

Polityka Bezpieczeństwa Informacji



POLITYKA BEZPIECZEŃSTWA INFORMACJI

Załącznik do uchwały Zarządu ERBUD SA nr 6/2023 z dnia 23.01.2023

§ 1

Wstęp

1. Polityka Bezpieczeństwa Informacji jest podstawowym elementem Systemu Zarządzania Bezpieczeństwem Informacji w GK ERBUD.
2. Polityka zawiera ogólne wymagania, zasady, procedury i instrukcje w zakresie ochrony informacji przetwarzanych w GK ERBUD. Polityka Bezpieczeństwa Informacji jest dokumentem nadrzędnym w stosunku do pozostałych wewnętrznych aktów dotyczących bezpieczeństwa informacji, wraz z którymi tworzy kompleksową dokumentację bezpieczeństwa.
3. Polityka Bezpieczeństwa Informacji podlega regularnej weryfikacji pod kątem aktualności, przydatności i adekwatności.

§ 2

Cel

1. W GK ERBUD ustanawia się, uwzględniające obowiązujące przepisy, zasady i wymagania w zakresie bezpieczeństwa informacji oraz wyniki analizy ryzyka oraz cele bezpieczeństwa informacji.
2. Ustanowione cele bezpieczeństwa wspierają przyjętą strategię i realizację celów GK ERBUD, jak i zadań wykonywanych przez pracowników GK ERBUD, praktykantów, stażystów, wolontariuszy oraz inne osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz podmiotów z GK ERBUD i/lub mające dostęp do aktywów informacyjnych GK ERBUD.
3. Do głównych celów bezpieczeństwa informacji w GK ERBUD należy:
 - a) zapewnienie bezpieczeństwa aktywów informacyjnych GK ERBUD (w tym ochrona wizerunku i relacji z podmiotami zewnętrznymi) zgodnie z wymogami obowiązującego prawa oraz stosownie do wyników oceny ryzyka w bezpieczeństwie informacji,

- b) usprawnienie funkcjonowania GK ERBUD poprzez uporządkowanie zasad przetwarzania informacji oraz zarządzanie aktywami informacyjnymi w zorganizowany sposób, by ułatwić doskonalenie i dostosowanie do bieżących celów GK ERBUD,
 - c) minimalizowanie ryzyka i ograniczanie skutków utraty bezpieczeństwa informacji,
 - d) podnoszenie świadomości pracowników oraz pozostałych osób i podmiotów, o których mowa w ust. 2 powyżej, w zakresie bezpieczeństwa informacji.
- 4. W ramach realizacji celów, odpowiednio do poziomu zidentyfikowanych zagrożeń, podejmowane są działania w kierunku osiągnięcia poziomu organizacyjnego i technicznego GK ERBUD, który w szczególności zapewni:
 - a) podnoszenie świadomości pracowników oraz pozostałych osób i podmiotów, o których mowa w ust. 2 powyżej, w zakresie bezpieczeństwa informacji.
 - b) integralność informacji oraz ich dostępność,
 - c) uwzględnienie dodatkowych elementów bezpieczeństwa zgodnie z wymaganiami i decyzjami oraz zapewnienie bezpiecznego przetwarzania informacji, w tym zdolność do podejmowania działań w sytuacjach kryzysowych,
 - d) udokumentowane informacje dotyczące celów bezpieczeństwa informacji i stopnia ich realizacji.
- 5. W GK ERBUD prowadzona jest okresowa ocena stopnia realizacji wyznaczonych celów bezpieczeństwa informacji.

§ 3

Zakres Systemu Zarządzania Bezpieczeństwem Informacji

- 1. Zakres ustanowionego SZBI obejmuje:
 - a) procesy oraz realizowane w GK ERBUD działania i zadania
 - b) wszelkie informacje przetwarzane w ramach ww. procesów i zadań, w tym:
 - przetwarzane w formie tradycyjnej (m.in. informacje wydrukowane lub zapisane na papierze),
 - przetwarzane w formie elektronicznej (np. przesyłane za pośrednictwem poczty elektronicznej lub urządzeń elektronicznych, elektronicznych nośników),
 - wypowiedane słownie,
 - będące własnością GK ERBUD lub innych podmiotów, o ile zostały przekazane na podstawie obowiązujących przepisów prawa lub umów.



- c) aktywa wspierające przetwarzanie informacji w ramach realizowanych w GK ERBUD działań i zadań, w tym:
- pracownicy (wszyscy pracownicy GK ERBUD bez względu na podstawę współpracy),
 - praktykanci, stażyści, wolontariusze oraz inne osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz GK ERBUD i/lub mające dostęp do aktywów informacyjnych GK ERBUD),
 - budynki i pomieszczenia GK ERBUD, w których są lub będą przetwarzane informacje, sprzęt, w tym sprzęt komputerowy, urządzenia mobilne oraz inne nośniki danych, na których znajdują się informacje podlegające ochronie, oprogramowanie, infrastruktura sieciowa,
 - technologie służące pozyskiwaniu, selekcjonowaniu, analizowaniu, przetwarzaniu, zarządzaniu i udostępnianiu informacji, do których zalicza się zarówno systemy papierowe jak i elektroniczne,
 - struktura organizacyjna.
2. Z uwagi na szczególny charakter informacji niejawnych wynikający z obowiązujących przepisów prawa, ochrona informacji niejawnych i aktywów wspierających ich przetwarzanie podlega wyłączeniu z ustanowionego SZBI.

§ 4

Podstawowe zasady bezpieczeństwa informacji

1. W celu zabezpieczenia informacji i aktywów wspierających ich przetwarzanie, w GK ERBUD wprowadza się następujące, podstawowe zasady bezpieczeństwa informacji:
- a) zasada „adekwatności zabezpieczeń” – stosowane zabezpieczenia muszą być adekwatne do zidentyfikowanych zagrożeń,
 - b) zasada „bezpiecznego przetwarzania” – przetwarzanie informacji szczególnie chronionych powinno odbywać się wyłącznie w bezpiecznych środowiskach, tj. w wydzielonych systemach informatycznych, zabezpieczonych pomieszczeniach etc.,
 - c) zasada „bezpiecznej współpracy z podmiotami zewnętrznymi” – dokumenty regulujące współpracę z podmiotami zewnętrznymi (m.in. treść umów i porozumień) zawierają zapisy dot. bezpieczeństwa informacji, w tym klauzule bezpieczeństwa o zachowaniu poufności,



- d) zasada „czystego biurka” – w celu wyeliminowania ryzyka przypadkowego lub celowego odczytania informacji, ich skopiowania, zniszczenia lub zmodyfikowania przez osoby nieuprawnione, opuszczając stanowisko pracy należy usunąć z blatu biurka dokumenty zawierające informacje inne niż informacje o charakterze jawnym, umieszczając je w przeznaczonych do tego celu zabezpieczonych meblach biurowych: szafach, szufladach lub sejfach,
 - e) zasada „czystego ekranu” – na czas nieobecności, dostęp do komputera należy skutecznie blokować a po zakończeniu pracy komputer wyłączyć,
 - f) zasada „segregacji obowiązków i zadań” – obowiązki i uprawnienia powinny być tak rozdzielone, aby jedna osoba nie dysponowała pełnią uprawnień do wykonywania zadań w całości,
 - g) zasada „uprawnionego dostępu” – korzystanie z aktywów informacyjnych GK ERBUD odbywać się może tylko w oparciu o formalne uprawnienia do korzystania z wybranych aktywów,
 - h) zasada „doskonalenia SZBI” – system zarządzania bezpieczeństwem informacji jest dostosowywany do zmieniających się warunków w oparciu o wyniki okresowo prowadzonego monitorowania i nadzoru,
 - i) zasada „wiedzy uzasadnionej” – osoby, o których mowa w § 5 dysponują wiedzą o aktywach informacyjnych w ograniczonym zakresie, niezbędnym do realizacji powierzonych im zadań.
2. Dodatkowe zasady bezpieczeństwa mogą zostać określone w pozostałych dokumentach wchodzących w skład dokumentacji bezpieczeństwa.
3. Pracownicy GK ERBUD, praktykanci, stażyści, wolontariusze oraz inne osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz GK ERBUD i/lub mające dostęp do aktywów informacyjnych GK ERBUD zobowiązani są do przestrzegania obowiązujących w GK ERBUD zasad bezpieczeństwa.

§ 5

Role i odpowiedzialność w zakresie bezpieczeństwa informacji

1. Odpowiedzialność za bezpieczeństwo informacji ponoszą wszyscy pracownicy GK ERBUD, praktykanci, stażyści, wolontariusze oraz inne ww. osoby i podmioty objęte zakresem ustanowionego SZBI.
2. Odpowiedzialność polega na przestrzeganiu wymagań prawa powszechnie obowiązującego, zapisów niniejszego dokumentu oraz pozostałych wymogów wskazanych w dokumentacji bezpieczeństwa, w szczególności na:
 - a) realizacji przypisanych zadań w obszarze bezpieczeństwa informacji



- b)** ochronie powierzonych informacji i zabezpieczeniu aktywów wspierających ich przetwarzanie,
 - c)** nieudostępnianiu informacji osobom nieuprawnionym,
 - d)** zachowaniu w tajemnicy chronionych informacji oraz sposobów ich zabezpieczenia,
 - e)** informowaniu o podejrzeniu/wszelkich zauważonych nieprawidłowościach, które mogą mieć wpływ na bezpieczeństwo informacji.
- 3.** Kadra zarządzająca GK ERBUD odpowiedzialna jest za zapewnienie zasobów niezbędnych do bieżącego funkcjonowania, utrzymania i ciągłego monitorowania oraz doskonalenia SZBI.
- 4.** W celu rozdzielenia funkcji zarządczych i kontrolnych od funkcji wykonawczych, role i odpowiedzialność w ramach ustanowionego SZBI zostały ustanowione w dwóch obszarach:
- a)** Role i odpowiedzialność w obszarze administrowania związane są przede wszystkim z utrzymaniem, bieżącym zarządzaniem i rozwojem SZBI.
 - b)** Role i odpowiedzialność w obszarze bezpieczeństwa związane są przede wszystkim z nadzorem, monitorowaniem i ciągłym doskonaleniem SZBI.

Informacje przetwarzane w GK ERBUD objęte zakresem ustanowionego SZBI klasyfikowane są w następujących grupach:

- 1)** dane osobowe (w rozumieniu przepisów dot. ochrony danych osobowych),
- 2)** tajemnice prawnie chronione (tajemnice powołane na mocy ustaw, których obowiązek ochrony wynika z ustaw),
- 3)** tajemnice GK ERBUD (informacje, których ujawnienie mogłoby narazić GK ERBUD na szkodę oraz informacje wewnętrzne udostępniane na zasadzie „wiedzy uzasadnionej”),
- 4)** informacje jawne (w tym informacje udostępniane w trybie informacji publicznej).

Dariusz Grzeszczak
Prezes Zarządu

Agnieszka Głowacka
Wiceprezes Zarządu

Jacek Leczkowski
Wiceprezes Zarządu

