

Baltic Security Pact

Gdańsk, 8 grudnia 2025 r.
AmberExpo – Konferencja BeSecure 2025

PREAMBUŁA

Współczesny świat stoi w obliczu dynamicznie zmieniających się zagrożeń — zarówno w przestrzeni cyfrowej, jak i w wymiarze energetycznym, środowiskowym, infrastrukturalnym i społecznym.

Bezpieczeństwo stało się wspólnym dobrem, a jego ochrona — wspólną odpowiedzialnością.

Sygnatariusze niniejszego Baltic Security Pact deklarują wolę współpracy ponadsektorowej na rzecz ochrony ludzi, organizacji i środowiska przed współczesnymi zagrożeniami.

Dokument ten stanowi fundament sojuszu wiedzy, technologii i zaufania, budującego odporność Polski i regionu Morza Bałtyckiego.

§1. CEL PAKTU

Celem Baltic Security Pact jest:

- Zintegrowanie środowisk instytucjonalnych, akademickich, samorządowych i biznesowych
- Zintegrowanie działań i strategii w zakresie bezpieczeństwa narodowego, regionalnego i społecznego w kontekście dynamicznych zagrożeń XXI wieku.
- Podnoszenie poziomu świadomości i kompetencji w zakresie cyberbezpieczeństwa wśród obywateli, pracowników i liderów organizacji.
- Rozwój współpracy międzynarodowej w obszarze bezpieczeństwa cyfrowego, militarnego oraz w obszarze dual-use, zwłaszcza w regionie Morza Bałtyckiego i wschodniej flanki NATO.
- Promowanie dobrych praktyk i standardów ochrony danych, infrastruktury i systemów w sektorze publicznym oraz prywatnym.

- Wspieranie innowacji i edukacji w obszarze cyberbezpieczeństwa, w tym startupów, programów badawczych oraz inicjatyw społecznych.

§2. ZASADY WSPÓŁPRACY

Sygnatariusze zobowiązują się do:

- Wymiany wiedzy, danych i doświadczeń między sektorami publicznym, prywatnym i naukowym.
- Wspierania inicjatyw edukacyjnych i szkoleniowych w obszarze bezpieczeństwa, szczególnie skierowanych do sektora MŚP, samorządów i młodzieży.
- Budowy wspólnej infrastruktury wiedzy i innowacji – w tym laboratoriów, hubów i centrów kompetencji.
- Rozwijania partnerstw projektowych w zakresie wdrażania innowacyjnych technologii cyberbezpieczeństwa.
- Promowania etyki cyfrowej oraz zasad odpowiedzialnego wykorzystania sztucznej inteligencji i danych.
- Budowy kultury bezpieczeństwa, opartej na zaufaniu, współodpowiedzialności i transparentności działań.
- Współpracy międzynarodowej, w tym w ramach NATO, UE

§3. OBSZARY DZIAŁANIA

Pakt obejmuje współpracę w następujących obszarach:

- Edukacja i kompetencje cyfrowe – wspieranie programów szkoleniowych i warsztatów związanych z cyberbezpieczeństwem
- Technologia i innowacje – tworzenie wspólnych inicjatyw badawczo-rozwojowych w obszarze AI, cyberdefence, kwantowych metod szyfrowania i ochrony danych.
- Bezpieczeństwo infrastruktury krytycznej – wspieranie inicjatyw wymiany wiedzy i standardów dotyczących ochrony sektora energetycznego, zdrowia, transportu, telekomunikacji i przemysłu.
- Społeczna odpowiedzialność i zaufanie cyfrowe – działania na rzecz edukacji obywatelskiej, przeciwdziałania dezinformacji i budowy odporności społecznej.

§4. KOORDYNACJA I ROZWÓJ PAKTU

- Koordynację działań prowadzi Rada Programowa BeSecure, działająca przy Fundacji CODE:ME.
- Rada może zapraszać do współpracy instytucje, organizacje oraz ekspertów z Polski i zagranicy.
- Postanowienia Paktu mogą być rozwijane w formie rocznych planów działań i wspólnych inicjatyw partnerskich.
- Co roku podczas konferencji BeSecure prezentowany będzie Raport o stanie cyberbezpieczeństwa regionu oraz efekty współpracy w ramach Paktu.

§5. POSTANOWIENIA KOŃCOWE

- Baltic Security Pact jest dobrowolną deklaracją współpracy i solidarności na rzecz wspólnego bezpieczeństwa.
- Pakt jest dokumentem otwartym – do jego sygnowania mogą przystępować kolejne instytucje, samorządy, firmy i organizacje.
- Dokument podpisano w Gdańsku, dnia 8 grudnia 2025 r., podczas konferencji BeSecure 2025.

SYGNATARIUSZE

- Fundacja CODE:ME, Marcin Młyński, CEO
- Gdańska Fundacja Przedsiębiorczości, Dariusz Słodkowski, Wiceprezes Zarządu
- Gdański Uniwersytet Medyczny, Anna Żaczek, Prorektor ds. rozwoju i współpracy
- Miasto Gdańsk, Piotr Grzelak, Zastępca Prezydenta ds. zrównoważonego rozwoju i gospodarki
- Gmina Miasta Sopotu, Magdalena Cieślik, Wiceprezydent Miasta Sopotu
- Infoshare, Grzegorz Borowski, Prezes Zarządu
- Invest in Pomerania / Agencja Rozwoju Pomorza, Piotr Ciechowicz, Wiceprezes Agencji Rozwoju Pomorza
- InvestGDA, Karol Kotz, Prokurent
- Interizon, Jarosław Parzuchowski, Prezes Zarządu
- ISSA Polska, Mateusz Nosek, Prezes Zarządu
- Kainos, Jakub Stempnik, Country Lead for Poland

- Międzynarodowe Targi Gdańskie SA, Andrzej Bojanowski, Prezes Zarządu
- Obszar Metropolitalny Gdańsk Gdynia Sopot, Michał Glaser, Prezes Zarządu
- Pomorska Specjalna Strefa Ekonomiczna Mirosław Kamiński, Prezes Zarządu i Błażej Konkol, Wiceprezes Zarządu
- Pracodawcy Pomorza, Michał Maksymiuk, Zastępca Dyrektora Zarządzającego
- R&D B4Future, Łukasz Brandt, CTO
- Simplito, Błażej Zyglarski, CTO
- S4, Dariusz Kłos, CEO
- Uniwersytet Gdański, Paweł Antonowicz, Prorektor ds. Finansów i Rozwoju
- Uniwersytet Morski w Gdyni, Sygnatariusz: mgr. inż. Rafał Cichocki, Kierownikowi Centrum Cyberbezpieczeństwa Morskiego
- Województwo Pomorskie, Leszek Bonna, Wicemarszałek Województwa Pomorskiego
- Wyższa Szkoła Administracji i Biznesu im. Eugeniusza Kwiatkowskiego w Gdyni, Tomasz Białas, Rektor WSAIB
- Wyższa Szkoła Bankowa Merito, Maja Głuchowska-Wójcicka, Dziekan Wydziału Prawa i Administracji

Załącznik do Baltic Security Pact

Deklaracje sygnatariuszy paktu

Fundacja CODE:ME

Sygnatariusz: Marcin Młyński, CEO

- Realizacja projektu She CODE:ME – 1000 kobiet w cybersec zakładającego serię wydarzeń, spotkań i szkoleń dedykowanych kobietom, które chcą wejść do świata IT związanego z cyberbezpieczeństwem;
- Organizacja minimum 5 lokalnych meetupów z zakresu cybersec we współpracy z ISSA Polska dla 100 uczestników;
- Organizacja konferencji BeSecure 2026, która stanie się największym wydarzeniem poświęconym cybersec w regionie Morza Bałtyckiego;
- Aktywizacja Hackerspace Trójmiasto – największej społeczności technologicznej w północnej Polsce – ze szczególnym uwzględnieniem zasad bezpieczeństwa i security awareness;
- Organizacja cyklu spotkań z zakresu security awareness dla NGO, w których weźmie udział min. 50 uczestników;
- Organizacja ogólnopolskiego wydarzenia Tydzień Programisty z dedykowaną ścieżką poświęconą cybersecurity;
- Rozwój Baltic Security Pact poprzez zaproszenie minimum 15 nowych partnerów oraz przygotowanie raportu podsumowującego działania obecnych partnerów w roku 2026.

Gdańska Fundacja Przedsiębiorczości

Sygnatariusz: Dariusz Słodkowski, Wiceprezes Zarządu

- Organizacja spotkań i projektów promujących rozwiązania z zakresu bezpieczeństwa cyfrowego przeznaczonych dla przedsiębiorców;
- Działania edukacyjne dla młodzieży szkół ponadpodstawowych.

Gdański Uniwersytet Medyczny

Sygnatariusz: Anny Żaczek, Prorektor ds. rozwoju i współpracy

- Projekty badawcze, meetupy oraz konsultacje na rzecz innych podmiotów dot. żywności funkcjonalnej itp.

Miasto Gdańsk

Sygnatariusz: Piotr Grzelak, Zastępca Prezydenta ds. zrównoważonego rozwoju i gospodarki

- Rozwój w Gdańskim Centrum Informatycznym Lokalnego Centrum Cyberbezpieczeństwa dla Gminy Miasta Gdańska. Celem inicjatywy jest zapewnienie cyberodporności infrastruktury miejskiej, ochrona danych mieszkańców oraz zagwarantowanie ciągłości świadczenia e-usług publicznych.

Gmina Miasta Sopotu

Sygnatariusz: Magdalena Cieślik, Wiceprezydent Miasta Sopotu

- Wdrożenie chmurowej platformy bezpieczeństwa typu Secure Access Service Edge w miejskich jednostkach oświatowych. Rozwiązanie znacznie podniesie poziom cyberbezpieczeństwa placówek bez rozbudowy lokalnej infrastruktury, zapewni bezpieczny dostęp do Internetu i zasobów szkolnych, centralne zarządzanie politykami bezpieczeństwa, filtrowanie ruchu, ochronę urządzeń oraz automatyczne wykrywanie i blokowanie zagrożeń;
- Uruchomienie systemu mStraż, polegającego na udostępnieniu Straży Miejskiej mobilnego dostępu do Rejestru Dowodów Osobistych oraz Rejestru PESEL za pomocą bezpiecznych terminali wykorzystywanych w pracy terenowej. Rozwiązanie umożliwi szybkie potwierdzanie tożsamości, weryfikację dokumentów oraz sprawne reagowanie na zdarzenia wymagające identyfikacji osób, co przełoży się na podniesie poziomu bezpieczeństwa funkcjonariuszy i mieszkańców.

Infoshare

Sygnatariusz: Grzegorz Borowski, Prezes Zarządu

- Realizacja bloków dedykowanych cyberbezpieczeństwu podczas dużych konferencji organizowanych pod marką Infoshare.

InvestGDA

Sygnatariusz: Karol Kotz, Prokurent

- Aktywne wspieranie rozwoju ekosystemu bezpieczeństwa poprzez wsparcie wydarzeń branżowych: konferencji, targów oraz innych wydarzeń biznesowych odbywających się w regionie, które uwzględniają kluczowe komponenty cyberbezpieczeństwa lub obronności;
- Wsparcie strategii dla sektorów kluczowych poprzez intensywne działania na rzecz rozwoju i promocji branż o strategicznym znaczeniu dla bezpieczeństwa, ze szczególnym uwzględnieniem: przemysłu zbrojeniowego i technologii podwójnego zastosowania (dual use), sektora kosmicznego, branży cyberbezpieczeństwa oraz zaawansowanych systemów bezpieczeństwa, sektora militarnego.

Invest in Pomerania / Agencja Rozwoju Pomorza

Sygnatariusz: Piotr Ciechowicz, Wiceprezes Agencji Rozwoju Pomorza

Fundacja Interizon

Sygnatariusz: Jarosław Parzuchowski, Prezes Zarządu

- Networking i działania sieciujące;
- Rozwój Living Labu;
- Organizacja spotkań tematycznych, szkoleń i warsztatów.

ISSA Polska

Sygnatariusz: Mateusz Nosek, Prezes Zarządu ISSA Polska

- Współpraca ze środowiskami instytucjonalnymi, akademickimi, samorządowymi i biznesowymi w zakresie organizacji konferencji i innych wydarzeń o charakterze edukacyjnym i networkingowym. Integracja środowisk akademickich będzie następować poprzez podpisywanie porozumień z uczelniami oraz współtworzenie kierunków studiów w obszarze cyberbezpieczeństwa;
- Reagowanie na bieżące zagrożenia, aktywizując swoich członków wokół najważniejszych obszarów bezpieczeństwa cyfrowego – w szczególności poprzez prowadzenie programów mentoringowych;
- Podnoszenie poziomu świadomości i kompetencji w zakresie cyberbezpieczeństwa wśród obywateli, pracowników i liderów organizacji poprzez realizację projektów społecznych, dedykowanych edukacji obywateli, zwłaszcza w grupach najbardziej narażonych na wykluczenie cyfrowe poprzez

inicjatywy przeznaczone do edukacji młodzieży – Cyfrowy Skaut – i obejmujące opieką osoby starsze – Cyfrowy Senior;

- Zarząd Stowarzyszenia będzie ambasadorem założeń Paktu w obszarze współpracy międzynarodowej dotyczącej bezpieczeństwa cyfrowego, militarnego oraz dual-use na poziomie partnerów z ISSA International, wskazując na możliwości związane ze współpracą w kontekście integracji środowisk regionu Morza Bałtyckiego;
- Lokalne społeczności, zrzeszone wokół ISSA Polska, będą aktywnie promować dobre praktyki i standardy bezpieczeństwa, włączając zainteresowane osoby i podmioty na poziomie regionalnym i organizując cykliczne spotkania w ramach inicjatywy ISSA Local, budując i rozwijając kulturę ochrony danych, infrastruktury i systemów;
- ISSA Polska będzie rozwijać działania prowadzone w ramach społecznych inicjatyw takich jak ISSA Student, Cyfrowy Senior, Cyfrowy Skaut, ISSA Local, wdrażając innowacyjne rozwiązania (takie jak np. edukacja cyfrowa w wirtualnej rzeczywistości), czy realizując badania społeczne w obszarach spójnych z celami ustalonymi przez sygnatariuszy Paktu.

Kainos

Sygnatariusz: Jakub Stempnik, Country Lead for Poland

- Seria wykładów o cyberbezpieczeństwie na uniwersytetach i w szkołach w Gdańsku i Gdyni;
- Moduł cyberbezpieczeństwa w ramach Code Camp Poland 2026;
- Q-Camp 2026 z (post)kwantową ścieżką cyberbezpieczeństwa;
- Blok dotyczący cyberbezpieczeństwa kwantowego i technologii dual-use na Q-Con 2026;
- Meetup BeSecure w biurze Kainos.

Międzynarodowe Targi Gdańskie SA

Sygnatariusz: Andrzej Bojanowski, Prezes Zarządu

- Organizacja PowerConnect Energy Summit 2026. W ramach wydarzenia zrealizowane zostaną następujące działania:
 - Powstanie Strefa Bezpieczeństwa, stanowiąca specjalistyczną przestrzeń prezentacji technologii wzmacniających odporność infrastruktury krytycznej sektora energetycznego;

- Powstanie odrębna ścieżka konferencyjna poświęcona bezpieczeństwu infrastruktury, odporności systemów oraz międzynarodowej wymianie doświadczeń w tym obszarze;
- W strefie startupów, tworzonej we współpracy z Infoshare, szczególny nacisk zostanie położony na inicjatywy związane z bezpieczeństwem energetycznym i cyfrowym, którym zapewniona zostanie możliwość bezpłatnych prezentacji innowacji oraz uczestnictwa w programie wystawienniczym.
- Organizacja Międzynarodowych Targów Morskich i Militarnych BALTEXPO 2027. W ramach wydarzenia zrealizowane zostaną następujące działania:
 - Powstanie strefa poświęcona tematyce militarnej i obronnej przeznaczona na prezentację technologii i rozwiązań oraz moduły poświęcone ochronie cywilnej, technologiom dual-use, cyberbezpieczeństwu portów i transportu morskiego;
 - Program konferencyjny zostanie rozszerzony o debaty eksperckie i sesje tematyczne poświęcone bezpieczeństwu morskemu, militarnemu i odporności infrastruktury krytycznej, w tym perspektywie międzynarodowej i współpracy państw regionu Morza Bałtyckiego;
 - Integralną częścią projektu będzie strefa startupów wspierająca rozwój innowacyjnych technologii dla sektora morskiego i obronnego oraz umożliwiającą nawiązywanie współpracy z partnerami instytucjonalnymi i biznesowymi.

Obszar Metropolitalny Gdańsk Gdynia Sopot

Sygnatariusz: Michał Glaser, Prezes Zarządu

- Rozwijanie współpracy na rzecz podniesienia poziomu cyberbezpieczeństwa we wszystkich 61 jednostkach samorządu Obszaru Metropolitalnego Gdańsk-Gdynia-Sopot;
- Organizacja szkoleń w ramach Metropolitalnego Centrum Kompetencji,
- organizacja audytów i testów bezpieczeństwa w ramach wykonywanych projektów;
- Wsparcie tworzenia Lokalnego Centrum Cyberbezpieczeństwa.
- Organizacja hackathonów, konferencji i popularyzacja wiedzy na ten temat w instytucjach publicznych w OMGGS;
- Prowadzenie drogi legislacyjnej tak, aby OMGGS stał się koordynatorem i organizatorem współpracy samorządów w kwestii cyberbezpieczeństwa.

Pomorska Specjalna Strefa Ekonomiczna

Sygnatariusze:

Mirosław Kamiński, Prezes Zarządu

Błażej Konkol, Wiceprezes Zarządu

- Aktywne wspieranie rozwoju ekosystemu cyberbezpieczeństwa w regionie, ze szczególnym uwzględnieniem technologii dual-use;
- Realizacja inicjatyw wzmacniających współpracę między biznesem i nauką;
- Tworzenie warunków sprzyjających rozwojowi innowacji;
- Wspieranie startupów poprzez programy akceleratorów i organizację tematycznych hackathonów, przyczyniając się do zwiększenia odporności cyfrowej i bezpieczeństwa technologicznego regionu.

Pracodawcy Pomorza

Sygnatariusz: Michał Maksymiuk, Zastępca Dyrektora Zarządzającego

- Aktywna działalność Forum ds. bezpieczeństwa i przemysłu obronnego Pracodawców Pomorza w obszarach wymagających wsparcia firm z branży przez nie reprezentowanej;
- Podjęcie działań edukacyjnych dla przedsiębiorców z szeroko pojętego bezpieczeństwa (także cyberbezpieczeństwa): organizacja seminariów, webinarów, konsultacji.

R&D B4Future

Sygnatariusz Łukasz Brandt, CTO

- Organizacja spotkań i konsultacji dla firm w zakresie bezpieczeństwa cyfrowego, w szczególności w obliczu wyzwań NIS2, CRA, dynamicznego rozwoju sztucznej inteligencji i zagrożeń dla istniejących systemów związanych z rozwojem komputerów kwantowych.

Simplito

Sygnatariusz: Błażej Zyglarski, CTO

- Organizacja hackathonów, spotkań i konsultacji.

S4

Sygnatariusz: Dariusz Kłós, CEO

- Prowadzenie konsultacji, audytów, analiz ryzyka i warsztatów dla firm oraz samorządów w zakresie cyberbezpieczeństwa, ochrony danych, odporności infrastruktury oraz zgodności z regulacjami (NIS2, RODO, DORA);

Uniwersytet Gdański

Sygnatariusz: Paweł Antonowicz, Prorektor ds. Finansów i Rozwoju

- Otwarcie nowego kierunku studiów – cyberbezpieczeństwo;
- Organizacja szkoleń wspólnie z ekspertami działającymi w sektorze IT;
- Wykłady dające możliwość uzyskania mikropoświadczeń;
- Rozwój Living Labu;
- Organizacja konferencji tematycznych (meetupów);
- Projekty badawcze dotyczące cyberbezpieczeństwa kwantowego i postkwantowego;
- Webinaria i wykłady otwarte.

Uniwersytet Morski w Gdyni

Sygnatariusz: Rafał Cichocki, Kierownikowi Centrum Cyberbezpieczeństwa Morskiego

- Konsultacje opracowanych treści edukacyjnych;
- Organizacja wspólnych wydarzeń, w tym popularyzujących naukę tj. seminariów, warsztatów, konferencji, spotkań;
- Organizacja konsultacji i doradztwa dla firm
- Budowanie partnerstwa we wspólnych przedsięwzięciach krajowych i międzynarodowych;
- Prowadzenie kierunków studiów i kursów.

Województwo Pomorskie

Sygnatariusz: Leszek Bonna, Wicemarszałek Województwa Pomorskiego

- Realizacja projektu w zakresie podniesienia poziomu cyberbezpieczeństwa oraz kompetencji cyfrowych pracowników jednostek samorządu terytorialnego, a także dostosowania 44 podległych samorządowych jednostek organizacyjnych województwa pomorskiego – wskazanych w projekcie nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa jako podmioty kluczowe i ważne – do obowiązujących przepisów prawa w obszarze bezpieczeństwa systemów informacyjnych. W ramach projektu przewidziano [m.in.:](#)

- przeprowadzenie audytów systemów informacyjnych,
 - modernizację infrastruktury sprzętowej oraz systemów bezpieczeństwa,
 - wsparcie w zakresie migracji zasobów do chmury,
 - szkolenia obejmujące m.in.: reagowanie na incydenty, zarządzanie ryzykiem, ochronę danych osobowych oraz bezpieczeństwo infrastruktury,
 - promowanie dobrych praktyk i standardów w zakresie ochrony systemów informacyjnych w sektorze publicznym.
- Rozwijanie współpracy w ramach Regionalnych Agend Badawczych, w tym partnerstwa CyberSec Pomorze skupionego wokół tematyki cyberbezpieczeństwa. Wspieranie kooperacji w tych obszarach poprzez integrowanie działań podejmowanych przez Województwo Pomorskie, środowisko naukowe oraz sektor technologiczny.
 - Zagadnienia związane z cyberbezpieczeństwem oraz wspieraniem agendy CyberSec Pomorze będą uwzględniane w realizowanych przedsięwzięciach, w szczególności w planowanym projekcie „Smart Green Progress”, w ramach którego podejmowane będą inicjatywy wzmacniające wiedzę i wymianę doświadczeń — takie jak konferencje, warsztaty, wydarzenia eksperckie i sieciujące.

Wszystkie wymienione działania mają przyczyniać się do budowania kompetencji oraz zwiększania odporności cyfrowej pomorskich podmiotów, w tym firm i instytucji publicznych, a w konsekwencji do podnoszenia poziomu bezpieczeństwa cyfrowego w regionie.

Wyższa Szkoła Administracji i Biznesu im. Eugeniusza Kwiatkowskiego w Gdyni

Sygnatariusz: Tomasz Białas, Rektor WSAIB

- Organizacja spotkań Forum Cyberbezpieczeństwa;
- Organizacja meetupów;
- Konsultacje dla firm i instytucji.

Wyższa Szkoła Bankowa Merito

Sygnatariusz: Maja Głuchowska-Wójcicka, Dziekan Wydziału Prawa i Administracji

- Wykorzystanie Laboratorium Cyberbezpieczeństwa dla realizacji specjalistycznych szkoleń dla organizacji;
- Nowy kierunek studiów II stopnia: Cyberbezpieczeństwo;

- Promowanie specjalności Bezpieczeństwo cyberprzestrzeni na I stopniu studiów;
- Organizowanie i promowanie specjalistycznych szkoleń z zakresu cyberbezpieczeństwa;
- Organizowanie i promowanie szkoleń z normy ISO 27001 z zakresu bezpieczeństwa informacji;
- Organizowanie i promowanie wykładów specjalistów, webinarów mających na celu zwiększenie świadomości w zakresie cyberbezpieczeństwa wśród studentów UWSB Merito;
- Podejmowanie współpracy naukowej z Działem Nauki UWSB Merito i/lub Innonovawsb spółką celową uczelni w zakresie realizacji wspólnych projektów;
- Realizacja projektów wdrożeniowych z udziałem studentów w zakresie cyberbezpieczeństwa;
- Realizacja wspólnych działań w ramach RAB CyberSec Pomorze (RAB CyberSec Pomorze to Regionalna Agenda Badawcza w temacie cyberbezpieczeństwa).