIALNOŚCI]

przykład:

- Zarząd: Odpowiada za zatwierdzenie Polityki Bezpieczeństwa Informacji, zapewnienie niezbędnych zasobów do jej wdrożenia oraz nadzór nad jej realizacją.
- Pełnomocnik ds. Bezpieczeństwa Informacji: Odpowiada za opracowanie, wdrożenie i monitorowanie SZBI, raportowanie do Zarządu o stanie bezpieczeństwa informacji.
- Pracownicy: Odpowiadają za przestrzeganie zasad określonych w Polityce Bezpieczeństwa Informacji, zgłaszanie incydentów bezpieczeństwa oraz uczestnictwo w szkoleniach.

2.2 Struktura zarządzania bezpieczeństwem informacji

[OPISZ STRUKTURĘ]

przykład: W Spółce XYZ Sp. z o.o. działa Komitet ds. Bezpieczeństwa Informacji, w skład którego wchodzą: Prezes Zarządu, Pełnomocnik ds. Bezpieczeństwa Informacji, Dyrektor IT oraz Inspektor Ochrony Danych. Komitet spotyka się raz na kwartał w celu omówienia kwestii związanych z bezpieczeństwem informacji.

3. Klasyfikacja i kontrola aktywów informacyjnych

3.1 Schemat klasyfikacji informacji

[DOSTOSUJ DO POTRZEB ORGANIZACJI]

przykład:

- Informacje jawne: Dostępne publicznie, np. informacje na stronie internetowej firmy.
- Informacje poufne: Dostępne tylko dla pracowników, np. wewnętrzne procedury, dane klientów.
- Informacje ściśle poufne: Dostępne tylko dla wybranych osób, np. strategia firmy, dane finansowe.

3.2 Zasady oznaczania i obchodzenia się z informacjami

[OPISZ ZASADY DLA KAŻDEJ KATEGORII]

przykład:

- Informacje jawne: Nie wymagają specjalnego oznaczenia.
- Informacje poufne: Oznaczone jako "Poufne", przechowywane w zamkniętych szafkach lub zabezpieczonych folderach elektronicznych.
- Informacje ściśle poufne: Oznaczone jako "Ściśle poufne", przechowywane w sejfie lub zaszyfrowanych plikach, dostęp tylko za zgodą Zarządu.

4. Bezpieczeństwo zasobów ludzkich

4.1 Szkolenia i podnoszenie świadomości

[OPISZ PROGRAM SZKOLEŃ]

przykład: Wszyscy nowi pracownicy przechodzą obowiązkowe szkolenie z zakresu bezpieczeństwa informacji w ciągu pierwszego miesiąca pracy. Szkolenia odświeżające organizowane są raz w roku dla wszystkich pracowników. Dodatkowo, raz na kwartał rozsyłany jest newsletter z aktualnymi informacjami na temat bezpieczeństwa.

4.2 Proces zatrudniania i zwalniania pracowników

[OPISZ PROCEDURY]

przykład: Przed zatrudnieniem: Sprawdzenie referencji, podpisanie umowy o poufności. W trakcie zatrudnienia: Nadanie niezbędnych uprawnień, szkolenie z bezpieczeństwa informacji. Przy zwolnieniu: Odebranie uprawnień dostępu, zwrot sprzętu firmowego, przypomnienie o obowiązku zachowania poufności.

5. Bezpieczeństwo fizyczne i środowiskowe

5.1 Kontrola dostępu do pomieszczeń

[OPISZ ZASADY DOSTĘPU]

przykład: Wejście do biura zabezpieczone kartami dostępu. Pomieszczenia serwerowni dostępne tylko dla upoważnionego personelu IT, zabezpieczone dodatkowo kodem PIN. Rejestr wejść i wyjść prowadzony elektronicznie.

5.2 Ochrona sprzętu

[OPISZ ŚRODKI OCHRONY]

przykład: Laptopy zabezpieczone programem antywirusowym i szyfrowaniem dysku. Serwery umieszczone w klimatyzowanym pomieszczeniu z kontrolą dostępu i systemem gaśniczym. Regularne przeglądy i konserwacja sprzętu.

6. Zarządzanie systemami i sieciami

6.1 Ochrona przed złośliwym oprogramowaniem

[OPISZ STOSOWANE ZABEZPIECZENIA]

przykład: Zainstalowane oprogramowanie antywirusowe na wszystkich stacjach roboczych i serwerach, aktualizowane codziennie. Firewall na brzegu sieci. Regularne skanowanie sieci pod kątem podatności.

6.2 Kopie zapasowe

[OPISZ PROCEDURY TWORZENIA I PRZECHOWYWANIA KOPII]

przykład: Pełne kopie zapasowe wykonywane codziennie w nocy, przechowywane w dwóch lokalizacjach: lokalnie i w chmurze. Testy odtwarzania danych przeprowadzane raz na kwartał.

7. Kontrola dostępu

7.1 Polityka haseł

[OKREŚL WYMAGANIA DOTYCZĄCE HASEŁ]

przykład: Minimalna długość hasła: 12 znaków. Wymagane użycie małych i wielkich liter, cyfr oraz znaków specjalnych. Zmiana hasła wymagana co 90 dni. Blokada konta po 5 nieudanych próbach logowania.

7.2 Zarządzanie uprawnieniami użytkowników

[OPISZ PROCES NADAWANIA I ODBIERANIA UPRAWNIEŃ]

przykład: Nadawanie uprawnień na podstawie pisemnego wniosku przełożonego. Przegląd uprawnień przeprowadzany co 6 miesięcy. Natychmiastowe odbieranie uprawnień przy zmianie stanowiska lub zakończeniu współpracy.

8. Zarządzanie incydentami bezpieczeństwa informacji

8.1 Procedury zgłaszania i obsługi incydentów

[OPISZ PROCEDURY]

przykład: Incydenty zgłaszane do helpdesku IT (telefon: 123-456-789, email: helpdesk@xyz.com). Wstępna analiza w ciągu 1 godziny od zgłoszenia. Klasyfikacja incydentu i podjęcie działań zgodnie z procedurą reakcji na incydenty.

8.2 Plan reakcji na incydenty

[ZARYSUJ PLANU REAKCJI]

przykład:

1. Identyfikacja i klasyfikacja incydentu
2. Izolacja systemów/danych, których dotyczy incydent
3. Zebranie dowodów
4. Usunięcie przyczyny incydentu
5. Przywrócenie normalnego funkcjonowania
6. Raport z incydentu i wyciągnięcie wniosków

9. Zgodność z wymogami prawnymi i standardami

9.1 Ochrona danych osobowych

[ODWOŁANIE DO POLITYKI OCHRONY DANYCH OSOBOWYCH]

przykład: Spółka XYZ Sp. z o.o. przestrzega zasad określonych w RODO. Szczegółowe zasady przetwarzania danych osobowych określone są w osobnej Polityce Ochrony Danych Osobowych.

9.2 Audyty bezpieczeństwa informacji

[OPISZ CZĘSTOTLIWOŚĆ I ZAKRES AUDYTÓW]

przykład: Wewnętrzny audyt bezpieczeństwa informacji przeprowadzany raz w roku. Zewnętrzny audyt bezpieczeństwa (penetration testing) zlecany co dwa lata.

10. Ciągłość działania

10.1 Plan ciągłości działania

[ZARYS PLANU]

przykład: Plan obejmuje scenariusze awaryjne dla kluczowych procesów biznesowych, w tym:

- Awaria głównego serwera
- Brak dostępu do biura
- Atak ransomware Dla każdego scenariusza określone są procedury działania, osoby odpowiedzialne i dane kontaktowe.

10.2 Testowanie planów awaryjnych

[OPISZ PROCES TESTOWANIA]

przykład: Testy planów awaryjnych przeprowadzane raz w roku, obejmujące symulację wybranych scenariuszy. Wnioski z testów wykorzystywane do aktualizacji planów.

11. Bezpieczeństwo w relacjach z dostawcami

11.1 Wymagania bezpieczeństwa dla dostawców

[OPISZ KLUCZOWE WYMAGANIA]

przykład:

- Podpisanie umowy o zachowaniu poufności
- Zgodność z wymogami RODO przy przetwarzaniu danych osobowych
- Zapewnienie szyfrowania danych przesyłanych przez internet
- Udostępnienie wyników ostatniego audytu bezpieczeństwa (jeśli dotyczy)

12. Bezpieczeństwo pracy zdalnej i urządzeń mobilnych

12.1 Zasady pracy zdalnej

[OPISZ GŁÓWNE ZASADY]

przykład:

- Korzystanie z VPN przy łączeniu się z siecią firmową
- Zakaz korzystania z publicznych sieci Wi-Fi bez VPN
- Zakaz pozostawiania urządzeń bez nadzoru w miejscach publicznych
- Regularne aktualizacje oprogramowania na urządzeniach używanych do pracy zdalnej

12.2 Bezpieczeństwo urządzeń mobilnych

[OPISZ WYMAGANIA]

przykład:

- Obowiązkowe szyfrowanie dysków w laptopach
- Używanie silnych haseł lub PIN-ów do blokowania urządzeń
- Możliwość zdalnego wymazania danych z urządzeń w przypadku zgubienia lub kradzieży
- Zakaz instalowania aplikacji z nieznanych źródeł

13. Monitorowanie i przeglądy bezpieczeństwa

13.1 Rejestrowanie zdarzeń i monitoring

[OPISZ ZAKRES I METODY MONITORINGU]

przykład: Logowanie wszystkich prób dostępu do systemów IT. Monitoring ruchu sieciowego 24/7. Analiza logów systemowych raz w tygodniu przez zespół IT.

13.2 Regularne przeglądy polityki

[OKREŚL CZĘSTOTLIWOŚĆ I PROCES PRZEGLĄDÓW]

przykład: Przegląd Polityki Bezpieczeństwa Informacji przeprowadzany co roku lub w przypadku istotnych zmian w organizacji lub otoczeniu prawnym.

14. Sankcje za naruszenie polityki

[OPISZ POTENCJALNE KONSEKWENCJE]

przykład: Naruszenie zasad Polityki Bezpieczeństwa Informacji może skutkować:

- Upomnieniem ustnym lub pisemnym
- Ograniczeniem uprawnień dostępu do systemów
- Konsekwencjami dyscyplinarnymi, włącznie z rozwiązaniem umowy o pracę
- W przypadku poważnych naruszeń - odpowiedzialnością prawną

15. Zatwierdzenie i historia zmian

Wersja: 1.0 Data zatwierdzenia: [DATA] Zatwierdzone przez: [IMIĘ NAZWISKO, FUNKCJA, np. Jan Kowalski, Prezes Zarządu]

Historia zmian:

- 15.09.2024 - Wersja 1.0 - Utworzenie dokumentu
- [MIEJSCE NA REJESTROWANIE KOLEJNYCH ZMIAN]