ASTAT

Poznań, 02.12.2024

POLITYKA
BEZPIECZEŃSTWA INFORMACJI

Celem Polityki Bezpieczeństwa Grupy ASTAT jest zapewnienie ochrony zasobów firmy, w tym informacji, systemów informatycznych, danych osobowych oraz pracowników, przed zagrożeniami wewnętrznymi i zewnętrznymi. Celem jest również zgodność z obowiązującymi przepisami prawa, w tym RODO.

Polityka obejmuje wszystkich pracowników, kontrahentów, partnerów biznesowych Grupy ASTAT oraz wszystkie systemy informatyczne, sieci, aplikacje i dane należące do Grupy ASTAT.

ZAKRES STOSOWANIA

Polityka Bezpieczeństwa dotyczy wszystkich pracowników, współpracowników, partnerów biznesowych oraz innych osób korzystających z zasobów Grupy ASTAT. Obejmuje następujące obszary:

- bezpieczeństwo informacji,
- ochrona danych osobowych,
- bezpieczeństwo systemów IT,
- bezpieczeństwo fizyczne.

ZOBOWIĄZANIA

Ochrona informacji i danych osobowych

- przetwarzanie danych osobowych odbywa się zgodnie z RODO oraz wewnętrznymi procedurami,
- dostęp do danych jest ograniczony do osób upoważnionych,
- wdrażane są środki techniczne (np. ochrona hasłami) i organizacyjne (np. szkolenia, procedury) w celu ochrony danych.

ASTAT

ZOBOWIĄZANIA

Bezpieczeństwo systemów informatycznych

- ◇ przetwarzanie danych osobowych odbywa się zgodnie z RODO oraz wewnętrznymi procedurami,
- ◇ dostęp do danych jest ograniczony do osób upoważnionych,
- ◇ wdrażane są środki techniczne (np. ochrona hasłami) i organizacyjne (np. szkolenia, procedury) w celu ochrony danych.

Bezpieczeństwo fizyczne

- ◇ dostęp do biur i serwerowni firmy jest monitorowany (kontrola dostępu, monitoring),
- ◇ w przypadku zagrożenia (pożar, włamanie) obowiązują procedury awaryjne i plany ewakuacji.

Szkolenia i odpowiedzialność

- ◇ wszyscy pracownicy są zobowiązani do regularnego uczestnictwa w szkoleniach dotyczących bezpieczeństwa,
- ◇ każdy pracownik ma obowiązek przestrzegania zasad zawartych w niniejszej polityce,
- ◇ naruszenie zasad polityki może skutkować odpowiedzialnością dyscyplinarną, a w przypadku rażących naruszeń - sankcjami prawnymi.

Zarządzanie ryzykiem:

Stosujemy systematyczne podejście do identyfikacji i oceny ryzyka związanego z bezpieczeństwem informacji, co pozwala na priorytetyzację środków zaradczych. Regularnie aktualizujemy nasze plany zarządzania ryzykiem, aby odpowiadały one na zmieniające się zagrożenia i warunki biznesowe.

Zarządzanie incydentami:

Posiadamy zdefiniowane i przetestowane procedury reagowania na incydenty bezpieczeństwa, które umożliwiają szybką identyfikację, analizę i reakcję na naruszenia bezpieczeństwa. Działania te minimalizują potencjalne szkody i przywracają normalne operacje w możliwie najkrótszym czasie.

ASTAT

ZOBOWIĄZANIA

Ciągłe doskonalenie:

Nasze procesy i środki zapewniające bezpieczeństwo informacji są regularnie przeglądane i aktualizowane w oparciu o feedback, wyniki audytów i zmiany w otoczeniu technologicznym. Dąży to do ciągłego doskonalenia skuteczności naszego i efektywności systemu zarządzania bezpieczeństwem informacji.

Przegląd i aktualizacja polityki:

Nasza polityka bezpieczeństwa informacji jest regularnie przeglądana i aktualizowana, aby odzwierciedlać zmiany w prawie, technologii oraz w naszym otoczeniu biznesowym. Proces ten zapewnia, że polityka pozostaje odpowiednia i efektywna.

CELE BEZPIECZEŃSTWA INFORMACJI

1. Zabezpieczenie poufności danych i zapewnienie, że dostęp do danych jest ograniczony tylko dla uprawnionych osób.
2. Zachowanie integralności danych oraz ochrona danych przed nieautoryzowanymi zmianami.
3. Zapewnienie dostępności danych i gwarancja, że dane i systemy są dostępne dla uprawnionych użytkowników w razie potrzeby.
4. Zarządzanie ryzykiem bezpieczeństwa wraz z regularną oceną i minimalizacją ryzyka związanego z bezpieczeństwem danych.
5. Zwiększenie świadomości bezpieczeństwa oraz budowanie kultury bezpieczeństwa informacji wśród wszystkich pracowników.
6. Spełnianie wymagań regulacyjnych i zapewnienie zgodności z obowiązującymi przepisami i standardami dotyczącymi bezpieczeństwa informacji.

Prezes Grupy ASTAT

Romuald Winter