



**AEGIS**  
SECURITY

**PORADY DOTYCZĄCE  
CYBERBEZPIECZEŃSTWA  
DLA PODMIOTÓW MSP**

# STWÓRZ KULTURĘ CYBERBEZPIECZEŃSTWA

Przeprowadzaj regularne audyty bezpieczeństwa informacji.

Pamiętaj o RODO.

Opublikuj politykę cyberbezpieczeństwa.

Przypisz odpowiedzialność za zarządzanie.

Przedstaw cele i powody zmian w firmie.



**AEGIS**  
SECURITY

# **ORGANIZUJ ODPOWIEDNIE SZKOLENIA**

Zorganizuj cykliczne szkolenia w celu zwiększenia świadomości na temat cyberbezpieczeństwa dla Twoich pracowników. W celu dopilnowania, aby potrafili oni rozpoznawać i radzić sobie z różnymi zagrożeniami dla Twojej firmy. Szkolenia powinny koncentrować się na rzeczywistych sytuacjach życiowych, które mogą dotknąć Twoją organizację.

Szkól nie tylko szeregowego pracownika. Dbaj i zapewnij specjalistyczne szkolenia dla osób odpowiedzialnych za zarządzanie cyberbezpieczeństwem w przedsiębiorstwie, aby zapewnić im umiejętności i kompetencje wymagane do wykonywania pracy i skutecznej obrony.



# ZACZNIJ SKUTECZNE ZARZĄDZANIE PODMIOTAMI ZEWNĘTRZNYMI



Dbaj, aby wszyscy dostawcy, a w szczególności ci, którzy mają dostęp do wrażliwych danych lub systemów, byli kontrolowani i osiągnęli uzgodnione poziomy bezpieczeństwa. Warto zawrzeć umowy regulujące sposób, w jaki dostawcy spełniają wymogi bezpieczeństwa.





**AEGIS**  
SECURITY

# OPRACUJ PLAN REAGOWANIA NA INCYDENTY

Stwórz plan reagowania na incydenty  
Powinien być jasny i precyzyjny.

Zapewnij odpowiednią obsługę  
incydentu.

Wyznacz role dla pracowników  
odpowiedzialnych za obsługę incydentu.

Wyposaż swój zespół w odpowiednie  
narzędzia, które mogą monitorować  
i tworzyć alerty w przypadku wystąpienia  
podejrzanej aktywności lub naruszenia  
bezpieczeństwa.

# ZABEZPIECZ DOSTĘP DO SYSTEMÓW

Zachęcaj wszystkich do używania hasła-frazy, czyli zbioru co najmniej trzech przypadkowych, popularnych słów połączonych we frazę, które stanowią bardzo dobre połączenie łatwości zapamiętywania i bezpieczeństwa.

**Jeśli jednak zdecydujesz się na typowe hasło:**

- niech będzie długie,
- z małymi i wielkimi literami,
- ewentualnie także cyframi i znakami specjalnymi,
- unikaj oczywistych fraz, takich jak „hasło”, ciągów liter lub cyfr, takich jak „abc”, liczb jak „123”,
- unikaj używania danych osobowych, które można znaleźć w Internecie.

Niezależnie od tego, czy używasz haseł czy fraz, nie używaj ich ponownie w innych miejscach, nie udostępniaj ich współpracownikom, włącz uwierzytelnianie wieloskładnikowe, korzystaj z dostosowanego menedżera haseł.



**AEGIS**  
SECURITY

# ZABEZPIECZ URZĄDZENIA



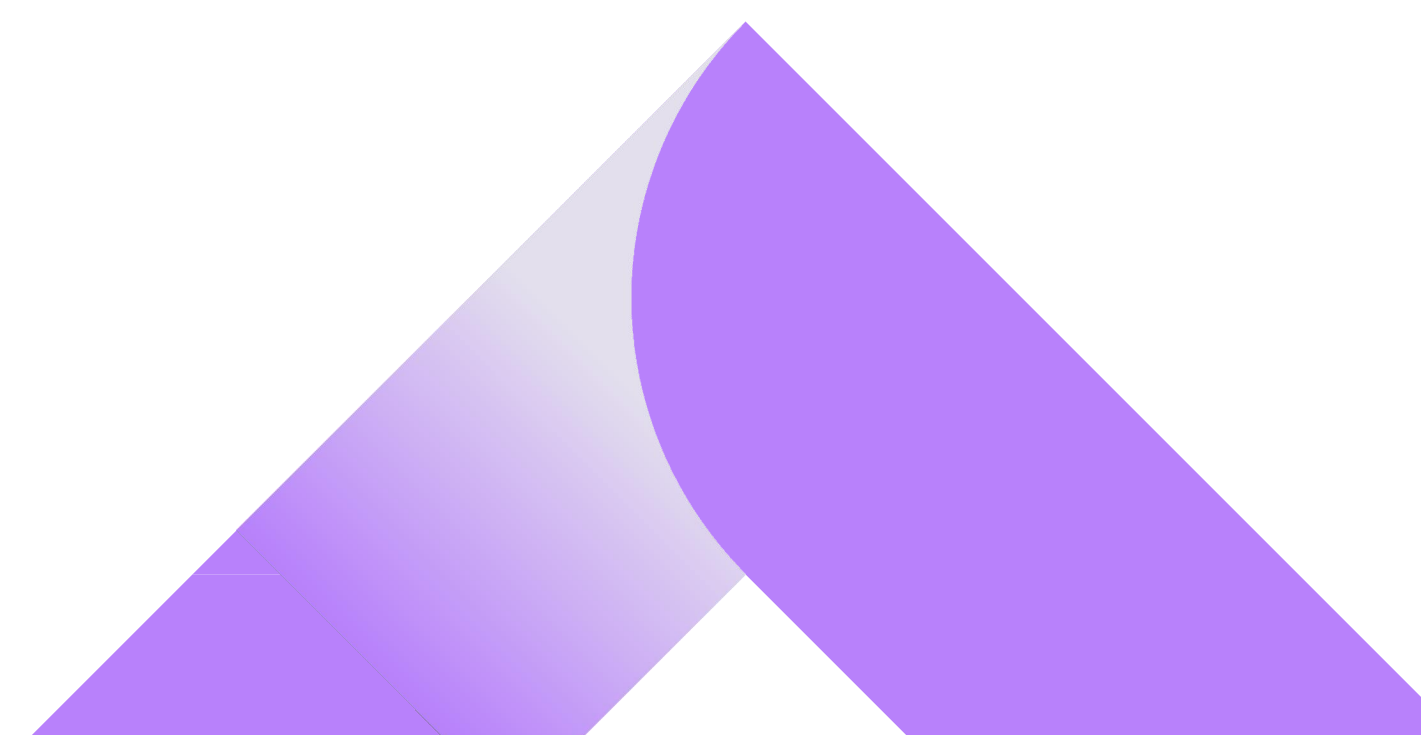
Regularnie aktualizuj oprogramowanie.

Stosuj narzędzia ochrony poczty elektronicznej i stron WWW.

Szyfruj urządzenia.

Zainstaluj dobrego Antywirusa.

Wprowadź rejestr i zarządzaj urządzeniami mobilnymi.



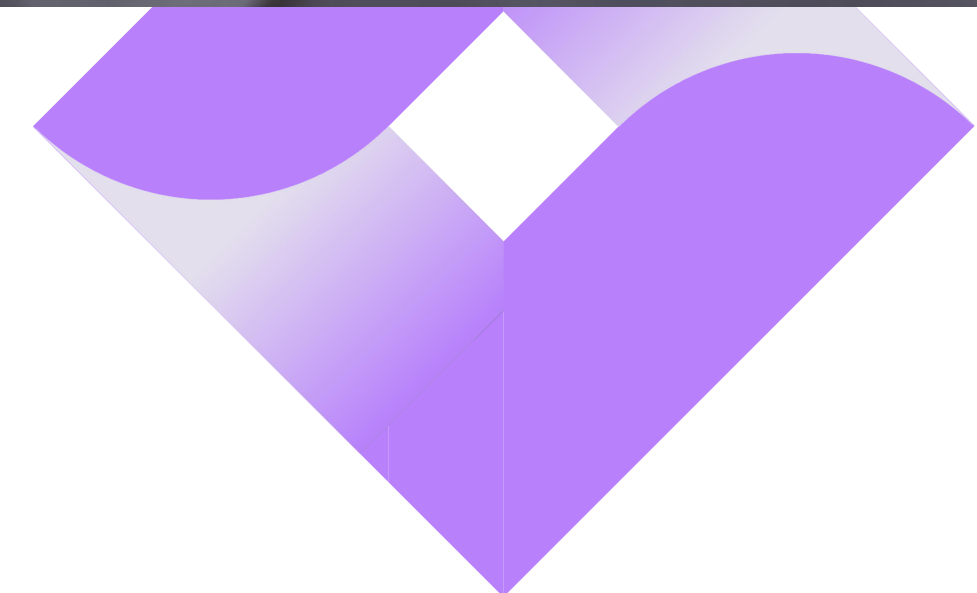
# ZABEZPIECZ SWOJĄ SIĘĆ

## **STOSUJ ZAPORY SIECIOWE**

Zapory sieciowe powinny być rozmieszczone w celu ochrony wszystkich kluczowych systemów, w szczególności zaporę sieciową należy stosować do ochrony sieci MŚP przed Internetem.

## **DOKONUJ PRZEGLĄDU ROZWIĄZAŃ ZDALNEGO DOSTĘPU:**

upewnij się, że całe oprogramowanie zdalnego dostępu jest poprawione i aktualne,  
ograniczaj dostęp zdalny z podejrzanych połączeń geograficznych lub określonych adresów IP,  
ograniczaj zdalny dostęp pracowników tylko do tych systemów i komputerów, które są im potrzebne do pracy,  
egzekwuj stosowanie silnych haseł przy dostępie zdalnym i w miarę możliwości włączaj uwierzytelnianie wieloskładnikowe,  
zapewnij monitorowanie i ostrzeganie o podejrzanych atakach lub nietypowej podejrzanej aktywności.





**AEGIS**  
SECURITY

# POPRAW BEZPIECZEŃSTWO FIZYCZNE



**AEGIS**  
SECURITY

Wszędzie tam, gdzie znajdują się ważne informacje, należy stosować odpowiednie kontrole fizyczne.

Wdrażaj zasady i egzekwuj ich wykonywanie: np. firmowego laptopa lub smartfona nie powinno się zostawiać bez opieki na tylnym siedzeniu samochodu.

Za każdym razem, gdy użytkownik odchodzi od swojego komputera, powinien go zablokować. W przeciwnym razie należy włączyć funkcję automatycznego blokowania na każdym urządzeniu używanym do celów służbowych.

Wrażliwe dokumenty drukowane również nie powinny być pozostawiane bez nadzoru, a gdy nie są używane, należy je bezpiecznie przechowywać.



# STWÓRZ I ZABEZPIECZ KOPIE ZAPASOWE

## **Aby umożliwić odzyskanie kluczowych informacji, należy utrzymywać kopie zapasowe!!!**

Nie ma lepszego sposobu na odzyskanie cennych informacji po atakach ransomware.

### **Należy stosować następujące zasady tworzenia kopii zapasowych:**

- twórz kopie zapasowe regularne i w miarę możliwości zautomatyzowane,
- kopia zapasowa jest przechowywana oddzielnie od środowiska produkcyjnego MŚP,
- kopie zapasowe są szyfrowane, zwłaszcza jeśli mają być przenoszone między lokalizacjami,
- testuj zdolność do przywracania danych z kopii zapasowych.



# KORZYSTAJ Z CHMURY

Wybierając dostawcę usług w chmurze, przedsiębiorcy powinni upewnić się, że nie narusza ono żadnych przepisów lub regulacji poprzez przechowywanie danych, zwłaszcza danych osobowych, poza UE/EOG.



Na przykład unijne RODO wymaga, aby dane osobowe osób zamieszkałych w UE/EOG nie były przechowywane ani przekazywane poza UE/EOG, chyba że na bardzo szczególnych warunkach.

# ZABEZPIECZ STRONY INTERNETOWE



**AEGIS**  
SECURITY

Istotne jest zapewnienie, aby Twoja strona internetowa była skonfigurowana i utrzymywana w bezpieczny sposób oraz aby wszelkie dane osobowe lub szczegóły finansowe, takie jak dane kart kredytowych, były odpowiednio chronione.

Wykonuj regularne testy bezpieczeństwa stron internetowych oraz aplikacji w celu zidentyfikowania wszelkich potencjalnych słabości bezpieczeństwa.

Dostosowuj stronę do aktualnie obowiązujących przepisów.

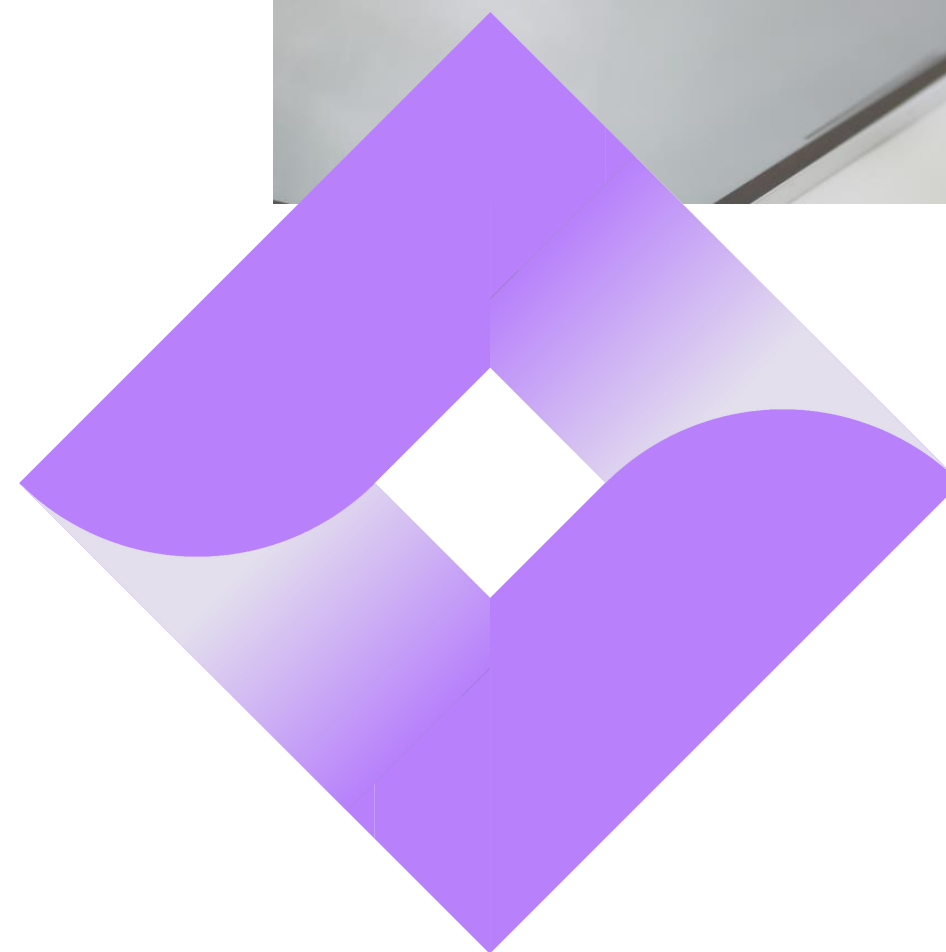
**POSZUKUJ INFORMACJI  
I DZIEL SIĘ NIMI**

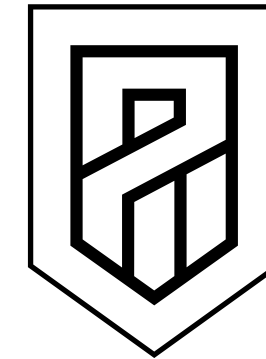
Nie wstydź się, że padłeś ofiarą ataku cyberprzestępcy!!

Rozmawiaj z innymi przedstawicielami firm z Twojego sektora w jaki sposób zabezpieczają się przed nieautoryzowanymi atakami.

Zweryfikuj w jaki sposób inne firmy z rynku dbają o cyberbezpieczeństwo i zacznij powielać dobre schematy.

Zainwestuj w specjalistę z rynku, wykonaj audyt bezpieczeństwa i przeanalizuj raport wdrażając wnioski z niego płynące.





**AEGIS**  
SECURITY

Aegis Security Sp. z o.o.  
ul. Cybernetyki 19B  
02-677 Warszawa

[kontakt@aegissecurity.pl](mailto:kontakt@aegissecurity.pl)  
[www.aegissecurity.pl](http://www.aegissecurity.pl)