

POLITYKA BEZPIECZEŃSTWA INFORMACJI W DIAGNOSTYKA S.A.

Diagnostyka to największa sieć laboratoriów medycznych w Polsce, działająca od 1998 roku. Firma rozpoczęła działalność w Krakowie, a dziś posiada ponad 150 laboratoriów i ponad 1100 punktów pobrań na terenie całego kraju, oferując najszerszy zakres badań w Polsce. Firma obsługuje pacjentów indywidualnych oraz placówki medyczne, instytucje publiczne i firmy, wykonując rocznie ponad 200 milionów badań.

Diagnostyka zatrudnia ponad 9000 pracowników, w tym największą liczbę diagnostów laboratoryjnych w Polsce. Kluczowe laboratorium w Warszawie jest jednym z największych i najnowocześniejszych ośrodków diagnostycznych w Europie Środkowo-Wschodniej.

Firma opiera swój sukces na inwestycjach w nowoczesne technologie, automatyzację procesów oraz rozwój usług online, takich jak platforma e-commerce, umożliwiające wygodne zamawianie badań i dostęp do wyników. Diagnostyka posiada liczne certyfikaty jakości, m.in. ISO 9001, 14001, 27001 oraz akredytacje PN-EN ISO 15189 i 17025.

Zaangażowanie w zrównoważony rozwój, inwestycje w innowacje medyczne, takie jak genetyka, histopatologia czy medycyna obrazowa, a także działania na rzecz społeczności, to istotne elementy strategii firmy. Misja Diagnostyki to „*Badamy, aby pomagać ludziom dbać o zdrowie i żyć dłużej*”, a wizja firmy to wyznaczanie światowych standardów w diagnostyce i profilaktyce. Firma także aktywnie angażuje się w edukację społeczeństwa i środowiska medycznego w zakresie profilaktyki zdrowotnej.

Zarząd firmy w pełni angażuje się w realizację i utrzymanie najwyższych standardów bezpieczeństwa informacji. Poprzez wdrożenie i regularne aktualizowanie niniejszej polityki oraz wdrożonych procedur, zarząd zapewnia, że wszystkie działania związane z przetwarzaniem danych są zgodne z obowiązującymi przepisami prawnymi oraz najlepszymi praktykami w zakresie ochrony informacji. Naszym celem jest stworzenie środowiska, w którym bezpieczeństwo informacji jest priorytetem, a każdy pracownik rozumie swoją rolę w jego utrzymaniu.

W tym celu Zarząd ustanawia System Zarządzania Bezpieczeństwem Informacji (SZBI) zgodny z wymogami normy PN-ISO/IEC 27001:2022, w głównej siedzibie firmy, mieszczącej się przy ulicy Życzkowskiego 16 w Krakowie.

Cele strategiczne bezpieczeństwa informacji obejmują:

1. **zdefiniowanie Systemu Zarządzania Bezpieczeństwem Informacji** poprzez m.in: opracowanie, implementację, utrzymanie, ciągłe monitorowanie, okresowe przeglądy oraz systematyczne doskonalenie procesów;
2. **zarządzanie ryzykiem i cyberzagrożeniami** poprzez m.in: identyfikację, ocenę i zarządzanie ryzykiem związanym z bezpieczeństwem informacji, w tym ryzykiem związanym z chmurą obliczeniową i pracą zdalną oraz implementację i przestrzeganie przyjętej strategii bezpieczeństwa fizycznego oraz informatycznego;
3. **zarządzanie incydentami bezpieczeństwa** poprzez kompleksowe podejście do ich identyfikacji, zgłaszania, analizy, reagowania i eliminowania zagrożeń;
4. **zarządzanie ciągłością działania** poprzez opracowanie planów i procedur, które zapewnią utrzymanie kluczowych funkcji podczas kryzysu;
5. **ochronę aktywów informacyjnych** poprzez zapewnienie poufności, integralności i dostępności informacji z zastosowaniem Polityki Klasyfikacji Informacji oraz odpowiednich zabezpieczeń technicznych i organizacyjnych;
6. **zgodność z przepisami** poprzez przestrzeganie obowiązujących przepisów prawnych i regulacji dotyczących ochrony danych oraz zapewnienie zgodności z wymaganiami normy;
7. **podnoszenie świadomości pracowników** poprzez m.in: edukację i szkolenia w zakresie najlepszych praktyk bezpieczeństwa informacji;
8. **ciągłe doskonalenie** poprzez m.in. regularne przeglądy i aktualizacje polityki bezpieczeństwa informacji oraz procedur w celu dostosowania do zmieniających się zagrożeń i technologii.

Deklarujemy zapewnienie odpowiednich środków niezbędnych do prawidłowego funkcjonowania SZBI. Ponadto deklarujemy nasze zaangażowanie w doskonalenie SZBI oraz realizację założonych celów zgodnych z kierunkiem strategicznym i misją, firmy oraz kontekstem jej funkcjonowania.