

Celem wszystkich działań Certum, jako kwalifikowanego dostawcy usług zaufania, w zakresie zapewnienia bezpieczeństwa informacji jest osiągnięcie takiego poziomu organizacyjnego i technicznego, który:

1. zapewni zachowanie:
 - a. poufności informacji – tj. zapewnienie, że informacja jest udostępniana jedynie osobom upoważnionym,
 - b. integralności informacji – tj. zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,
 - c. dostępności informacji - tj. zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy istnieje taka potrzeba;
2. zagwarantuje odpowiedni poziom bezpieczeństwa przetwarzanych informacji zarówno w systemach informatycznych, jak i papierowych,
3. istotnie ograniczy ryzyko wystąpienia zagrożeń dla bezpieczeństwa informacji,
4. zapewni poprawne i bezpieczne funkcjonowanie systemów przetwarzania informacji,
5. zapewni gotowość do podjęcia działań w sytuacjach kryzysowych.

Spójna ochrona informacji jest realizowana poprzez rozpoznanie grup informacji, które podlegać będą ochronie, systemów oraz obszaru ich przetwarzania. Wyznaczone cele w zakresie ochrony informacji osiągnięte są poprzez:

1. właściwe wyznaczenie kontekstu organizacyjnego,
2. wprowadzenie podziału na informacje jawne i chronione,
3. określenie informacji stanowiących tajemnicę firmy jako podlegających ochronie ze względu na jej dobro, interes i pozycję na rynku,
4. określenie informacji chronionych ze względu na wymogi prawne oraz oczekiwania interesariuszy wewnętrznych i zewnętrznych,
5. wprowadzenie podziału informacji chronionych na grupy i zarządzanie nimi,
6. nadawanie informacji chronionej odpowiedniej klauzuli,
7. określenie organizacyjnych i technicznych wymogów bezpieczeństwa przetwarzania grup informacji chronionych,
8. utworzenie struktur organizacyjnych odpowiedzialnych za zarządzanie bezpieczeństwem i przetwarzaniem informacji,
9. zarządzanie ciągłością przetwarzania informacji,
10. standaryzację procedur postępowania oraz opracowanie niezbędnej dokumentacji w postaci zasad zarządzania bezpieczeństwem grup informacji i systemów ich przetwarzania,
11. wdrożenie rozwiązań technicznych zapewniających wymagany poziom bezpieczeństwa przetwarzanych informacji,
12. efektywne propagowanie zasad bezpieczeństwa informacji wśród kierownictwa i pracowników,
13. podstawowe szkolenia z zakresu bezpieczeństwa informacji dla nowozatrudnionych pracowników i podwykonawców,
14. szkolenia aktualizujące wiadomości w zakresie bezpieczeństwa informacji dla pracowników i podwykonawców,
15. cykliczne przeglądy dokumentacji w ramach przeglądu systemu bezpieczeństwa informacji i audytów wewnętrznych,

16. ograniczenie ryzyka wycieku informacji, poprzez monitorowanie przepływu informacji w systemach przetwarzania.

Niniejszy dokument opisuje ogólne zasady bezpieczeństwa stosowane w Certum – jednostce organizacyjnej Asseco Data Systems S.A.

Polityka Bezpieczeństwa Certum dostępna jest na stronie internetowej Certum pod linkiem: https://www.certum.pl/pl/cert_wiedza_repozytorium_pl_en/.

Historia zmian dokumentu

Wersja	Data	Opis wersji i zmian
1.0	31 stycznia 2020	Opracowanie dokumentu.