Polityka Bezpieczeństwa Informacji – Elephantus

1. Wprowadzenie

Elephantus zobowiązuje się do zapewnienia najwyższego poziomu bezpieczeństwa informacji w swojej działalności.
Celem niniejszej polityki jest ochrona informacji przed nieuprawnionym dostępem, utratą, zniszczeniem lub ujawnieniem oraz zapewnienie ich poufności, integralności i dostępności.

---

2. Zakres obowiązywania

Polityka obejmuje:

- *wszystkich pracowników i współpracowników*
- *systemy informatyczne i urządzenia wykorzystywane w firmie*
- *dane klientów, kontrahentów oraz dane wewnętrzne*

---

3. Definicja informacji

Informacją w rozumieniu niniejszej polityki są wszelkie dane przetwarzane przez Elephantus, w szczególności:

- *dane osobowe*
- *dane klientów i kontrahentów*
- *dokumenty firmowe*
- *informacje finansowe i operacyjne*

---

4. Podstawowe zasady bezpieczeństwa informacji

Elephantus stosuje następujące zasady:

✓***Poufność*** *– dostęp do informacji mają wyłącznie osoby uprawnione*
✓***Integralność*** *– dane są chronione przed nieautoryzowaną zmianą*
✓***Dostępność*** *– informacje są dostępne dla uprawnionych użytkowników w odpowiednim czasie*

---

5. Ochrona danych osobowych

Elephantus przetwarza dane osobowe zgodnie z obowiązującymi przepisami prawa, w tym z Rozporządzeniem RODO (GDPR).

Firma zapewnia:

- *przetwarzanie danych zgodnie z prawem*
- *minimalizację zakresu przetwarzanych danych*
- *odpowiednie zabezpieczenia techniczne i organizacyjne*

---

6. Zarządzanie dostępem

- *Dostęp do systemów i danych nadawany jest zgodnie z zakresem obowiązków*
- *Stosowane są indywidualne konta użytkowników*
- *Hasła powinny być silne i regularnie zmieniane*
- *Dostępy są okresowo weryfikowane*

---

7. Bezpieczeństwo systemów IT

Elephantus stosuje środki ochrony, takie jak:

- *oprogramowanie antywirusowe i zapory sieciowe*
- *aktualizacje systemów i aplikacji*
- *kopie zapasowe danych*
- *zabezpieczenia urządzeń mobilnych*

---

8. Bezpieczeństwo fizyczne

- *Dostęp do pomieszczeń firmowych jest kontrolowany*
- *Dokumenty w formie papierowej są odpowiednio przechowywane*
- *Sprzęt i nośniki danych są zabezpieczone przed kradzieżą i zniszczeniem*

---

9. Postępowanie w przypadku incydentów

Każdy pracownik ma obowiązek niezwłocznie zgłosić incydent bezpieczeństwa, w szczególności:

- *naruszenie ochrony danych*
- *utratę sprzętu lub dokumentów*
- *podejrzane działania w systemach IT*

Firma zobowiązuje się do:

- *szybkiej analizy incydentu*
- *ograniczenia skutków naruszenia*
- *wdrożenia działań zapobiegawczych*

---

10. Szkolenia i świadomość

Elephantus zapewnia regularne szkolenia pracowników w zakresie:

- *ochrony danych*
- *cyberbezpieczeństwa*
- *bezpiecznego korzystania z systemów*

---

11. Odpowiedzialność

- *Zarząd odpowiada za wdrożenie i nadzór nad polityką*
- *Pracownicy są zobowiązani do jej przestrzegania*
- *Naruszenie zasad może skutkować konsekwencjami służbowymi*

---

12. Postanowienia końcowe

Polityka podlega okresowej aktualizacji w celu dostosowania do zmian prawnych, technologicznych i organizacyjnych.
Elephantus traktuje bezpieczeństwo informacji jako kluczowy element swojej działalności i zaufania klientów.