Poznań, 13.01.2025

DZIAŁ SZKOLENIOWY

Polityka Bezpieczeństwa Informacji

Dział Szkoleniowy

1. Postanowienia ogólne

1. Celem niniejszej Polityki Bezpieczeństwa Informacji jest określenie zasad, środków i procedur zapewniających bezpieczeństwo danych osobowych i informacji przetwarzanych w Dziale Szkoleniowym zgodnie z:
   - Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO),
   - ustawą o ochronie danych osobowych,
   - zasadami dobrej praktyki w zakresie bezpieczeństwa.
2. Polityka ma zastosowanie do wszystkich pracowników, współpracowników, trenerów oraz partnerów Działu Szkoleniowego, którzy mają dostęp do informacji lub danych.

---

2. Zakres i cel przetwarzania danych

1. Dział Szkoleniowy przetwarza dane osobowe w związku z prowadzeniem działalności szkoleniowej, w tym m.in.:
   - rekrutacją uczestników na szkolenia,
   - organizacją i realizacją usług szkoleniowo-rozwojowych,
   - wystawianiem zaświadczeń, certyfikatów i dokumentacji szkoleniowej,
   - obsługą finansową i administracyjną projektów,
   - realizacją obowiązków wynikających z umów, przepisów i wymogów instytucji finansujących.
2. Zakres przetwarzanych danych obejmuje m.in.: imię, nazwisko, data urodzenia, wykształcenie, dane pracodawcy, stanowisk, dane do faktur, dane wrażliwe tylko w sytuacjach przewidzianych prawem.

---

3. Role i odpowiedzialności

1. **Administrator Danych (ADO)** – Dział Szkoleniowy
2. **Osoba wyznaczona ds. bezpieczeństwa informacji** odpowiada za:
   - nadzór nad przestrzeganiem Polityki,
   - reakcję na incydenty,
   - szkolenia pracowników.
3. Każdy pracownik i współpracownik ma obowiązek:

- chronić powierzone mu dane i informacje,
- stosować się do procedur określonych w Polityce,
- zgłaszać incydenty bezpieczeństwa.

---

4. Zasady nadawania i kontroli dostępu

1. Dostęp do informacji przyznawany jest zgodnie z zasadą **minimalnych uprawnień**.
2. Każda osoba posiada indywidualne konto dostępu do dysku.
3. Po zakończeniu współpracy dostęp jest niezwłocznie odbierany.

---

5. Bezpieczeństwo systemów i infrastruktury

1. Systemy informacyjne Działu Szkoleniowego są zabezpieczone:
   - oprogramowaniem antywirusowym,
   - zaporą firewall,
   - szyfrowaniem danych (AES-256, TLS 1.2+),
   - automatycznymi aktualizacjami.
2. Dane przechowywane w chmurze wykorzystywane są wyłącznie u dostawców spełniających wymogi RODO.
3. Urządzenia służbowe zabezpieczone są:
   - szyfrowaniem dysków,
   - blokadą ekranu,
   - zakazem instalowania aplikacji niezatwierdzonych przez ADO.

---

6. Zabezpieczenia fizyczne

1. Dokumenty papierowe przechowywane są:
   - w zamykanych szafach,
   - w pomieszczeniach z kontrolą dostępu.
2. Druki nadmiarowe i dokumenty niepotrzebne są niszczone w niszczarkach.

---

7. Zasady bezpiecznej komunikacji

1. Dane przekazywane są wyłącznie za pomocą:
   - szyfrowanej poczty elektronicznej (SSL/TLS),
2. Zabrania się przesyłania danych osobowych prywatnymi kontami lub poprzez niezabezpieczone kanały.

---

8. Kopie zapasowe (backup)

1. Kopie danych są wykonywane regularnie i przechowywane w odseparowanym środowisku.
2. Backupy są szyfrowane i chronione przed dostępem osób nieuprawnionych.

---

9. Szkolenia pracowników

1. Każdy pracownik oraz współpracownik przechodzi szkolenie w zakresie:
   - bezpieczeństwa informacji,
   - ochrony danych osobowych,
   - rozpoznawania zagrożeń (phishing, malware).

---

10. Zgłaszanie i obsługa incydentów

1. Incydentem bezpieczeństwa jest każde zdarzenie, które prowadzi lub może prowadzić do:
   - utraty danych,
   - nieuprawnionego dostępu,
   - naruszenia poufności, integralności lub dostępności.
2. Każdy pracownik ma obowiązek natychmiast zgłosić incydent osobie odpowiedzialnej za bezpieczeństwo.
3. Dział prowadzi **Rejestr Incydentów**.
4. W razie naruszenia danych osobowych ADO podejmuje działania zgodne z RODO, w tym:
   - analizę skutków,
   - podjęcie działań naprawczych,
   - zgłoszenie do UODO, jeśli jest wymagane.

---

11. Współpraca z podmiotami zewnętrznymi

1. Współpracujący dostawcy i partnerzy, którzy przetwarzają dane, działają na podstawie **umów powierzenia**, zgodnych z RODO.
2. Podmioty zewnętrzne mogą podlegać audytom bezpieczeństwa.

---

12. Monitorowanie i audyty

1. Organizacja prowadzi regularne przeglądy procedur bezpieczeństwa.
2. Audyty wewnętrzne i zewnętrzne są przeprowadzane zgodnie z wymaganiami SUS 3.0.
3. Wnioski z audytów są dokumentowane oraz wdrażane w formie planów naprawczych.

Poznań, 13.01.2025

13. Postanowienia końcowe

1. Polityka obowiązuje wszystkie osoby mające dostęp do danych lub informacji Działu.
2. Dokument podlega przeglądowi co najmniej raz w roku lub w przypadku wystąpienia zmian organizacyjnych, technologicznych lub prawnych.
3. Każdy pracownik potwierdza znajomość Polityki podpisanym oświadczeniem.
4. Osobą wyznaczoną do nadzoru nad. bezpieczeństwem informacji jest Dariusz Janiec – członek zarządu Działu Szkoleniowego.

Wojciech **Szalbierz**

CZŁONEK ZARZĄDU
DZIAŁ SZKOLENIOWY SPÓŁKA Z O.O.
.....
Wojciech Szalbierz
Członek Zarządu Działu Szkoleniowego

Jakub Janiec

CZŁONEK ZARZĄDU
DZIAŁ SZKOLENIOWY SPÓŁKA Z O.O.
.....
Jakub Janiec
Członek Zarządu Działu Szkoleniowego

Dariusz Janiec

CZŁONEK ZARZĄDU
DZIAŁ SZKOLENIOWY SPÓŁKA Z O.O.
.....

Dariusz Janiec
Członek Zarządu Działu Szkoleniowego