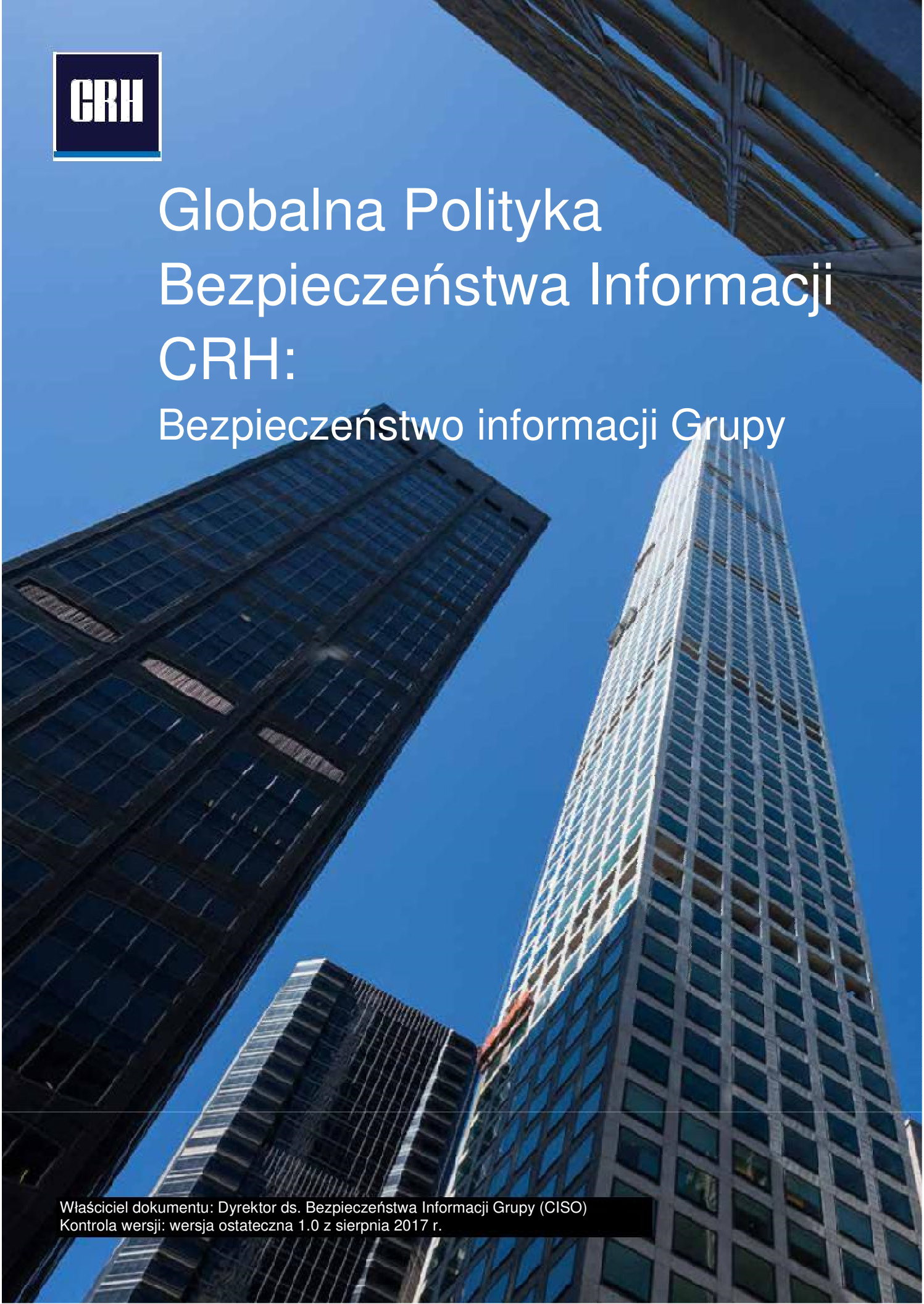


Globalna Polityka Bezpieczeństwa Informacji CRH:

Bezpieczeństwo informacji Grupy

Właściciel dokumentu: Dyrektor ds. Bezpieczeństwa Informacji Grupy (CISO)
Kontrola wersji: wersja ostateczna 1.0 z sierpnia 2017 r.

Globalna Polityka Bezpieczeństwa Informacji Grupy CRH

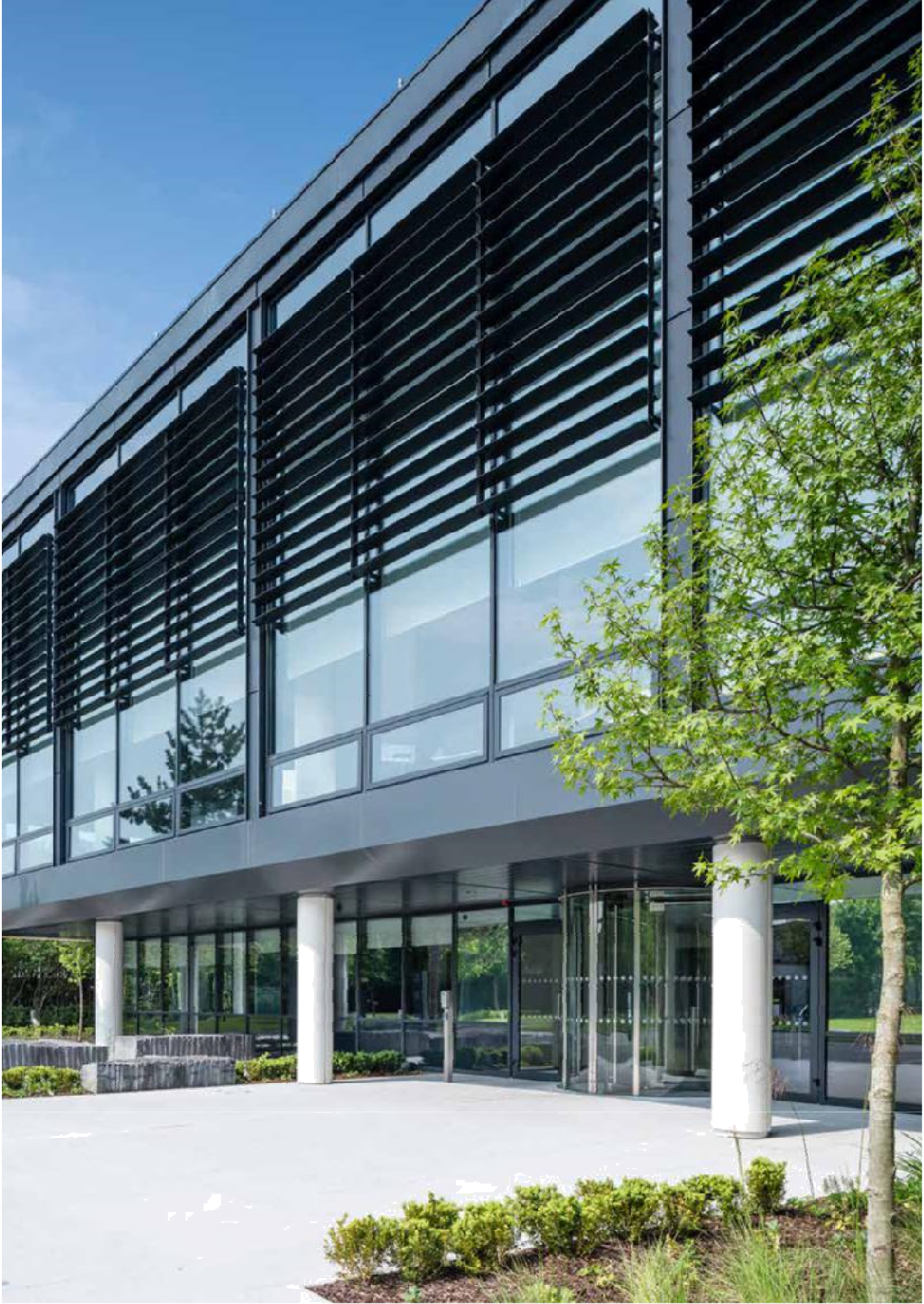
Historia wersji

Wersja	Opis zmian	Data	Zaktualizował(a)
1.0	Wersja ostateczna	listopad 2017 r.	Michael Dwyer / Dział bezpieczeństwa informacji Grupy

Zarządzanie

Zatwierdził(a)	Data zatwierdzenia
Jared Carstensen CISO	sierpień 2017 r.
Globalne kierownictwo	listopad 2017 r.

Spis treści



1. Wprowadzenie

Niniejsza Polityka stanowi wyraz ciągłego zaangażowania Grupy CRH na rzecz bezpieczeństwa w odniesieniu do poufności, integralności oraz dostępności aktywów informacyjnych CRH, a także określenia zasad odpowiedzialności za aktywa informacyjne. Ochrona takich aktywów ma zasadnicze znaczenie dla zabezpieczenia firmy, jej pracowników, akcjonariuszy oraz klientów. W ramach strategii bezpieczeństwa informacji CRH, zespół ds. bezpieczeństwa informacji Grupy dokonał gruntownego przeglądu dotychczas istniejących polityk bezpieczeństwa informacji na poziomie Grupy, celem opracowania niniejszej pojedynczego, wspólnego dla całej Grupy dokumentu - Globalnej Polityki Bezpieczeństwa Informacji.

Informacje spółek, które w niniejszym dokumencie są również nazwane „aktywami informacyjnymi", występują w wielu postaciach, od materiałów drukowanych do dokumentów przechowywanych w formie elektronicznej. Podstawowymi celami niniejszej Polityki są:

- Identyfikacja ryzyk bezpieczeństwa informacji związanych z nieuprawnionym dostępem, niewłaściwym użyciem, modyfikacją lub zniszczeniem aktywów informacyjnych, zarządzanie nimi oraz wdrożenie środków kontroli, mających na celu ograniczenie wpływu tych ryzyk,
- Zapewnienie zgodności z lokalnymi przepisami ustawowymi i regulacjami. Uwaga: jeżeli lokalne przepisy i regulacje są bardziej rygorystyczne niż środki kontroli przewidziane w niniejszej Polityce, wówczas takie lokalne przepisy i regulacje będą mieć pierwszeństwo w stosunku do niniejszej Polityki,
- Wzmocnienie i poprawa poziomu świadomości oraz dojrzałości w zakresie bezpieczeństwa informacji w skali całej spółki.

1.1 Zakres Globalnej Polityki Bezpieczeństwa Informacji

Niniejsza Polityka ma zastosowanie dla wszystkich firm działających w ramach Grupy CRH, jej spółek operacyjnych oraz osób trzecich, które zarządzają, przechowują lub przetwarzają informacje CRH. Polityka nie ma zastosowania do operacji technologicznych stosowanych w przemysłowych systemach sterowania, tzn. urządzeń w technologii SCADA wykorzystywanych w wielu naszych cementowniach. Mając na uwadze charakter globalnych cyber zagrożeń, CRH musi mieć pewność, że poziom ryzyka cybernetycznego oraz świadomość w trakcie fuzji i przejęć (*ang. M&A – Mergers & Acquisitions*) podlega należytemu rozumieniu i jest przestrzegany. Tego rodzaju ryzyka mogą mieć potencjalnie globalnie negatywny wpływ na wszystkie spółki CRH, jeśli ich identyfikacja i odpowiednie działania nie zostaną natychmiast podjęte. Niniejsza Polityka wymaga stosowania w połączeniu z dotychczas istniejącymi procedurami biznesowymi przejęć w trakcie analiz due diligence, dla zapewnienia, że nowe spółki przestrzegają i dostosowują się do Globalnej Polityki Bezpieczeństwa Informacji CRH.

Niniejsza Polityka została opracowana zgodnie z najlepszymi praktykami zawartymi w zestawie norm ISO/IEC 27000, które są wykorzystywane do zarządzania ryzykami bezpieczeństwa informacji.

Uwaga: formalna certyfikacja poszczególnych jednostek wg norm ISO nie jest obowiązkowa. Jeżeli potrzebujesz pomocy w uzyskaniu certyfikacji, prosimy o kontakt pod adresem: cyber@crh.com.

1.2 Zakres odpowiedzialności i obowiązków wynikających z Polityki

Odpowiedzialność za Globalną Politykę Bezpieczeństwa Informacji spoczywa na Dyrektorze ds. Bezpieczeństwa Informacji Grupy (CISO). Wyższe kierownictwo CRH jest odpowiedzialne za wdrożenie bezpieczeństwa informacji we wszystkich spółkach działających w Grupie CRH. Niniejsza Polityka jest sponsorowana i zatwierdzona przez CRH Global Leadership Team (globalny zespół kierowniczy CRH - GLT).

1.2.1 Obowiązki Działu Bezpieczeństwa Informacji Grupy

Dział Bezpieczeństwa Informacji Grupy (*ang. Group Information Security GIS*) może służyć doradztwem i wytycznymi poszczególnym jednostkom funkcjonalnym i spółkom operacyjnym CRH w zakresie metod środków kontroli wymaganych w niniejszej Polityce. GIS dokonuje przeglądu oraz aktualizacji niniejszej Polityki co roku lub po wystąpieniu istotnych zmian w otoczeniu rynkowym, regulacyjnym lub gospodarczym. GIS przyjmuje, opracowuje, aktualizuje i utrzymuje niniejszą Politykę z uwzględnieniem wkładu i uwag właściwych interesariuszy, zgodnie z:

- obecnie obowiązującymi międzynarodowymi standardami bezpieczeństwa;
- korporacyjnymi wymogami biznesowymi;
- ogólnymi wymogami ustawowymi i regulacyjnymi;
- ogólną strategią bezpieczeństwa informacji CRH;
- po uzyskaniu sponsorowania i zatwierdzenia ze strony wyższego kierownictwa.

1.2.2 Obowiązki kierownictwa

Poszczególne jednostki funkcjonalne CRH i kierownictwo spółek operacyjnych ponoszą odpowiedzialność za:

- zapewnienie przestrzegania Polityki oraz wymogów w niej zawartych;
- wdrożenie niniejszej Polityki i przewidzianych w niej środków kontroli;
- opracowywanie lokalnych standardów, wytycznych i procedur na potrzeby wsparcia niniejszej Polityki;

zapewnienie dostępności Polityki dla pracowników, a także w stosownych przypadkach, dla właściwych osób trzecich;

zapewnienie, że pracownicy rozumieją spoczywające na nich obowiązki w zakresie ochrony poufności, integralności i dostępności aktywów informacyjnych CRH.

1.3 Przestrzeganie Polityki

Przestrzeganie niniejszej Polityki jest obowiązkowe dla wszystkich pracowników CRH, spółek operacyjnych, podwykonawców i firm zewnętrznych, które zarządzają, przechowują lub przetwarzają aktywa informacyjne CRH. Niniejsza Polityka zostanie ogłoszona i globalnie wdrożona w całym CRH z dniem 1 stycznia 2018 r. Aby zapewnić jednak, że CRH i jej spółki operacyjne zdążą skutecznie wdrożyć środki kontroli i osiągną zgodność z niniejszą Polityką, wejdzie ona formalnie w życie z dniem 1 lipca 2018 r. Departamenty audytu wewnętrznego CRH będą dokonywać weryfikacji i potwierdzenia przestrzegania niniejszej Polityki.

1.4 Naruszenia i odstępstwa

W przypadku braku możliwości pełnego dostosowania się do wymogów zawartych w niniejszej Polityce, jeżeli;

a. jednostka funkcjonalna bądź spółka operacyjna CRH uzna, że w stosunku do niej nie ma zastosowania jeden, bądź większa liczba środków kontroli wprowadzonych w niniejszej Polityce

lub

b. w razie stwierdzenia, że nie jest możliwe wdrożenie środka kontroli w terminie do dnia 1 lipca 2018 r.

W przypadku a: zatwierdzona przez wyższe kierownictwo dokumentacja i uzasadnienie świadczące o braku lub akceptacji ryzyka muszą być poddane weryfikacji CISO, poprzez przesłanie e-mail na adres ***cyber@crh.com.***

W przypadku b: musi zostać opracowany plan naprawczy, służący zapewnieniu pełnego przestrzegania Globalnej Polityki Bezpieczeństwa Informacji. Plan musi być formalnie udokumentowany i przekazany do CISO w formie wiadomości e-mail, przesłanej na adres cyber@crh.com, celem przeglądu i zatwierdzenia.

Wszelkie umyślne, złośliwe lub mające charakter zaniedbania zachowania, prowadzące do nieprzestrzegania niniejszej Polityki, mogą skutkować wszczęciem postępowania dyscyplinarnego.

2. Uwarunkowania

2.1 Znaczenie Globalnej Polityki Bezpieczeństwa Informacji

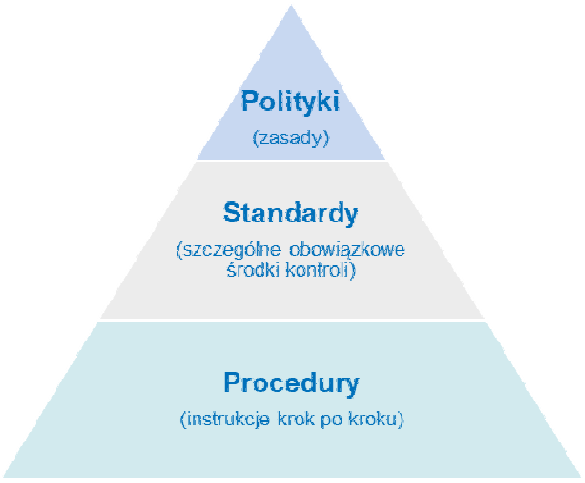
Bezpieczeństwo informacji obejmuje następujące elementy:

- Poufność – informacje są dostępne tylko dla osób upoważnionych do dostępu do nich;
- Integralność – zabezpieczona jest dokładność i kompletność informacji;
- Dostępność – informacje są dostępne wtedy, kiedy są potrzebne;
- Odpowiedzialność – gwarantowana jest identyfikacja osób, systemów i procesów dokonujących wszelkich operacji oraz gwarantowana jest rejestracja autorów i charakteru wykonywanych przez nich operacji - możliwość monitorowania (*ang. tracability*).

Globalna Polityka Bezpieczeństwa Informacji i ramowa struktura standardów

Polityki – niniejsza Globalna Polityka Bezpieczeństwa Informacji, posiada wsparcie wyższego kierownictwa CRH, obejmuje szereg istotnych deklaracji i wytycznych z zakresu ochrony informacji. Polityka określa zakresy obowiązków i odpowiedzialności, wskazuje zakres informacji podlegających ochronie oraz opisuje środki kontroli, wymagające wdrożenia dla ochrony informacji.

Standardy – na standardy składają się szczegółowo opisane obowiązkowe środki kontroli, które wprowadzają w życie i wspierają funkcjonowanie Polityki bezpieczeństwa informacji. Standardy pomagają zapewnić spójność w obszarze bezpieczeństwa informacji w całej korporacji oraz definiują środki kontroli bezpieczeństwa informacji odnoszące się do określonej technologii, sprzętu i oprogramowania. Spółki powinny opracować swoje własne standardy, stosując się do istniejących obecnie norm bezpieczeństwa (np. SANS, NIST, ISO, CIS).



Procedury – polityki, standardy i procedury razem tworzą listę środków kontroli wymagających całościowego wdrożenia. Procedury definiują kontrole na najbardziej szczegółowym poziomie. Zawierają instrukcje do wykonania krok po kroku, wspierając użytkowników we właściwym wdrożeniu środków kontroli bezpieczeństwa informacji.

Uwaga: niniejszy dokument Polityki nie zawiera standardów ani procedur. Ma na celu uzupełnienie istniejących lokalnie w spółce standardów i procedur bezpieczeństwa informacji. W przypadku braku istniejących lokalnych standardów lub procedur, spółki powinny zwrócić się o pomoc do GIS, na adres cyber@crh.com, celem określenia, jakie standardy powinny spełniać.

3. Organizacja bezpieczeństwa informacji

3.1 Odpowiedzialność i obowiązki z zakresu bezpieczeństwa i ochrony informacji

- Obowiązki z zakresu czynności zarządzania ryzykiem bezpieczeństwa informacji oraz akceptacji ryzyka rezydualnego powinny podlegać dokumentacji zgodnie z uznaną normą, np. ISO/IEC 27005: 2011.
- Nadzór nad bezpieczeństwem i ochroną informacji w odniesieniu do dostawców, którzy zarządzają, przechowują lub przetwarzają informacje spółek, powinien być zidentyfikowany i udokumentowany.
- W celu zmniejszenia ryzyka nieuprawnionej lub niezamierzonej modyfikacji bądź niewłaściwego użycia aktywów informacyjnych CRH, konfliktujące się ze sobą obowiązki i zakresy odpowiedzialności powinny być zidentyfikowane i rozdzielone - segregacja obowiązków (*ang. SoD*).
- Utworzenia wymaga lista prawomocnych organów i kontaktów właściwych dla spraw bezpieczeństwa informacji w celu ułatwienia komunikacji, podczas sytuacji awaryjnych (tzn. incydent z zakresu bezpieczeństwa lub katastrofa), bądź gdy niezbędna jest zewnętrzna pomoc, tzn. lokalnych organów ścigania lub regionalnego inspektora ds. ochrony danych.

3.2 Bezpieczeństwo i ochrona informacji w zarządzaniu projektami

Zagadnienia bezpieczeństwa informacji muszą być uwzględniane we wszystkich fazach cyklu zarządzania projektem a zwłaszcza w przypadku projektów związanych z poufnością, integralnością i dostępnością informacji spółki lub danych osobowych.

3.3 Regulamin w sprawie urządzeń mobilnych i pracy zdalnej

- Wszystkie służbowe laptopy muszą być zaszyfrowane przy użyciu uznanych w branży standardów szyfrowania. Pozostałe służbowe urządzenia, dla których dostępne jest szyfrowanie, tzn. tablety i smartfony, muszą mieć uruchomione technologie szyfrowania.
- Użytkownicy nie powinni mieć prawa instalacji niezatwierdzonego oprogramowania ani dokonywania zmian istniejących ustawień i konfiguracji urządzeń. Zmiany te powinny być możliwe do wykonania wyłącznie przez upoważniony personel IT.
- Dostęp do informacji spółki z poziomu urządzenia użytkownika może odbywać się jedynie przy użyciu lokalnie zatwierdzonych mechanizmów.
- Urządzenia muszą być utrzymywane zgodnie z wymogami zatwierdzonych lokalnie standardów w zakresie sprzętu, oprogramowania i bezpieczeństwa.
- Wszystkie urządzenia muszą posiadać zainstalowany zatwierdzony program antywirusowy.
- Urządzania służbowe, na których przechowuje się informacje spółki, wymagają wdrożenia środków kontroli poprawności wykonania backupów.
- Treści związane z użytkowaniem urządzeń służbowych, przez użytkowników powinny być objęte lokalnym programem podnoszenia świadomości bezpieczeństwa informacji w celu:
    - podniesienia poziomu świadomości zagrożeń związanych z urządzeniami użytkownika, w tym bezpieczeństwa fizycznego i złośliwego oprogramowania;
    - poinformowania o procedurach i konieczności jak najszybszego zgłaszania zgubionych lub skradzionych urządzeń w celu zablokowania konta użytkownika i w stosownych wypadkach uruchomienia zdalnego usunięcia danych.

3.3.1 Praca zdalna

Jeżeli dozwolona jest praca zdalna (w charakterze tymczasowym lub stałym), należy wdrożyć dodatkowe środki kontroli, celem ochrony informacji udostępnianych, przetwarzanych lub przechowywanych w miejscach pracy zdalnej. Do takich środków kontroli należą:

- upoważnienie i zatwierdzenie pracy zdalnej przez kierownictwo;
- fizyczne zabezpieczenie służbowych aktywów informacyjnych, znajdujących się poza zakładem, np. zamykane na klucz szafki, zamykane na klucz drzwi;
- właściwe zabezpieczenia i urządzenia telekomunikacyjne realizujące bezpieczny zdalny dostęp, tzn. wirtualne sieci prywatne (ang. VPN) lub inne podobne;
- wymóg korzystania tylko ze służbowych urządzeń do łączenia się z sieciami spółki, z wyjątkiem przypadku:
    - dostępu do webowej poczty elektronicznej i webowych aplikacji internetowych, np. webowa wersji programu Outlook;
    - korzystanie z technologii zabezpieczonego zdalnego dostępu lub innych podobnych.

3.3.2 Prywatne urządzenia mobilne i stacjonarne

- Prywatne urządzenia mobilne, w tym smartfony, tablety, laptopy i inne urządzenia przenośne, nie mogą być wykorzystywane do przechowywania służbowych danych, chyba, że w charakterze wyjątku zostały wyraźnie zgłoszone i zatwierdzone do użytkowania w tym celu przez lokalne kierownictwo.
- Wszystkie urządzenia i systemy operacyjne, dla których dostępne jest oprogramowanie antywirusowe, muszą mieć zainstalowany zatwierdzony program antywirusowy.

4. Bezpieczeństwo i ochrona informacji z zakresu zasobów ludzkich

4.1 Weryfikacja

Odpowiednie weryfikacje, zgodnie z właściwymi przepisami i regulacjami, powinny być wykonywane przez Dział Zasobów ludzkich, bądź odpowiednie osoby trzecie w odniesieniu do zatrudnianych kandydatów. Weryfikacje te są obowiązkowe w przypadku stanowisk dotyczących dostępu do aktywów informacyjnych o wysokiej wartości, tzn. dane finansowe, informacje z zakresu fuzji i przejęć.

4.2 Obowiązki kierownictwa

- Kierownictwo musi wymagać od wszystkich pracowników stosowania się do zasad bezpieczeństwa informacji zgodnie z przyjętymi w całej firmie politykami i procedurami, tzn. dotychczas obowiązującymi zasadami zaznajamiania się i akceptacji.
- Pracownicy spółek powinni przechodzić szkolenia, których celem jest podniesienie świadomości bezpieczeństwa informacji, stosownie do powierzonych im obowiązków.
- Każda umowa z pracownikami powinna regulować obowiązki pracownika i spółki w zakresie bezpieczeństwa informacji oraz odpowiedzialność pracownika za przestrzeganie zasad bezpieczeństwa informacji i sposobu użytkowania aktywów informacyjnych spółki.

Uwaga: na potrzeby niniejszej Polityki pod pojęciem „pracownik” rozumie się także osoby fizyczne świadczące stale usługi na rzecz spółki

5. Zarządzanie aktywami informacyjnymi

5.1 Nabywanie aktywów informacyjnych

Nabywanie aktywów informacyjnych musi odbywać się zgodnie z poniższymi wymogami:

- zakupy aktywów sprzętowych i oprogramowania wymagają zatwierdzenia przez zespół ds. zaopatrzenia; w przypadku braku lokalnego zespołu ds. zaopatrzenia, zatwierdzenie należy uzyskać od lokalnego kierownictwa;
- wnioski o nabycie aktywów muszą być właściwie udokumentowane, zaakceptowane zamówienie zakupu lub zaakceptowane zapotrzebowanie przekazane do zatwierdzenia przez odpowiedni organ zakupowy, tzn. departament zaopatrzenia;
- bezpieczeństwo informacji powinno być analizowane przy zakupach wszelkiego rodzaju systemów, sprzętu lub oprogramowania.

5.2 Odpowiedzialność za aktywa informacyjne

Wszelkie logiczne i fizyczne aktywa informacyjne muszą posiadać wskazanego właściciela i muszą podlegać należytej rejestracji w rejestrze aktywów informacyjnych. Wszyscy użytkownicy muszą być świadomi tego, do jakich informacje posiadają dostęp; ma to służyć zapewnieniu, że wszelkie aktywa informacyjne (użytkowane lub wycofane z użytkowania) w CRH podlegają odpowiedniemu rozliczeniu.

5.3 Licencje na oprogramowanie

Zagwarantowanie zgodności i braku naruszeń praw autorskich w odniesieniu do licencjonowanego oprogramowania wymaga właściwej rejestracji wszystkich informacji licencyjnych. Zasady w odniesieniu do oprogramowania:

- wszelkie ujawnione, niezatwierdzone lub nielicencjonowane oprogramowanie wymaga zgłoszenia do kierownictwa IT i usunięcia w trybie natychmiastowym;
- należy wdrożyć środki kontroli służące zarządzaniu licencjami i oprogramowaniem w celu rejestracji i monitorowania liczby zainstalowanych kopii licencjonowanego oprogramowania celem zagwarantowania, że nie przekracza ona ograniczeń wynikających z umowy licencyjnej.

5.4 Wycofanie aktywów informacyjnych po upływie terminu ważności

Gdy składnik aktywów informacyjnych osiągnie koniec swojego cyklu życia, wówczas wymaga wycofania z użytkowania i usunięcia w sposób bezpieczny oraz kontrolowany. Podczas wycofania składnika aktywów z użytkowania:

- wszystkie dane znajdujące się na nim należy w sposób trwały usunąć; wszelkie elementy identyfikujące składnik aktywów jako należący do CRH należy również usunąć (tj. oznaczenia, etykiety);
- rejestr aktywów wymaga aktualizacji, celem odzwierciedlenia zmiany statusu składnika aktywów wycofywanego z użytkowania.

5.5 Klasyfikacja informacji

5.5.1 Klasyfikacja informacji

Logiczne (systemowe) i fizyczne (papierowe) aktywa informacyjne powinny podlegać klasyfikacji pod kątem wymagań prawnych, wartości i podatności na nieuprawnione ujawnienie lub modyfikację.

5.5.2 Oznakowanie aktywów informacyjnych

Odpowiedni zestaw procedur oznakowania informacji powinien zostać opracowany i wdrożony zgodnie ze schematem klasyfikacji informacji.

5.5.3 Postępowanie z aktywami informacyjnymi

- Procedury postępowania z aktywami informacyjnymi (tj. w zakresie dostępu, przechowywania i archiwizacji, dystrybucji i transmisji, powielania, usuwania i niszczenia) powinny zostać opracowane i wdrożone zgodnie z przyjętym schematem klasyfikacji informacji.
- Użytkownicy powinni być przeszkoleni w zakresie postępowania z informacjami w zależności od wdrożonego schematu klasyfikacji.

Uwaga: projekt służący klasyfikacji danych korporacyjnych uruchomiono w Grupie CRH w 2017 r. Do czasu jego pełnego wdrożenia oczekuje się, że jednostki funkcjonalne CRH i spółki operacyjne będą stosować swoje własne schematy klasyfikacyjne.

5.6 Akceptowalne korzystanie ze sprzętu komputerowego

- Pracownicy CRH i zewnętrzni pracownicy mają zakaz realizacji którejkolwiek z poniższych czynności:
  - umyślne powodowanie szkody w systemach spółki lub systemach osób trzecich;
  - skanowanie systemów lub wykorzystywanie luk lub podatności na zagrożenia w systemach informacyjnych należących do CRH lub osób trzecich, z wyłączeniem sytuacji, gdy została uprzednio udzielona odpowiednia zgoda wyższego kierownictwa lub działu bezpieczeństwa informacji Grupy;
  - wymiana plików, cyfrowych filmów, oprogramowania lub wszelkich innych materiałów licencjonowanych lub chronionych prawami autorskimi, w przypadku których CRH lub użytkownik nie posiada licencji ani zezwolenia na korzystanie z praw autorskich.

- Wszyscy pracownicy spółki oraz pracownicy zewnętrzni mają zakaz instalowania poniżej wymienionej infrastruktury technicznej bez formalnej zgody lokalnego wyższego kierownictwa lub lokalnego przedstawiciela ds. bezpieczeństwa informacji:
  - sieci lokalne (LAN), sieci rozległe (WAN), punkty dostępu bezprzewodowego (WAP);
  - serwery, sieciowe pamięci masowe (SAN);
  - urządzenia sieciowe i urządzenia bezpieczeństwa IT, takie jak przełączniki, routery, modemy i zapory sieciowe (ang. firewall);
  - oprogramowanie lub inne technologie umożliwiające zdalny dostęp do istniejących wewnętrznych sieci, systemów lub komputerów użytkowników.

6. Kontrola dostępu

6.1 Wymagania biznesowe w zakresie kontroli dostępu

- Środki kontroli dostępu powinny uwzględniać poniższe zasady:
  - Zasada najmniejszych uprawnień: użytkownikom należy przyznawać jedynie minimalny poziom uprawnień i dostępu niezbędny do wykonywania ich obowiązków służbowych.
  - Zasada bezwzględnie potrzebnej wiedzy: użytkownikom przyznaje się dostęp tylko do informacji potrzebnych im do wykonywania ich obowiązków służbowych.
- Zasady kontroli logicznego i fizycznego dostępu, powinny być zdefiniowane, stosownie do poziomu ryzyka związanego z każdym składnikiem aktywów informacyjnych.
- Prawa dostępu muszą być właściwie zarządzane, tj. wnioski o dostęp, formalne zezwolenia, rezerwacje zasobów, delegowanie, anulowanie i monitorowanie dostępu muszą być zgodne z zasadą rozdziału obowiązków (ang. SoD).
- Dostęp do systemów i informacji spółki, powinien być ograniczony do uprawnionych pracowników, zewnętrznych podwykonawców lub konsultantów, w oparciu o właściwe zatwierdzenia.
- W przypadku przejścia użytkownika na nowe stanowisko w ramach spółki, jego prawa dostępu powinny podlegać przeglądowi pod kątem nowych obowiązków i w razie potrzeby cofnięte.
- Dostęp innych osób (np. personel ochrony, obsługa infrastruktury, catering) wymaga formalnej zgody lokalnego kierownictwa spółki.

6.2 Zarządzanie dostępem użytkowników

6.2.1 Rejestrowanie i wyrejestrowywanie użytkowników

- Formalny proces rejestracji i wyrejestrowywania użytkowników należy wdrożyć celem zarządzania, przyznawania praw dostępu do systemów, aplikacji i sieci spółki, tj. pracowników nowo przyjętych, przeniesionych i odchodzących. Proces musi obejmować następujące elementy:
  - unikalne identyfikatory użytkownika na potrzeby skutecznej identyfikacji użytkowników;
  - natychmiastowa dezaktywacja kont użytkowników w przypadku pracowników opuszczających organizację;
  - okresowa weryfikacja i dezaktywacja zbędnych kont;
- Katalogi, sieci i systemy powinny być regularnie konfigurowane w taki sposób, by umożliwiać dezaktywację nieaktywnych kont.

6.2.2 Konfiguracja dostępu użytkowników

- Formalny proces konfiguracji dostępu użytkowników musi zostać wdrożony celem zatwierdzania lub wycofywania praw dostępu i uprawnień dla wszystkich typów użytkowników, do wszystkich systemów i usług.
- Dostęp powinien podlegać zatwierdzeniu przez osobę odpowiedzialną za dany system informacyjny lub usługę.
- Poziom przyznanego dostępu powinien podlegać weryfikacji zgodnie z lokalnymi zasadami kontroli dostępu i być spójny z pozostałymi wymaganiami takimi jak:
  - Zasada rozdziału obowiązków, zasada najmniejszych uprawnień i zasada bezwzględnie potrzebnej wiedzy.
  - Dostępu osobom trzecim udziela się tylko w uzgodnionym trybie tymczasowym.
  - Prawa dostępu i uprawnienia nie powinny być przydzielane zanim proces zatwierdzenia zostanie zakończony.
- Centralny rejestr praw dostępu i uprawnień nadanych poszczególnym identyfikatorom użytkowników w zakresie dostępu do systemów informacyjnych i usług musi być należycie prowadzony i regularnie aktualizowany.

6.2.3 Zarządzanie uprzywilejowanymi prawami dostępu

- Przydzielanie i nadawanie uprzywilejowanych praw dostępu powinno być ograniczone i nadzorowane poprzez formalny proces zatwierdzania.
- Uprzywilejowane prawa dostępu powinny być ograniczone i udzielane użytkownikom tylko zgodnie z zasadą przydzielania najmniejszych uprawnień zgodnie z polityką kontroli dostępu (tzn. z uwzględnieniem minimalnego zakresu uprawnień wymaganego do realizacji obowiązków służbowych).
- Dostęp administracyjny powinien zawsze posiadać zdefiniowany termin wygaśnięcia uprawnień sięgający 90 dni lub mniej, żeby zapobiec posiadaniu bezterminowego uprzywilejowanego dostępu.
- Wykonywanie czynności biznesowych nie powinno być prowadzone przy użyciu kont uprzywilejowanych.
- Konta uprzywilejowane nigdy nie powinny być udostępniane.
- Uprzywilejowane konta użytkowników i aktywność na nich powinny podlegać regularnym weryfikacjom.
- Należy opracować i stosować właściwe procedury w celu uniknięcia nieuprawnionego użycia systemowych kont administracyjnych.
- W przypadku systemowych kont administracyjnych informacje uwierzytelniające muszą być utrzymywane w sposób zabezpieczony.

6.2.4 Zarządzanie danymi uwierzytelniającymi użytkowników

- Przekazywanie danych uwierzytelniających powinno odbywać się drogą formalnego procesu zarządzania.
- Użytkownicy powinni potwierdzać znajomość spoczywającego na nich obowiązku zabezpieczenia osobistych informacji uwierzytelniających.
- Tożsamość użytkownika musi podlegać weryfikacji przed przekazaniem zmienianych lub tymczasowych danych uwierzytelniających.
- Domyślne uwierzytelnienia nowo zainstalowanego oprogramowania lub systemów muszą podlegać zmianie przed ich wdrożeniem.

6.2.5 Przegląd praw dostępu użytkowników

- Prawa dostępu użytkowników powinny być definiowane i przydzielane zgodnie z wcześniej określonymi profilami stanowiskowymi i zasadą rozdziału obowiązków (np. użytkownik w obszarze rachunkowości uzyskuje dostęp z prawem do odczytu i zapisu w katalogu sieciowym systemu rachunkowości).
- Właściciele aktywów powinni dokonywać przeglądu praw dostępu użytkowników do sieci i krytycznych systemów, przynajmniej raz w roku, zgodnie z biznesowymi wymogami przeglądu praw dostępu.
- Zezwolenia na uprzywilejowane prawa dostępu powinny podlegać przeglądowi, zgodnie z zapisami umów, wymogami prawnymi lub wymogami ograniczania ryzyka.
- Wszystkie konta niezwiązane z uprawnionym procesem biznesowym lub właścicielem muszą podlegać blokowaniu.

6.2.6 Usuwanie lub zmiana praw dostępu

- Standardy i procedury z jasno określonymi zakresami obowiązków i odpowiedzialności powinny zostać ustalone w celu zapewnienia, że prawa dostępu użytkowników są terminowo wycofywane, gdy nie są już potrzebne.
- Właściwy proces powinien zostać wdrożony na potrzeby usuwania kont po określonym czasie zgodnie z lokalnymi przepisami lub lokalną polityką przechowywania danych.

6.3 Obowiązki użytkowników

Użytkownicy muszą być świadomi swoich obowiązków w zakresie ochrony danych uwierzytelniających, w tym:

- obowiązku utrzymania poufności haseł i niedzielenia się nimi z nikim i w żadnych okolicznościach;
- nieużywania tych samych haseł do celów służbowych i prywatnych;
- wyboru hasła, które spełnia lub przewyższa wymagania regulaminu haseł CRH.

6.4 Dostęp do sieci i usług sieciowych

- Użytkownicy powinni mieć przyznany dostęp jedynie do sieci i usług, które zostały precyzyjnie określone, a dostęp zatwierdzony zgodnie z przyjętymi politykami i procedurami kontroli dostępu.
- Dostęp do usług sieciowych powinien podlegać zatwierdzeniu przez kierownictwo.

6.5 Zarządzanie hasłami użytkowników końcowych

Minimalne wymagania dotyczące haseł są następujące:

- hasła muszą być złożone* – muszą składać się z co najmniej 8 znaków (bez powszechnie znanych nazw ani wyrażeń);
- hasła do ogólnych kont użytkowników muszą być zmieniane co najmniej raz na 30 dni;
- hasła podwykonawców i pracowników tymczasowych muszą być konfigurowane w sposób zapewniający automatyczne wygasanie;
- historia haseł musi być rejestrowana w sposób systematyczny, zaś ponowne wykorzystanie hasła musi być zakazane w odniesieniu do co najmniej trzech wcześniejszych haseł;
- hasła do kont użytkowników muszą być zmieniane po pierwszym logowaniu;
- hasła nie powinny być przechowywane, chyba że mechanizm przechowywania jest zatwierdzony i przewiduje środki kontroli bezpieczeństwa oraz podlega potwierdzeniu przez Dział bezpieczeństwa informacji Grupy.

** Złożone hasła muszą zawierać znaki z co najmniej trzech z następujących czterech kategorii:*

Opis	Przykład
Wielkie litery	A, B, C ... Z
Małe litery	a, b, c ... z
Cyfry	0, 1, 2 ... 9
Znaki niealfanumeryczne („znaki specjalne”)	Znaki interpunkcyjne i inne symbole

7. Szyfrowanie

7.1 Środki ochrony kryptograficznej

- Wszystkie służbowe laptopy muszą być zabezpieczone w trybie szyfrowania.
- Wszystkie informacje zapisane na służbowych przenośnych urządzeniach multimedialnych (tzn. laptopach, smartfonach i przenośnych pamięciach masowych) muszą podlegać zabezpieczeniu w trybie szyfrowania.
- Hasła powinny być chronione podczas przesyłania przez sieć przy użyciu najnowszych środków szyfrujących odpowiadających najlepszym praktykom w branży.
- We wszelkiej komunikacji, w której przekazuje się służbowe informacje ze strefy zaufanej (tzn. wewnętrzne sieci korporacyjne) do strefy częściowo zaufanej lub niezaufanej (np. zewnętrzny dostawca usług chmurowych) należy korzystać z szyfrowania.
- Wiadomości e-mail powinny być szyfrowane przy użyciu najnowszych standardów odpowiadających najlepszym praktykom w branży.
- Dane przesyłane za pośrednictwem sieci bezprzewodowej powinny być szyfrowane zgodnie z obowiązującymi standardami bezpieczeństwa odpowiadającymi najlepszym praktykom.
- Sesje tunelowe zdalnego dostępu również muszą być szyfrowane.

7.2 Zarządzanie kluczami

- Wszystkie klucze szyfrujące muszą być chronione przed nieuprawnionym dostępem, ujawnieniem, zmianą i utratą.
- Sprzęt używany do generowania, przechowywania i archiwizacji kluczy musi podlegać fizycznej ochronie.
- Daty aktywacji i dezaktywacji kluczy muszą być zdefiniowane.

8. Bezpieczeństwo fizyczne i środowiskowe

8.1.1 Obszary bezpieczeństwa fizycznego

- Parametry bezpieczeństwa fizycznego powinny zostać należycie określone w celu ochrony obszarów, które zawierają służbowe dane i obiekty, w których są przetwarzane informacje , tzn. biura, serwerownie, centra danych.
- Procedury i środki kontroli bezpieczeństwa fizycznego służące ochronie obiektów, w których są przetwarzane informacje powinny podlegać corocznemu przeglądowi i aktualizacji.
- Należy ustanowić procedury dostępu dla każdego obiektu. Procedury powinny co najmniej określać, co najmniej:
  - godziny dostępu dla pracowników, podwykonawców i gości, np. 24/7;

- zasady wydawania identyfikatorów dla pracowników i gości;
- zasady rejestracji wszystkich gości, w tym czasu ich wejścia i wyjścia z obiektów;
- zasady instalacji zamków lub czytników kart dostępu we wszystkich punktach wejścia do obiektów i pomieszczeń zawierających systemy bezpieczeństwa, IT i łączności;
- zasady instalacji zamków w szafkach i innych urządzeniach wykorzystywanych do przechowywania informacji o wysokiej wartości;
- gościom, w tym personelowi realizującemu dostawy do obiektów spółki, podczas pobytu na terenie spółki powinien towarzyszyć pracownik. Jeżeli gość odwiedza obszar, w którym przechowuje lub przetwarza się aktywa informacyjne o wysokiej wartości, wówczas obecność pracownika jest obowiązkowa.

8.1.2 Ochrona przed zagrożeniami o charakterze fizycznym i środowiskowym

Fizyczna ochrona przed klęskami żywiołowymi, złośliwymi atakami i wypadkami powinna być należycie wdrożona. Ryzyko związane z każdą z potencjalnie zagrożonych lokalizacji wymaga należytego rozważenia, w tym zagrożenia związane z klęskami żywiołowymi i czynnikami ryzyka ludzkiego, tzn. przestępstwa, zamieszki, terroryzm.

8.1.3 Strefy dostaw i załadunku

Celem uniknięcia nieuprawnionego dostępu, punkty dostępowe takie jak strefy dostaw i załadunku oraz inne punkty, przez które nieupoważnione osoby mogą wejść do pomieszczeń spółki, powinny podlegać kontroli oraz w miarę możliwości powinny zostać oddzielone od obiektów, w których odbywa się przetwarzanie danych.

8.2 Bezpieczeństwo sprzętu komputerowego

8.2.1 Lokalizacja i ochrona sprzętu komputerowego

Sprzęt komputerowy powinien być chroniony w celu zmniejszenia ryzyka związanego z zagrożeniami środowiskowymi i nieuprawnionym dostępem, tj. poprzez uniemożliwienie podejrzenia informacji zza pleców poprzez wykorzystanie ochraniacza ekranu.

8.2.2 Urządzenia i systemy wspierające

- Sprzęt powinien być chroniony przed awariami zasilania i innymi zakłóceniami spowodowanymi przez awarie urządzeń w obiektach wspomagających. W odniesieniu do urządzeń i obiektów wspomagających fizyczne środki kontroli, takie jak ciągłość zasilania, ogrzewania, wentylacji i klimatyzacji, oraz logiczne środki kontroli dostępu powinny zostać wdrożone.
- Kable elektryczne i telekomunikacyjne wykorzystywane do transmisji danych i usług informacyjnych powinny być zabezpieczone przed przechwyceniem danych, zakłóceniami lub uszkodzeniami.

8.2.3 Polityka czystego biurka i czystego ekranu

Należy wdrożyć politykę czystego biurka i czystego ekranu obejmującą następujące elementy:

- Komputery i terminale, kiedy pozostają bez nadzoru, powinny być pozostawiane w stanie wylogowanym lub chronione przy użyciu mechanizmu blokowania ekranu i klawiatury za pomocą hasła.
- Urządzenia użytkownika powinny być konfigurowane w taki sposób, że wygaszacze ekranu zabezpieczone hasłami są automatycznie uruchamiane po upływie określonego czasu, np. 5 minut.
- Służbowe informacje o wysokiej wartości powinny być możliwie jak najszybciej usuwane z drukarek i kserokopiarek.
- Wszystkie dokumenty fizyczne muszą być usuwane z biurek na koniec każdego dnia.
- Informacje o wysokiej wartości nie powinny być nigdy pozostawiane bez nadzoru na biurkach lub w otwartych przestrzeniach biurowych.

9. Bezpieczeństwo użytkowania komputerów

9.1 Zarządzanie zmianą i potencjałem systemów IT

- Wykonywanie zmian w procesach biznesowych spółki, obiektach w których są przetwarzane informacje, systemach które mają wpływ na bezpieczeństwo informacji, powinno być kontrolowane poprzez zarządzany procesu zmiany, ze stosownymi zatwierdzeniami.
- Wykorzystywanie zasobów IT powinno być monitorowane, dopasowywane i prognozowane celem zapewnienia właściwej wydajności i dostępności systemów IT w wymaganym czasie.

9.2 Rozdzielenie środowiska programistycznego, testowego i produkcyjnego

Środowiska programistyczne i testowe muszą być logicznie i/lub fizycznie oddzielone od środowisk produkcyjnych, żeby zmniejszyć ryzyko nieuprawnionego dostępu lub wykonania zmian w środowisku produkcyjnym.

9.3 Ochrona przed złośliwym oprogramowaniem

- Środki kontroli mające na celu wykrywanie, zapobieganie i zapewnienie możliwości odtworzenia systemów dla ochrony przed złośliwym oprogramowaniem powinny być należycie wdrążone, tzn. narzędzia antywirusowe lub usługi wykrywania włamań.
- Wszystkie urządzenia mobilne, dla których dostępne jest oprogramowanie antywirusowe, muszą mieć zainstalowane rozwiązanie antywirusowe z aktualizacją do poziomu najnowszych sygnatur.
- Szkolenia użytkowników podnoszące świadomość bezpieczeństwa, powinny być przeprowadzane co najmniej raz w roku celem zapewnienia, że użytkownicy są świadomi zagrożeń. Kierownictwo powinno monitorować skuteczność tych szkoleń.
- Systemy, urządzenia i nośniki danych, przekazywane użytkownikom do pracy, powinny posiadać ochronę przed złośliwym oprogramowaniem, poprzez instalację zatwierdzonego, centralnie zarządzanego programu zabezpieczającego przed złośliwym oprogramowaniem. Program zabezpieczający powinien wykonywać skanowania obejmujące:
  - wszelkie pliki otrzymane za pośrednictwem sieci z Internetu lub za pośrednictwem nośników wymiennych w jakiejkolwiek formie, natychmiast po ich podłączeniu, tzn. oprogramowanie antywirusowe potrafi wykryć złośliwe oprogramowanie na nośnikach wymiennych;
  - załączniki do wiadomości e-mail oraz pliki pobierane z Internetu.
- Pełne skanowania systemu pod kątem wirusów, muszą być realizowane w regularnych odstępach czasu, co najmniej raz w tygodniu, żeby uwzględnić wszystkie pliki w systemie.
- Sygnatury i silniki programów chroniących przed złośliwym oprogramowaniem w systemach i urządzeniach użytkowników, powinny być aktualizowane możliwie jak najszybciej.
- Urządzenia i systemy użytkowników powinny być konfigurowane w taki sposób, żeby uniemożliwić automatyczne otwieranie/wyświetlanie treści z urządzeń przenośnych po ich podłączeniu, tzn. poprzez wyłączenie makr i plików wykonywalnych.
- Korzystanie z pamięci przenośnych nie wykorzystywanych do celów służbowych, powinno być uniemożliwione.
- Należy wdrożyć środki kontroli, które pozwalają wykrywać i/lubi blokować dostęp do znanych lub podejrzanych złośliwych stron internetowych (tzw. czarna lista- ang. black list).
- Oprogramowanie, które zapewnia funkcjonalność filtrowania na poziomie systemu operacyjnego, powinno być włączone i używane do ograniczania komunikacji przychodzącej i wychodzącej, tj. zapory sieciowe systemu Windows, HIDS/HIPS.
- Komunikacja przychodząca i wychodząca (np. WWW, FTP/sFTP, SSH i ruch w komunikatorach) powinna być monitorowana pod kątem zagrożeń bezpieczeństwa, nadużyć w wymianie danych lub prób dostępu do znanych złośliwych internetowych linków, domen i adresów IP.

9.4 Kopie zapasowe danych

Polityki i procedury tworzenia kopii zapasowych, definiujące wymogi czasowe przechowywania i ochrony informacji muszą być ustanowione.

- Zadanie (*ang. job*) tworzenia kopii zapasowej, musi obejmować co najmniej informacje biznesowe o znaczeniu krytycznym, aby można było przywrócić je po awarii.
- Informacje i dane operacyjne powinny być archiwizowane w celu ochrony przed przypadkowym usunięciem lub utratą.
- Kopie zapasowe powinny być wykonywane okresowo. Zakres (tzn. pełna lub przyrostowa kopia zapasowa) oraz częstotliwość wykonywania kopii zapasowych, powinny spełniać wymagania biznesowe w zakresie okresu dostępności danych (*ang. data retention*) i możliwości odtworzenia danych (*ang. data recovery*) oraz stopień krytyczności informacji z punktu widzenia zapewnienia ciągłości i kontynuacji działalności biznesowej.
- Procesy odtwarzania danych z kopii zapasowej powinny podlegać regularnym testom w celu zagwarantowania, że można na nich polegać w sytuacji awaryjnej.
- Kopie zapasowe powinny być właściwie zabezpieczone zgodnie ze schematem klasyfikacji informacji i postępowania z nimi.
- Nośniki kopii zapasowych osiągające koniec cyklu swojego życia, powinny być usuwane lub niszczone w drodze formalnych procesów, zgodnie z lokalnymi wymogami w zakresie postępowania i przechowywania nośników danych.
- Kopie zapasowe powinny być przechowywane w odległym miejscu (*ang. backup off-site*) w wystarczającej odległości od głównej lokalizacji, żeby zapobiec ewentualnym ich uszkodzeniom w przypadku katastrofy w głównej lokalizacji.
- Nośnik kopii zapasowych musi mieć zapewniony poziom ochrony fizycznej i środowiskowej, właściwy dla standardów stosowanych w pierwotnej lokalizacji.

9.5 Rejestracja logów i monitorowanie

- Rejestracja logów musi być skonfigurowana w taki sposób, żeby rejestrować działania użytkowników, tzn. czasy logowania, wyjątki, błędy i zdarzenia związane z bezpieczeństwem. Lista systemów i urządzeń, dla których należy uruchomić rejestrację logów, przedstawiona jest poniżej:
  - krytyczna infrastruktura serwerowa;
  - systemy użytkowników przetwarzające informacje o wysokiej wartości;
  - zapory sieciowe (*ang. firewall*) i inne brzegowe urządzenia sieciowe, np. routery brzegowe;
  - systemy i urządzenia znajdujące się w bezpiecznej strefie DMZ (strefa zdemilitaryzowana);
  - serwery nazw domen, serwery poczty e-mail;
  - serwery usługi katalogowej Active Directory;
  - serwery plików.
- Celem szybkiej identyfikacji i reakcji na problemy związane z bezpieczeństwem powinny zostać wdrożone wszędzie, gdzie jest to techniczne możliwe, automatyczne powiadomienia.

9.5.1 Ochrona rejestrów i logów

- Urządzenia rejestrujące i zawartość logów powinny być chronione przed nieuprawnionym dostępem. Należy wdrożyć środki kontroli chroniące logi i rejestry problemów operacyjnych przed nieuprawnionymi zmianami, w tym umożliwiające wykrycie następujących czynności:
  - edycja lub usunięcie plików zawierających logi;
  - przekroczenie pojemności nośnika z plikiem logów skutkujące błędem w formie braku rejestracji zdarzeń bądź nadpisaniem wcześniej zapisanych zdarzeń.
- Logi zdarzeń powinny być przechowywane zgodnie z politykami przechowywania danych oraz lokalnymi przepisami i regulacjami.

9.5.2 Logi administratora i operatora

- Korzystanie z konta administracyjnego oraz operatorskiego musi podlegać rejestracji, przechowywaniu i ochronie celem przeglądu.
- Katalogi i systemy powinny być skonfigurowane w taki sposób, żeby rejestrować tworzenie, usuwanie i dokonywanie zmiany kont użytkowników, jak również dokonywanie przez użytkowników o uprawnieniach administratorów i operatorów zmian obiektów krytycznych i polityk systemowych.

9.5.3 Synchronizacja zegara

Dla celów integralności czasy wszystkich istotnych systemów przetwarzania informacji powinny być zsynchronizowane z uwierzytelnionym pojedynczym referencyjnym źródłem danych czasowych, tzw. protokołem synchronizacji czasu (*ang. Network Time Protocol*).

9.5.4 Monitorowanie

- CRH i jej spółki operacyjne mają słuszny interes, by chronić swoje biznesy, dobre imię, zasoby i sprzęt. Jednocześnie mają także prawny obowiązek ochrony danych osobowych pracowników i klientów. W razie incydentu lub podejrzenia nadużyć ze strony pracownika, CRH i jej spółki operacyjne mogą zdecydować się na monitorowanie historycznej aktywności pracownika w zakresie poczty e-mail i Internetu. Wszelkie ograniczenia prawa pracownika do prywatności powinny być proporcjonalne do prawdopodobnej szkody naruszenia słusznych interesów pracodawcy. Powinna zostać przyjęta Polityka dozwolonego korzystania z zasobów spółki odzwierciedlająca tego rodzaju równowagę, zaś pracownicy powinni zostać wyraźnie poinformowani o rodzaju, zakresie i celach monitorowania, o którym mowa w tej Polityce.
- Lokalizacje, w których systemach są przechowywane aktywa informacyjne, mające istotne znaczenie dla działalności gospodarczej (tzn. dane osobowe, informacje finansowe, regulacyjne lub prawne) powinny posiadać własne rejestry użyć i logi zdarzeń, zbierane oraz przechowywane przez właściwy okres na potrzeby późniejszych regularnych przeglądów. Dane z logów i monitorowania powinny być skorelowane w celu wykrywania nieprawidłowych działań i powinny umożliwiać analizy nietypowych zdarzeń.

9.6 Systemy operacyjne

9.6.1 Instalacja oprogramowania w systemach operacyjnych

- Systemy muszą być zabezpieczone przy użyciu uznanych branżowych standardów bezpieczeństwa, np. NIST, CIS, SANS.
- Instalacja oprogramowania w systemach operacyjnych, musi podlegać kontroli w celu zapewnienia integralności systemów operacyjnych.
- Procedury wycofania zmian, powinny być przygotowane przed wprowadzeniem jakichkolwiek zmian do systemów i oprogramowania.
- Oprogramowanie pochodzące od dostawców, wykorzystywane w systemach operacyjnych, powinno posiadać najwyższy dostępny poziom wsparcia oferowanego przez dostawcę. Jeżeli poziom ten reprezentuje wyższe ryzyko, niż jest akceptowane przez spółkę operacyjną, wówczas ryzyko to musi zostać zarejestrowane i zarządzane, zgodnie z rozdziałem niniejszego regulaminu zatytułowanym „Zakres odpowiedzialności i obowiązków wynikających z Polityki”.
- Fizyczny lub logiczny dostęp do systemów operacyjnych, powinien być przyznawany dostawcom wyłącznie na potrzeby świadczenia usług wsparcia, w razie zaistnienia stosownej potrzeby i na podstawie zgody kierownictwa. W odpowiednich przypadkach, działania dostawcy powinny podlegać monitorowaniu i rejestracji (tzn. sesje zdalnego dostępu).
- Systemy i usługi o krytycznym znaczeniu (np. serwery DNS, plików, poczty, WWW i baz danych) powinny być obsługiwane w dedykowanych fizycznych lub logicznych środowiskach serwerowych.
- Stare wersje oprogramowania powinny być archiwizowane wraz z wymaganymi informacjami, parametrami, procedurami, danymi konfiguracyjnymi umożliwiającymi ich odtworzenie i oprogramowaniem towarzyszącym przez wymagany okres przechowywania danych w archiwach.

9.7 Zarządzanie technicznymi podatnościami na zagrożenia

- Ekspozycja firmy na ryzyko luk systemowych, musi podlegać należytej ocenie i właściwe środki muszą być podejmowane dla zarządzania prawdopodobnym ryzykiem. Zakresy obowiązków i odpowiedzialności w obszarze zarządzania lukami systemowymi i podatnościami na zagrożenia, muszą zostać zdefiniowane.
- Skanowanie pod kątem podatności na zagrożenia krytycznych systemów należy przeprowadzać w odstępach miesięcznych, przy wykorzystaniu zautomatyzowanych narzędzi. Systemy z dostępem do Internetu o stwierdzonych krytycznych lukach bezpieczeństwa muszą mieć w trybie priorytetowym zainstalowane poprawki bezpieczeństwa. Nagłe poprawki wydawane przez dostawców w celu obniżenia ryzyka zagrożeniem atakami dnia zerowego lub wydawane celem zmniejszenia ryzyka zagrożeniem o dużej skali wymagają zainstalowania w ciągu trzech dni.
- Aktywa, które nie mogą podlegać inspekcji z wykorzystaniem zautomatyzowanych narzędzi, należy ręcznie identyfikować i analizować pod kątem dostępności poziomów poprawek.
- Okna serwisowe do instalacji poprawek dla aplikacji biznesowych wymagają uzgodnienia z właściwymi osobami odpowiedzialnymi. Ryzyko związane ze podatnościami na zagrożenia techniczne (określane na podstawie zagrożeń, podatności na zagrożenia, prawdopodobieństwa wystąpienia i skutków) powinno podlegać identyfikacji i rejestracji, zaś wszelkie podejmowane czynności mające na celu zarządzania ryzykiem, wykonywane zgodnie z procedurą zarządzania zmianą lub procedurą obsługi incydentów.

- Zidentyfikowane luki i podatności na zagrożenia, muszą podlegać naprawie lub formalnej dokumentacji jako akceptowalne ryzyko.
- Należy również opracować procedury identyfikacji nietypowych luk i podatności na zagrożenia. Dotyczy to sytuacji, gdy luka została zidentyfikowana, ale nie ma odpowiedniego środka naprawczego, np. w przypadku starszych systemów.

Uwaga: jeżeli spółki operacyjne CRH potrzebują pomocy w realizacji skanowania pod kątem podatności na zagrożenia, prosimy o kontakt pod adresem cyber@crh.com.

9.7.1 Ograniczenia instalacji oprogramowania

Środki kontroli dla zarządzania instalacją oprogramowania przez użytkowników muszą zostać zdefiniowane przez kierownictwo. Środki kontroli powinny wskazywać, jakie rodzaje oprogramowania użytkownicy mogą instalować i jakie rodzaje instalacji oprogramowania są zakazane.

10. Bezpieczeństwo komunikacji

10.1.1 Kontrola sieci

- Sieci powinny być zarządzane i kontrolowane w celu ochrony informacji w różnych systemach i aplikacjach.
- W miarę możliwości, czynności administracyjne w odniesieniu do sieci, powinny być oddzielone od czynności administracyjnych w stosunku do sprzętu komputerowego, tzn. inżynierzy sieciowi powinni pracować przede wszystkim w systemach sieciowych.
- Należy wdrożyć środki kontroli na rzecz zabezpieczenia poufności, integralności i dostępności danych przepływających przez sieć. Do takich środków kontroli należą:
    - wdrożenie zatwierdzonych standardów szyfrowania i uwierzytelniania dla wewnętrznych sieci bezprzewodowych podczas uzyskiwania dostępu do systemów lub aplikacji spółki;
    - wdrożenie środków kontroli pozwalających na zdalny dostęp do systemów lub informacji spółki tylko poprzez centralnie zarządzane rozwiązania zdalnego dostępu.
- Urządzenia służbowe udostępniane przez spółkę, łączące się z wewnętrzną siecią spółki przy użyciu sieci publicznych, powinny używać bezpiecznych szyfrowanych metod, tzn. wirtualnych sieci prywatnych (VPN).
- Środki kontroli dla zabezpieczenia urządzeń infrastruktury sieciowej, powinny być wdrażane na podstawie zatwierdzonych standardów bezpieczeństwa i konfiguracji, tzn. CIS. Należy również wdrożyć zarządzanie konfiguracją, obejmujące następujące elementy:
    - najnowsza stabilna wersja każdej aktualizacji związanej z bezpieczeństwem urządzenia sieciowego powinna być instalowana możliwie jak najszybciej po jej wydaniu;
    - aktualizacje powinny być testowane przed zainstalowaniem na urządzeniach produkcyjnych.
- Konfiguracje urządzeń sieciowych powinny być zabezpieczone, a ich kopie zapasowe wykonane.
- Właściwe rejestrowanie logów i monitoring powinno być włączone na wszystkich sieciowych urządzeniach bezpieczeństwa (w tym IPS, IDS i zapory sieciowe - firewalle). Logi powinny być przechowywane i chronione przed nieuprawnionym dostępem lub zmianami, a ich kopie zapasowe należy tworzyć zgodnie z lokalnymi politykami tworzenia i przechowywania kopii zapasowych.
- Dane z logów i monitoringu powinny być skorelowane w celu wykrywania działań nieprawidłowych i powinny umożliwiać analizy nietypowych zdarzeń.

10.1.2 Separacja sieci

- Środowiska z dostępem do Internetu powinny być oddzielone od wewnętrznych sieci spółki, tzn. poprzez strefy zdemilitaryzowane i strefy sieciowe. Poza tym należy wdrożyć routery i zapory sieciowe (*ang. firewall*), żeby ograniczyć ruch z serwerów publicznych do wewnętrznych sieci spółki .Zapory sieciowe (*ang. firewall*) muszą znajdować się we wszystkich punktach dostępu do sieci nie należących do spółki.
- Sieci wewnętrzne powinny być rozdzielone logicznie lub fizycznie odpowiednio od usług informacyjnych, użytkowników i systemów.
- Systemy, które są uznawane są za systemy wysokiego ryzyka, powinny być oddzielone od innych części sieci, tj. poprzez oddzielną sieć VLAN, DMZ, segment firewalla, wirtualizację, środowiska odizolowane od reszty sieci i Internetu.
- Sieci sterowania przemysłowego lub sieci technologii operacyjnej, muszą być fizycznie lub logicznie oddzielone od korporacyjnych sieci IT.

10.2 Przekazywanie informacji

10.2.1 Polityki i procedury przekazywania informacji

- Informacje Spółki muszą być zabezpieczone i chronione przed nieuprawnionym ujawnieniem lub niewłaściwym wykorzystaniem podczas ich przekazywania, tzn. przez e-mail, SFTP, transfer fizyczny dokumentów papierowych, transfery w chmurze itp.
- Należy ustanowić formalne standardy, procedury i środki kontroli przekazywania informacji w celu ochrony informacji spółki przed nieuprawnionym ujawnieniem lub niewłaściwym wykorzystaniem. Muszą one zostać opracowane w połączeniu z odpowiednimi zasadami zarządzania aktywami i klasyfikacji informacji.

10.2.2 Umowy dotyczące przekazywania informacji

- Bezpieczne przekazywanie informacji pomiędzy spółką a zewnętrznymi osobami trzecimi, wymaga uzgodnienia i dokumentacji. Mogą mieć one charakter standardowej istniejącej umowy lub porozumienia o świadczeniu usług.
- Ryzyko przekazywania informacji spółki osobie trzeciej, musi podlegać identyfikacji i zatwierdzeniu przez Spółkę lub lokalnego przedstawiciela ds. bezpieczeństwa informacji, np. spółka używająca usługi chmurowej do przekazywania poufnych informacji służbowych z której korzysta wiele innych firm obcych, musi uzyskać zgodę i zatwierdzenie ryzyka.

10.2.3 Komunikacja elektroniczna

- Informacje przekazywane za pomocą poczty elektronicznej lub komunikatorów internetowych (np. Skype) muszą być chronione z wykorzystaniem odpowiednich branżowych standardów szyfrowania.
- Transfer plików za pośrednictwem komunikatorów jest surowo zabroniony.
- Właściwe procesy powinny zostać wprowadzone w celu zapewnienia prawidłowego adresowania i przekazywania wiadomości, np. poprzez regularne kontrole poprawności numerów automatycznego wybierania faksu.

10.2.4 Transport nośników fizycznych zawierających informacje spółki

- Informacje spółki muszą być chronione przed nieuprawnionym ujawnieniem lub zmianą.
- Podpisany odbiór lub potwierdzenie dostawy powinny być zawsze uzyskiwane od odbiorcy. W przypadku aktywów o wysokiej wartości, podpisany odbiór jest obowiązkowy.
- W przypadku fizycznego przekazywania informacji o wysokiej wartości, należy korzystać z bezpiecznych środków transportu, np. znanych, bezpiecznych firm kurierskich.

10.2.5 Umowy o zachowaniu poufności i zakazie ujawniania informacji

Podczas współpracy z osobami trzecimi, które mają kontakt z informacjami spółki, należy przygotować do podpisu i akceptacji odpowiednie umowy o zachowaniu poufności lub zakazie ujawniania informacji.

11. Pozyskiwanie, rozwój i utrzymanie systemów

11.1.1 Analiza i specyfikacja wymagań bezpieczeństwa informacji

Wymagania bezpieczeństwa i środki kontroli, powinny podlegać identyfikacji i dokumentacji dla nowych systemów informacyjnych na etapie fazy określania wymogów dla projektu.

11.1.2 Zabezpieczanie usług aplikacyjnych w sieciach publicznych

Informacje spółki przechodzące przez sieci publiczne, powinny być chronione przed działaniami noszącymi znamiona oszustwa, nieuprawnionym dostępem, ujawnieniem i zmianami. Wdrożone środki kontroli muszą obejmować szyfrowanie i uwierzytelnianie.

11.1.3 Ochrona transakcji w ramach usług aplikacyjnych

Informacje dotyczące transakcji realizowanych usługami aplikacyjnymi, powinny być zabezpieczone w celu zapobieżenia niepełnej transmisji, błędnemu przekierowaniu, nieuprawnionej zmianie treści, nieuprawnionemu dostępowi, ujawnieniu, nieuprawnionemu powieleniu lub odtworzeniu wiadomości, tzn. przez *ang. Challenge Handshake Authentication Protocol* (CHAP).

11.2 Ochrona w procesach rozwoju i wsparcia oprogramowania

- Zmiany w systemach wykonywane w ramach cyklu tworzenia oprogramowania powinny być kontrolowane przy użyciu formalnych procedur kontroli zmiany i zarządzania wersjami.
- W razie zmiany platform operacyjnych, aplikacje biznesowe o znaczeniu krytycznym, powinny być sprawdzane i testowane w celu zapewnienia braku negatywnego wpływu zmiany platformy operacyjnej na działalność operacyjną.
- Zmian pakietów oprogramowania należy unikać lub ograniczać je do bezwzględnie niezbędnego zakresu, a wszelkie zmiany powinny być ściśle kontrolowane i dokumentowane (patrz rozdział niniejszej Polityki zatytułowany „Zarządzanie zmianą"), np. przez komitet ds. zatwierdzania zmian.
- Spółka powinna chronić i zabezpieczyć środowiska na potrzeby prac programistycznych, testowych i produkcyjnych, a wdrożone środki kontroli powinny obejmować następujące elementy:
  - uwierzytelnianie dostępu do środowisk programistycznych, testowych i produkcyjnych;
  - logicznie i fizycznie oddzielone środowiska;
  - użycie bezpiecznych technik programowania dla budowy bezpiecznych systemów, np. Microsoft Secure Software Development Lifecycle, OWASP Top 10 i SANS 25.

11.2.1 Ochrona danych testowych

Dane testowe powinny być starannie dobierane, chronione i kontrolowane. Dane produkcyjne wykorzystywane do testowania oprogramowania powinny być oczyszczane i zanonimizowane, z uwzględnieniem usuwania lub zmiany wszelkich danych osobowych i informacji wrażliwych.

12. Relacje z dostawcami

12.1 Polityka Bezpieczeństwa Informacji w ramach relacji z dostawcami

- Umowy z dostawcami, którzy zarządzają informacjami spółki, powinny obejmować wymogi służące uniknięciu zagrożeń dla bezpieczeństwa informacji związanych z usługami informacyjnymi, technologiami komunikacyjnymi i łańcuchem dostaw produktów (dotyczy to np. nabycia produktu lub usługi oraz wszelkich usług zewnętrznych dostawców, które następnie podzlecono innym zewnętrznym dostawcom).
- Informacje spółki nie powinny być przenoszone, przekazywane lub zatwierdzone do przetwarzania przez osobę trzecią, chyba że:
  - odbywa się to w zatwierdzonych celach biznesowych i podlegało zatwierdzeniu przez odpowiednie lokalne kierownictwo przed rozpoczęciem realizacji usług;
  - zagrożenia dla bezpieczeństwa informacji zostały ocenione pod kątem ich przeznaczenia.
- Przed podłączeniem zewnętrznego systemu lub sieci, należących do osób trzecich do infrastruktury spółki, osoby trzecie muszą zostać zobowiązane do zabezpieczenia swoich systemów w zakresie co najmniej zgodnym z niniejszą Polityką.
- CRH zastrzega sobie prawo do natychmiastowego przerwania połączeń sieciowych ze wszystkimi zewnętrznymi systemami, jeżeli uzna, że osoba trzecia nie spełnia wymagań lub jeśli zewnętrzne systemy stanowią zagrożenie dla systemów spółki.
- Osobom trzecim należy zezwalać na dostęp do systemów i informacji spółki dopiero po podpisaniu przez nie umowy o zakazie ujawniania informacji lub umowy o zachowaniu poufności.
- Wszystkie stosowne wymogi i obowiązki z zakresu bezpieczeństwa informacji, powinny zostać ustalone i uzgodnione w ramach umów i/lub porozumień dla każdej osoby trzeciej.
- Osoby trzecie muszą wyrazić zgodę na przekazywanie spółce i zespołowi GIS CRH informacji o wystąpieniu wszelkich incydentów bezpieczeństwa informacji lub naruszeń bezpieczeństwa danych.

Uwaga: wszelkie wnioski o pomoc w sprawie wytycznych bezpieczeństwa procesów zaopatrzeniowych prosimy kierować na adres cyber@crh.com.

12.2 Przestrzeganie regulaminów i procedur Grupy CRH

12.2.1 Czynności monitorowania i przeglądu w odniesieniu do osób trzecich

- Spółka musi mieć „prawo kontroli" osób trzecich, które przechowują lub przetwarzają krytyczne informacje spółki, bądź dane osobowe, umożliwiające identyfikację osób,
- Spółka musi dokonywać przeglądu i kontroli osób trzecich, które są odpowiedzialne za przechowywanie lub przetwarzanie krytycznych informacji spółki, bądź danych osobowych, umożliwiających identyfikację osób.

12.2.2 Zarządzanie zmianami w odniesieniu do osób trzecich

Zmiany w zakresie świadczenia usług przez zewnętrznych dostawców, które wpływają na uzgodnione wymogi bezpieczeństwa informacji, należy ponownie poddawać ocenie pod kątem ryzyka, a następnie odpowiednio nimi zarządzać.

13. Zarządzanie incydentami bezpieczeństwa informacji

13.1.1 Obowiązki i procedury

Należy ustanowić obowiązki i procedury reagowania na incydenty w celu zapewnienia szybkiego i skutecznego reagowania na incydenty z zakresu bezpieczeństwa informacji. Udokumentowane środki kontroli muszą obejmować następujące elementy:

- schemat klasyfikacji incydentów z zakresu bezpieczeństwa informacji oraz towarzyszące im procedury powinny zostać opracowane w celu ułatwienia klasyfikacji incydentów;
- planowanie, przygotowywanie, monitorowanie, wykrywanie, analizowanie i raportowanie incydentów z zakresu bezpieczeństwa informacji;
- reagowanie, w tym eskalacja i kontrolowane przywrócenie funkcjonalności po incydencie oraz komunikacja z wewnętrznymi lub zewnętrznymi osobami bądź organizacjami;
- zgłaszanie incydentów lub naruszeń dotyczących danych osobowych musi być również dokonywane do właściwych lokalnych organów w terminach wymaganych lokalnymi przepisami.

13.1.2 Raportowanie incydentów i zagrożeń związanych z bezpieczeństwem informacji

- Incydenty z zakresu bezpieczeństwa informacji powinny być zgłaszane do lokalnego działu IT oraz działu bezpieczeństwa informacji Grupy na adres cyber@crh.com. W zależności od skali, incydent powinien podlegać eskalacji w ramach istniejących procedur zarządzania incydentami. Wszyscy użytkownicy powinni być świadomi swoich obowiązków i znać punkty kontaktowe dla celów zgłaszania takich incydentów.
- Pracownicy i osoby trzecie, korzystające z systemów informacyjnych i usług CRH, powinny być zobowiązane do zgłaszania możliwie jak najszybciej wszelkich stwierdzonych lub podejrzewanych incydentów z zakresu bezpieczeństwa informacji lub słabości systemów bezpieczeństwa do działu bezpieczeństwa informacji Grupy.

13.1.3 Postępowanie po wystąpieniu incydentu związanego z bezpieczeństwem informacji

- Wiedza zdobyta podczas analiz i rozwiązywania wcześniejszych incydentów z zakresu bezpieczeństwa informacji, powinna być przekazywana odpowiednim zespołom IT, bezpieczeństwa i biznesu w celu zmniejszenia prawdopodobieństwa wystąpienia bądź skutków wszelkich przyszłych incydentów.
- Procedury identyfikacji, gromadzenia i zabezpieczenia informacji powinny być należycie udokumentowane na wypadek przestępstwa lub incydentu z zakresu naruszenia bezpieczeństwa. Zebrane informacje powinny nadawać się do analizy śledczej, żeby mogły w razie potrzeby służyć jako dowód.

Uwaga: wszelkie wnioski o pomoc w sprawie zbierania materiałów dowodowych prosimy kierować na adres cyber@crh.com.

14. Zapewnienie ciągłości funkcjonowania przedsiębiorstwa w przypadku utraty danych

- Plan ciągłości funkcjonowania przedsiębiorstwa na wypadek utraty danych, musi zostać opracowany w celu zarządzania przeniesieniem zasobów oraz przywróceniem sprawności systemów, obiektów i usług.
- Spółki operacyjne powinny określić wymagania na potrzeby bezpieczeństwa informacji i ciągłości zarządzania bezpieczeństwem informacji w sytuacjach nadzwyczajnych, tzn. w czasie kryzysu lub awarii.
- Dla systemów zawierających informacje spółki o krytycznym znaczeniu, należy wdrożyć redundantne i skalowalne środki kontroli w odniesieniu do obiektów przetwarzania informacji.
- Należy opracować, udokumentować, wdrożyć i utrzymywać wymagany poziom ciągłości funkcjonowania bezpieczeństwa i ochrony informacji w sytuacji niekorzystnej. Powinien on determinować wymagania dotyczące planu przywrócenia systemów IT po awarii.
- Możliwości w zakresie zapewnienia ciągłości funkcjonowania przedsiębiorstwa i przywrócenia działalności po awarii powinny podlegać testom co najmniej raz w roku.

15. Zgodność z przepisami

- Bezpieczeństwo, ochrona i prywatność danych osobowych (*ang. PII*) oraz wrażliwych informacji handlowych powinny być realizowane zgodnie z obowiązującymi lokalnymi regulacjami, przepisami i standardami, np. GDPR, HIPAA, SOX.
- Procedury ochrony PII i informacji wrażliwych, powinny być opracowane, wdrożone i przekazane wszystkim osobom zaangażowanym w kontrolę i przetwarzanie takich informacji.
- Właściciele informacji, którzy zlecają przetwarzanie PII i informacji spółki o wysokiej wartości, muszą być świadomi obowiązków w zakresie ochrony danych i prywatności wynikających z wymogów lokalnych, przepisów ustawowych lub regulacji.

16. Glosariusz

Środki kontroli dostępu	Środki kontroli praw dostępu lub uprawnień każdego użytkownika do danego obiektu systemowego takiego jak katalog plików, indywidualny plik lub drukarka.
Polityka zaznajamiania się akceptacji	Część ramowej struktury bezpieczeństwa informacji, która określa, co użytkownicy mają prawo, a czego nie mają prawa robić w systemach IT CRH i jej spółek operacyjnych. Powinna zawierać odwołania do Polityki Bezpieczeństwa Informacji oraz w stosownych przypadkach kierować użytkowników do pełnego brzmienia Polityki. Powinna również jasno określać sankcje stosowane w razie naruszenia Polityki przez użytkownika.
Atak	Próba zniszczenia, narażenia, zmiany, wyłączenia, kradzieży lub nieuprawnionego dostępu lub użytkowania składnika aktywów
Uwierzytelnienie	Proces zapewnienia, że powoływana charakterystyka jednostki jest poprawna.
Dostępność	Dostępność i użyteczność na wniosek upoważnionej jednostki.
Czarna lista (*ang. black list*)	Lista aplikacji, plików wykonywalnych (plików lub programów wykonywalnych) bądź docelowych adresów internetowych, które są uważane za nieodpowiednie lub niezatwierdzone do użytku służbowego. Czarna lista jest odwrotnością białej listy (*ang white list*).
Kontynuacja działalności gospodarczej	Opis procesów i procedur, które ustanowiono i wdrożono dla zapewnienia, że podstawowe funkcje biznesowe będą realizowane zarówno podczas, jak i po wystąpieniu awarii.
Dyrektor ds. Bezpieczeństwa Informacji (CISO)	Członek wyższego kierownictwa CRH odpowiedzialny za ustanowienie i utrzymywanie wizji, strategii oraz programu służącego zapewnieniu odpowiedniej ochrony aktywów i technologii informacyjnych.
System o krytycznym znaczeniu	System, który wykonuje istotną usługę lub funkcję wsparcia i którego utrata lub zakłócenie może znacząco wpłynąć na działalność.
Wyjątek	Wynik, który odbiega od normy lub oczekiwań.
Kierownictwo Grupy (GLT)	Grupa członków wyższego kierownictwa CRH odpowiedzialnych za ustanowienie i utrzymywanie wizji i strategii przedsiębiorstwa.
Dział Bezpieczeństwa Informacji Grupy (GIS)	Specjaliści bezpieczeństwa podlegający CISO i odpowiedzialni za ogólny nadzór i wsparcie działań na rzecz bezpieczeństwa informacji w całej CRH.
Zabezpieczenie	W systemach komputerowych zabezpieczenie odnosi się do procesu zabezpieczenia systemu poprzez ograniczenie podatności i luk oraz zmniejszenie ewentualnej powierzchni ataku.
Aktywa informacyjne	Każda informacja, jaką organizacja tworzy lub odbiera w trakcie działalności gospodarczej.
Klasyfikacja aktywów informacyjnych	Kategoria lub typ przypisany do danego składnika aktywów, wynikajacy z regulaminu klasyfikacji aktywów.
Incydent	Zdarzenie wykraczające poza zwykłą działalność, które zakłóca normalne procesy operacyjne. Może to być stosunkowo niewiele znaczące zdarzenie, takie jak wyczerpanie miejsca na dysku na serwerze lub poważne zakłócenie, takie jak złamanie zabezpieczeń bazy danych i utrata poufnych informacji.
Przemysłowe urządzenia sterowania SCADA	Urządzenia lokalne SCADA (Supervisory Control And Data Acquisition): Programowalne sterowniki l logiczne (PLC), główne i zdalne terminale (MTU, RTU), czujniki, urządzenia uruchamiające, itd. oraz inne urządzenia podłączone bezpośrednio do sprzętu produkcyjnego w zakładzie.
Systemy sygnalizacji włamania (IDS)	System kontroli bezpieczeństwa komputerów i sieci, który pozwala na kontrolę działania systemów i przychodzącego/wychodzącego ruchu sieciowego. Główną funkcją IDS jest identyfikacja podejrzanych działań lub schematów mogących wskazywać na atak sieciowy lub systemowy.
System zapobiegania włamaniom (IPS)	Zaawansowany system sygnalizacji włamania (IDS), który umożliwia administratorom konfigurowanie predefiniowanych działań, jakie należy podjąć w przypadku wykrycia podejrzanej aktywności.
Rejestr	Szczegółowy wykaz bieżących aktywów.
Urządzenie mobilne	Telefon komórkowy, smartfon, notebook lub tablet multimedialny.
Monitorowanie	Określanie stanu systemu, procesu lub działalności, które może obejmować konieczność sprawdzenia, nadzoru lub krytycznej obserwacji.
Spółka operacyjna	Spółka lub jednostka należąca do CRH.

Dane osobowe (PII)	Wszelkie informacje dotyczące określonej/możliwej do określenia osoby fizycznej, w szczególności wszelkie informacje dotyczące osoby, którą można zidentyfikować, w sposób bezpośredni lub pośredni, poprzez odwołanie do numeru identyfikacyjnego lub jednego bądź większej liczby czynników charakterystycznych dla jej tożsamości fizycznej, fizjologicznej, psychicznej, materialnej, kulturowej lub. Społecznej. Przykładem może być imię i nazwisko, adres, data urodzenia, wyniki analiz poprzedzających zatrudnienie, rejestry wyników oraz dane o czasie pracy i kosztach.
Ryzyko	Wpływ niepewności na cele. Ryzyko jest często wyrażane w połączeniu ze skutkami (lub oddziaływaniem) zdarzenia i powiązanym prawdopodobieństwem wystąpienia. W kontekście systemów zarządzania bezpieczeństwem informacji (IS - *ang. Information Security*)) ryzyko IS może być wyrażone jako wpływ niepewności na cele IS. Ryzyko IS jest związane z potencjalną możliwością, że zagrożenia będą wykorzystywać podatności składnika lub grupy aktywów informacyjnych, w ten sposób powodując szkody dla organizacji
Akceptacja ryzyka	Świadoma decyzja o podjęciu danego ryzyka. Może nastąpić bez ograniczania ryzyka lub w ramach procesu ograniczania ryzyka. Akceptowane czynniki ryzyka są przedmiotem monitorowania i przeglądu.
Ocena ryzyka	Cały proces identyfikacji, analizy i oceny ryzyka.
Środki kontroli bezpieczeństwa	Proces lub technologia wdrożona dla zwiększenia bezpieczeństwa danego składnika aktywów.
Zdarzenie z zakresu bezpieczeństwa informacji	Zidentyfikowane wystąpienie stanu systemu, usługi lub sieci wskazujące na ewentualne naruszenie Polityki Bezpieczeństwa Informacji, awarię środków kontroli lub nieznaną wcześniej sytuację, która może być istotna z punktu widzenia bezpieczeństwa.
Incydent w zakresie bezpieczeństwa informacji	Wszelkie niekorzystne zdarzenie, w związku z którym zagrożony może być pewien obszar bezpieczeństwa komputerowego lub które obejmuje utratę poufności danych, zakłócenie danych lub integralności Systemu, bądź zakłócenia lub odmowę dostępności. Sytuacja może się wiązać z jednym zdarzeniem lub serią niepożądanych lub niespodziewanych zdarzeń z zakresu bezpieczeństwa informacji, które cechuje znaczące prawdopodobieństwo pogorszenia stanu działalności gospodarczej i zagrożenie dla bezpieczeństwa informacji.
Zarządzanie incydentami bezpieczeństwa informacji	Reakcja na zdarzenie z zakresu bezpieczeństwa lub ewentualne naruszenie bezpieczeństwa. Reakcja obejmuje analizę, ocenę, działania naprawcze i raportowanie.
System	Każda aplikacja, sieć lub sprzęt bądź element infrastruktury, serwer, system głosowy i system sterowania (np. karty dostępu), baza danych lub dowolne inne urządzenie lub rozwiązanie, które nie jest urządzeniem użytkownika.
Zagrożenie	Potencjalna przyczyna niepożądanego incydentu, który może spowodować szkodę dla systemu lub organizacji.
Podatności	Podatność składnika aktywów lub środka kontroli, która może być wykorzystana przez zagrożenia.