Polityka Bezpieczeństwa Informacji

PIN BG AGH

(w wyborze)

Opis Punktu Informacji Normalizacyjnej (PIN)

Punkt Informacji Normalizacyjnej znajduje się w Bibliotece Głównej Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie. PIN gromadzi, opracowuje i udostępnia zbiory norm oraz inne polskie i zagraniczne dokumenty normatywne. PIN zapewnia dostęp do kompletu Polskich Norm i bogatego warsztatu informacyjnego – fachowej literatury i profesjonalnych baz danych.

Nasza specjalizacja

PIN prowadzi pełną obsługę użytkowników w zakresie informacji normalizacyjnej:
- prostej - dotyczącej m.in.: zbiorów norm i dokumentów normalizacyjnych, aktualności norm, zastąpień norm, cen dokumentów;
- specjalistycznej, m.in. dotyczącej powiązań Polskich Norm z normami międzynarodowymi i regionalnymi.

Kompletna oferta

PIN dysponuje zbiorem ponad 90 tysięcy norm na nośniku papierowym oraz ok. 30 tys. aktualnych Polskich Norm w wersji elektronicznej. Dostęp do tego zbioru możliwy jest wyłącznie na miejscu w Czytelni Norm. Zbiory normalizacyjne oraz bazy danych udostępniane są wszystkim zainteresowanym bezpłatnie.

Definicja bezpieczeństwa i zakres systemu

Celem Systemu Zarządzania Bezpieczeństwem Informacji w Punkcie Informacji Normalizacyjnej (PIN) w Bibliotece Głównej Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie jest zapewnienie bezpieczeństwa informacjom chronionym, zarówno własnym jak i powierzonym przez klientów, w tym danych osobowych, poprzez zapewnienie tym informacjom cech: poufności, integralności oraz dostępności.

Zakresem systemu objęte są:

- wszystkie istniejące, wdrażane obecnie lub w przyszłości systemy informatyczne oraz tradycyjne (papierowe), w których przetwarzane są lub będą informacje,
- informacje będące własnością instytucji, lub klientów instytucji, o ile zostały przekazane instytucji na podstawie umów,
- wszystkie typy nośników (np. papierowych, magnetycznych, optycznych), na których są lub będą znajdować się informacje,
- wszystkie lokalizacje – pomieszczenia, w których są lub będą przetwarzane informacje;
- wszyscy pracownicy w rozumieniu przepisów Kodeksu Pracy, praktykanci i inne osoby mające dostęp do informacji.

AKADEMIA GÓRNICZO-HUTNICZA
IM. STANISŁAWA STASZICA W KRAKOWIE

Deklaracja Dyrektora Biblioteki Głównej AGH

Bezpieczeństwo informacji oraz systemów, w których są one przetwarzane jest jednym z kluczowych elementów jakości oferowanej Klientom przez PIN oraz warunkiem ciągłego rozwoju PIN. Gwarancją sprawnej i skutecznej ochrony informacji jest zapewnienie odpowiedniego poziomu kultury bezpieczeństwa oraz zastosowanie przemyślanych rozwiązań technicznych.

Dyrektor Biblioteki Głównej AGH wprowadzając Politykę Bezpieczeństwa Informacji deklaruje, że wdrożony System Zarządzania Bezpieczeństwem Informacji będzie podlegał ciągłemu doskonaleniu zgodnie z wymaganiami normy ISO/IEC 27001. Zakres zarządzania bezpieczeństwem informacji obejmuje dane i informacje powierzone przez naszych Klientów oraz informacje własne PIN przetwarzane we wszystkich procesach.

Podejście do bezpieczeństwa informacji w PIN wywodzi się z trzech kluczowych kwestii:

- zapewnienia, że informacja jest udostępniana jedynie osobom upoważnionym (tzw. reguła poufności informacji),
- zapewnienia dokładności i kompletności informacji oraz metod jej przetwarzania (tzw. reguła integralności informacji),
- zapewnienia, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów tylko wtedy, gdy istnieje taka potrzeba (tzw. reguła dostępności informacji).

Celem wdrożonego systemu zarządzania bezpieczeństwem informacji jest osiągnięcie takiego poziomu organizacyjnego i technicznego, który:

- będzie gwarantem pełnej ochrony danych Klientów oraz ciągłości procesu ich przetwarzania,
- zapewni zachowanie poufności informacji chronionych, integralności i dostępności informacji chronionych oraz jawnych,
- zagwarantuje odpowiedni poziom bezpieczeństwa informacji, bez względu na jej postać, we wszystkich systemach jej przetwarzania,
- maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji, które wynikają z celowej bądź przypadkowej działalności człowieka oraz ich ewentualnego wykorzystania na szkodę PIN,
- zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów przetwarzania informacji,
- zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa PIN, jego interesów oraz posiadanych i powierzonych mu informacji.

Powyższe cele realizowane są poprzez:

- wyznaczenie struktury organizacyjnej zapewniającej optymalny podział oraz koordynację zadań i odpowiedzialności związanych z zapewnieniem bezpieczeństwa informacji,
- wyznaczenie właścicieli dla kluczowych aktywów przetwarzających informację, którzy zobowiązani są do zapewnienia im możliwie jak najwyższego poziomu bezpieczeństwa,
- przyjęcie za obowiązujące przez wszystkich pracowników polityk i procedur bezpieczeństwa obowiązujących w PIN,
- podział informacji na klasy i przyporządkowanie im zasad postępowania,
- określenie zasad przetwarzania informacji, w tym stref, w których może się ono odbywać,
- przegląd i aktualizację polityk i procedur postępowania dokonywanych przez odpowiedzialne osoby w celu jak najlepszej reakcji na zagrożenia i incydenty,
- ciągłe doskonalenie systemu zapewniającego bezpieczeństwo informacji, funkcjonującego w PIN zgodnie z wymaganiami normy ISO/IEC 27001 i zaleceniami wszystkich zainteresowanych stron.

Zasady ogólne

Każdy pracownik powinien być zapoznany z regułami oraz z kompletnymi i aktualnymi procedurami ochrony informacji w swojej jednostce organizacyjnej. Poniższe uniwersalne zasady są podstawą realizacji polityki bezpieczeństwa informacji:

- **Zasada uprawnionego dostępu**. Każdy pracownik przeszedł szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisał stosowne oświadczenie o zachowaniu poufności.
- **Zasada przywilejów koniecznych**. Każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań.
- **Zasada wiedzy koniecznej**. Każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań.
- **Zasada usług koniecznych**. PIN świadczy usługi zgodnie z zawartymi umowami.
- **Zasada asekuracji**. Każdy mechanizm zabezpieczający musi być ubezpieczony drugim, innym (podobnym). W przypadkach szczególnych może być stosowane dodatkowe (trzecie) niezależne zabezpieczenie.
- **Zasada świadomości zbiorowej**. Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych PIN i aktywnie uczestniczą w tym procesie.
- **Zasada indywidualnej odpowiedzialności**. Za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby.
- **Zasada obecności koniecznej**. Prawo przebywania w określonych miejscach mają tylko osoby upoważnione.
- **Zasada stałej gotowości**. System jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających.
- **Zasada najsłabszego ogniwa**. Poziom bezpieczeństwa wyznacza najsłabszy (najmniej zabezpieczony) element.
- **Zasada kompletności**. Skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji.
- **Zasada ewolucji**. Każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych.
- **Zasada odpowiedniości**. Używane mechanizmy muszą być adekwatne do sytuacji.
- **Zasada akceptowanej równowagi**. Podejmowane środki zaradcze nie mogą przekraczać poziomu akceptacji.
- **Zasada świadomej konwersacji**. Nie zawsze i wszędzie trzeba mówić, co się wie, ale zawsze i wszędzie trzeba wiedzieć co, gdzie i do kogo się mówi.