Polityka Bezpieczeństwa Informacji

1. Cel polityki

Celem Polityki Bezpieczeństwa Informacji jest zapewnienie odpowiedniego poziomu ochrony informacji przetwarzanych przez Efinistry Sp. z o.o. oraz budowanie zaufania klientów, partnerów biznesowych i pracowników poprzez stosowanie skutecznych środków organizacyjnych, technicznych i prawnych.

2. Zakres działalności

Efinistry Sp. z o.o. świadczy usługi w zakresie:

- projektowania i wdrażania dedykowanego oprogramowania,
- integracji systemów informatycznych,
- utrzymania i rozwoju systemów IT,
- automatyzacji procesów biznesowych,
- rozwiązań dla księgowości, e-commerce i zarządzania przedsiębiorstwem,
- doradztwa technologicznego i wsparcia operacyjnego.

3. Nasze zobowiązania

W ramach realizowanej działalności zobowiązujemy się do:

- ochrony poufności, integralności i dostępności informacji,
- przestrzegania obowiązujących przepisów prawa, w tym RODO,
- ograniczania ryzyk związanych z cyberbezpieczeństwem,
- zapewnienia ciągłości działania świadczonych usług,
- ciągłego doskonalenia stosowanych zabezpieczeń.

4. Zarządzanie bezpieczeństwem informacji

Bezpieczeństwo informacji jest integralnym elementem procesów biznesowych organizacji. Regularnie identyfikujemy zagrożenia i oceniamy ryzyka związane z przetwarzaniem informacji oraz wdrażamy adekwatne środki ochrony. Szczegółowe zasady bezpieczeństwa określają wewnętrzne polityki i procedury organizacji.

5. Ochrona informacji i systemów

W celu ochrony danych i systemów stosujemy między innymi:

- kontrolę dostępu opartą na zasadzie minimalnych uprawnień,
- uwierzytelnianie wieloskładnikowe (MFA) dla wybranych usług,

- szyfrowanie transmisji danych,
- regularne aktualizacje systemów i oprogramowania,
- ochronę antywirusową i monitorowanie bezpieczeństwa,
- wykonywanie kopii zapasowych oraz procedury odtwarzania danych,
- zabezpieczenia infrastruktury sieciowej i środowisk chmurowych.

6. Ochrona danych osobowych

Dane osobowe przetwarzane są zgodnie z obowiązującymi przepisami prawa oraz zasadami minimalizacji danych, ograniczenia dostępu i odpowiedniego zabezpieczenia informacji.

7. Zarządzanie incydentami

Posiadamy procedury identyfikacji, zgłaszania i obsługi incydentów bezpieczeństwa. Każdy incydent podlega analizie, a wyniki wykorzystywane są do dalszego doskonalenia zabezpieczeń.

8. Ciągłość działania

Podejmujemy działania mające na celu zapewnienie ciągłości świadczenia usług, w tym monitorowanie systemów, wykonywanie kopii zapasowych oraz przygotowanie procedur reagowania na sytuacje awaryjne.

9. Świadomość pracowników

Pracownicy i współpracownicy są zobowiązani do przestrzegania zasad bezpieczeństwa informacji oraz uczestniczą w działaniach podnoszących świadomość w zakresie cyberbezpieczeństwa i ochrony danych.

10. Ciągłe doskonalenie

Regularnie przeglądamy skuteczność stosowanych zabezpieczeń, analizujemy ryzyka oraz wdrażamy działania doskonalące w celu utrzymania wysokiego poziomu bezpieczeństwa informacji.

Deklaracja

Efinistry Sp. z o.o. traktuje bezpieczeństwo informacji jako jeden z kluczowych elementów odpowiedzialnego prowadzenia działalności. Dokładamy wszelkich starań, aby chronić dane naszych klientów, partnerów i pracowników oraz zapewniać bezpieczne i niezawodne usługi informatyczne.