Załącznik nr 1 do Zarządzenia nr 9/2024
Dyrektora ACK Cyfronet AGH z dnia 06.06.2024.

Akademickie Centrum Komputerowe Cyfronet AGH	**Polityka Bezpieczeństwa Informacji**	**Wersja 1.0**
	Dokument główny	**Data wyd.: 06.06.2024.** **Liczba stron: 25**

Spis treści

Załącznik nr 1. Wzór rejestru LASI

Załącznik nr 2. Wzór rejestru systemów i usług teleinformatycznych

Załącznik nr 3. Wzór rejestru obszarów (pomieszczeń) o szczególnym znaczeniu dla funkcjonowania Centrum w procesie przetwarzania danych

Załącznik nr 4. Wzór rejestru Administratorów Systemów (AS)

Załącznik nr 5. Wzór rejestru osób uprawnionych do przetwarzania danych osobowych

Załącznik nr 6. Wzór rejestru sprzętu i oprogramowania z elementami konfiguracji

Załącznik nr 7. Wzór rejestru użytkowników systemu/usługi

Załącznik nr 8. Wzór rejestru wejść osób obcych do pomieszczenia chronionego

Załącznik nr 9. Wzór zapisów umownych o powierzeniu danych osobowych

Załącznik nr 10. Wzór zapisów umownych o zachowaniu poufności

Załącznik nr 11. Rejestr aktów prawnych

Załącznik nr 12. Kontekst organizacji

Załącznik nr 13. Cele bezpieczeństwa informacji

Załącznik nr 14. Pomiar skuteczności zabezpieczeń

Używane skróty

ADO	Administrator Danych Osobowych
AGH	Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie
Cyfronet, Centrum	Akademickie Centrum Komputerowe Cyfronet AGH
DCB	Dział Cyberbezpieczeństwa ACK Cyfronet AGH
Dyrektor	Dyrektor ACK Cyfronet AGH
GAI	Główny Administrator Informacji
IODO	Inspektor Danych Osobowych – wymóg RODO
KDC	Kierownik Działu Centrum
Zespół	Zespół doradczy ds. Zarządzania Bezpieczeństwem Informacji
LABF	Lokalny Administrator Bezpieczeństwa Fizycznego
LABI	Lokalny Administrator Bezpieczeństwa Informacji
LASI	Lokalny Administrator Systemów Informatycznych
AS	Administrator Systemu (AS)
PBI	Polityka Bezpieczeństwa Informacji
PBI DG	Polityka Bezpieczeństwa Informacji Dokument Główny
PBI KW	Polityka Bezpieczeństwa Informacji Księga Wytycznych i Procedur
SZBI	System Zarządzania Bezpieczeństwem Informacji

1 Wstęp

Bezpieczeństwo informacji oraz systemów, w których są one przetwarzane jest jednym z kluczowych elementów zapewniających realizację zadań statutowych Centrum.

W celu zapewnienia bezpieczeństwa informacji, Cyfronet wprowadza spójny System Zarządzania Bezpieczeństwem Informacji.

System Zarządzania Bezpieczeństwem Informacji (SZBI) służy ochronie oraz udostępnianiu aktywów w taki sposób, aby poufność, dostępność oraz integralność przetwarzanych informacji pozostawały na odpowiednim poziomie.

Polityka Bezpieczeństwa Informacji (PBI) jest zestawem powiązanych ze sobą dokumentów (polityk, regulaminów, instrukcji, standardów, szablonów, reguł, umów) określających zasady i sposób zarządzania bezpieczeństwem aktywów informacyjnych Cyfronetu.

Dyrekcja Centrum zobowiązuje się do podejmowania niezbędnych działań mających na celu zapewnienie ochrony informacji na pożądanym poziomie, a tym samym spełnienie wymaganego poziomu bezpieczeństwa systemów informacyjnych.

Polityka Bezpieczeństwa Informacji w ACK Cyfronet AGH jest realizowana z uwzględnieniem uregulowań obowiązujących w tym zakresie w AGH, w szczególności Polityki Bezpieczeństwa Informacji wprowadzonej Zarządzeniem nr 9/2017 Rektora AGH z dnia 10 lutego 2017 r. oraz Polityki Ochrony Danych Osobowych AGH przyjętej Zarządzeniem nr 26/2019 Rektora AGH z dnia 27 czerwca 2019 r.

2 Podstawowe definicje

1. **Aktywo/zasób** - wszystko to, co ma wartość dla działalności Cyfronetu w zakresie informacji (zgromadzone informacje oraz środki techniczne i organizacyjne do ich przetwarzania).
2. **Administratorzy systemów informatycznych** - osoby zajmujące się zarządzaniem konkretnymi systemami informatycznymi.
3. **Bezpieczeństwo informacji** - zachowanie poufności, integralności i dostępności informacji.
4. **Dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej; Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
5. **Dostępność** - zapewnienie, że osoby uprawnione będą miały dostęp do informacji w określonym miejscu i czasie.
6. **Incydent związany z bezpieczeństwem informacji** - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działalności Centrum i zagrażają bezpieczeństwu informacji.
7. **Integralność** - cecha zapewniająca, że dane nie zostały zmienione lub usunięte w sposób nieautoryzowany.
8. **Interesariusze -** podmioty (osoby, społeczności, instytucje, organizacje, urzędy), które mogą wpływać na Centrum i/lub pozostają pod wpływem jego działalności.
9. **Postępowanie z ryzykiem** - proces wyboru i wdrażania środków ograniczających ryzyko.
10. **Poufność** - zapewnienie dostępu do informacji tylko osobom upoważnionym.

11. **Rozliczalność** – cecha zapewniająca, że określone działanie dowolnego podmiotu może być jednoznacznie przypisane temu podmiotowi; funkcja ta jest realizowana najczęściej za pomocą różnych form rejestrowania zdarzeń (logowania).
12. **Ryzyko** – kombinacja prawdopodobieństwa zdarzenia i jego konsekwencji (prawdopodobieństwo wystąpienia zagrożenia, które wykorzystując podatność(ci) aktywa, może doprowadzić do jego uszkodzenia, nieuprawnionego ujawnienia, zaginięcia lub zniszczenia).
13. **Ryzyko szczątkowe** – ryzyko pozostające po procesie postępowania z ryzykiem.
14. **System Zarządzania Bezpieczeństwem Informacji (SZBI)** to systematyczne podejście do zarządzania kluczowymi informacjami Centrum w celu zapewnienia ich bezpieczeństwa. Obejmuje on ludzi, procesy, infrastrukturę i systemy informatyczne.
15. **System informatyczny** - zestaw środków technicznych przeznaczonych do przetwarzania informacji.
16. **Szacowanie ryzyka** - całościowy proces analizy i oceny ryzyka.
17. **Usługa** - zestaw funkcjonalności udostępniany za pomocą jednego lub więcej aktywów.
18. **Właściciel aktywa** - osoba odpowiadająca za zarządzanie aktywem, w szczególności decydująca o zasadach przetwarzania informacji oraz sposobach dostępu do informacji. Właścicielem aktywa jest Kierownik Działu Centrum lub osoba wyznaczona przez Dyrektora lub Kierownika Działu Centrum.
19. **Zarządzanie ryzykiem** - proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych, przy zachowaniu akceptowalnego poziomu kosztów.
20. **Zdarzenie związane z bezpieczeństwem informacji** - określony stan systemu, usługi lub ich komponentu, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem (nieznana lub nieprzewidziana sytuacja mogąca mieć wpływ na bezpieczeństwo informacji).

3 Zakres stosowania i rozpowszechniania Polityki Bezpieczeństwa Informacji

1. System Zarządzania Bezpieczeństwem Informacji (SZBI) w Cyfronecie stanowi część całościowego systemu zarządzania, opartą na podejściu procesowym i odnosi się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji.
2. Celem SZBI jest zapewnienie wszystkim przetwarzanym w Cyfronecie informacjom, w tym zawierającym dane osobowe, zachowania atrybutów poufności, integralności oraz dostępności na odpowiednim poziomie.
3. Zasady określone przez dokumenty Polityki Bezpieczeństwa Informacji mają zastosowanie do wszystkich **zasobów informacyjnych** Cyfronetu, w szczególności do:
    - systemów informatycznych, w których są lub będą przetwarzane informacje podlegające ochronie;
    - informacji będących w dyspozycji Cyfronetu lub innych podmiotów, o ile zostały przekazane na podstawie stosownych umów;
    - wszystkich nośników (bez względu na ich rodzaj), na których są lub będą znajdować się informacje podlegające ochronie;
    - wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.

4. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa Informacji zobowiązane są wszystkie osoby mające dostęp do informacji, w tym pracownicy Cyfronetu, współpracownicy i inne osoby mające dostęp do informacji podlegających ochronie na podstawie odrębnych przepisów.
5. Niniejszy dokument może być przedstawiany podmiotom, z którymi Cyfronet związany jest umowami lub innym jednostkom współpracującym.

4 Deklaracja w zakresie bezpieczeństwa informacji w ACK Cyfronet AGH

1. Dyrekcja Cyfronetu uznając, że informacja jest newralgicznym zasobem każdej organizacji, wdrożyła System Zarządzania Bezpieczeństwem Informacji. Priorytetowym celem systemu jest zapewnienie poufności danych chronionych i dostępności wymaganych informacji oraz spełnienie wymagań prawnych.
2. Przez bezpieczeństwo informacji w Cyfronecie rozumie się zapewnienie dostępności, zabezpieczenie przed nieuprawnionym dostępem, naruszeniem integralności bądź zniszczeniem aktywów związanych z przechowywaniem i przetwarzaniem informacji. Zakres ochrony i podjęte środki mają być adekwatne do właściwości aktywów związanych z systemami przetwarzania informacji. Szczegółowe cele bezpieczeństwa informacji określa **Załącznik nr 13 - Cele bezpieczeństwa informacji – PBI DG.**
3. Główne cele Polityki Bezpieczeństwa Informacji:
   - zapewnienie właściwej ochrony zasobów informacyjnych;
   - wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI);
   - zapewnienie spełnienia wymagań prawnych;
   - ochrona systemów przetwarzania informacji (niezależnie od metody przetwarzania) przed nieuprawnionym dostępem; wyciekiem bądź zniszczeniem informacji;
   - zmniejszenie ryzyka utraty informacji;
   - podnoszenie świadomości pracowników w zakresie ochrony danych;
   - zaangażowanie wszystkich pracowników w ochronę informacji.
4. Powyższe cele realizowane w ramach struktury bezpieczeństwa informacji poprzez:
   - wyznaczenie osób odpowiedzialnych zapewniających optymalny podział i koordynację zadań związanych z zapewnieniem bezpieczeństwa informacji;
   - wyznaczenie właścicieli dla kluczowych aktywów informacyjnych, którzy zobowiązani są do zapewnienia im możliwie najwyższego poziomu bezpieczeństwa;
   - przyjęcie za obowiązujące przez wszystkich pracowników Cyfronetu polityk, procedur i zasad bezpieczeństwa wprowadzonych w ACK Cyfronet AGH;
   - określenie zasad przetwarzania informacji, w tym stref i miejsc, w których może się ono odbywać;
   - przeglądy i aktualizację polityk, procedur i zasad postępowania dokonywane przez odpowiedzialne osoby w celu minimalizacji zagrożeń oraz jak najlepszej reakcji na incydenty związane z przetwarzaniem informacji;
   - ciągłe doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji funkcjonującego w Centrum.
5. W ACK Cyfronet AGH System Zarządzania Bezpieczeństwem Informacji uwzględnia procesy utrzymania odpowiedniego poziomu bezpieczeństwa poprzez:
   - zarządzanie dostępem do zasobów informacyjnych,
   - zarządzanie ryzykiem,

- monitorowanie poziomu bezpieczeństwa,
- zarządzanie incydentami,
- rozwój i bezpieczną eksploatację systemów informacyjnych,
- zarządzanie ciągłością działania,
- zarządzanie zmianami,
- nadzór nad dokumentacją SZBI.

6. Dla utrzymania odpowiedniego poziomu bezpieczeństwa informacji Dyrektor Cyfronetu zapewnia szkolenia z zakresu ochrony informacji oraz ułatwia podnoszenie kwalifikacji zawodowych pracowników.
7. Nakłady ponoszone na realizację zasad Polityki Bezpieczeństwa Informacji, w tym wymagane zabezpieczenia, poprzedzane są analizą ryzyka i kosztów oraz powinny być adekwatne do potencjalnych strat spowodowanych naruszeniem zasad bezpieczeństwa.
8. Dyrektor Cyfronetu zapewnia środki niezbędne do realizacji Polityki Bezpieczeństwa Informacji.

5 Ogólne zasady bezpieczeństwa informacji

Wprowadzając System Zarządzania Bezpieczeństwem Informacji Cyfronet przyjmuje poniższe uniwersalne zasady, które są podstawą dla skutecznego zarządzania bezpieczeństwem informacji:

1. **Zasada uprawnionego dostępu.**
   Każdy nowo przyjęty pracownik przechodzi szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisuje stosowne oświadczenie o zachowaniu poufności.
2. **Zasada przywilejów koniecznych.**
   Każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań.
3. **Zasada wiedzy koniecznej.**
   Każdy pracownik posiada wiedzę o systemie, do którego ma dostęp ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań.
4. **Zasada usług koniecznych.**
   Udostępniane powinny być tylko takie usługi, jakie są wymagane do realizacji zadań statutowych Centrum.
5. **Zasada asekuracji.**
   Każdy mechanizm zabezpieczający powinien być ubezpieczony drugim, innym (podobnym). W przypadkach szczególnych może być stosowane dodatkowe (trzecie) niezależne zabezpieczenie.
6. **Zasada świadomości zbiorowej.**
   Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych i aktywnie uczestniczą w tym procesie.
7. **Zasada indywidualnej odpowiedzialności.**
   Za bezpieczeństwo poszczególnych elementów odpowiadają osoby, które wykorzystują informacje chronione w swojej pracy.
8. **Zasada obecności koniecznej.**
   Prawo przebywania w określonych miejscach mają tylko osoby uprawnione na czas wykonywania pracy.

9. **Zasada stałej gotowości.**
   System jest przygotowany na zidentyfikowane zagrożenia. Niedopuszczalne jest jakiekolwiek wyłączanie mechanizmów zabezpieczających.
10. **Zasada najsłabszego ogniwa.**
    Poziom bezpieczeństwa wyznacza najsłabszy (najmniej zabezpieczony) element.
11. **Zasada ewolucji.**
    Każdy system musi ciągle dostosowywać i aktualizować mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych.
12. **Zasada odpowiedniości.**
    Używane środki techniczne i organizacyjne muszą być adekwatne do sytuacji.
13. **Zasada świadomej konwersacji.**
    Nie należy mówić wszystkiego co się wie, ale należy wiedzieć wszystko to co się mówi (i do kogo).
14. **Zasada segregacji zadań.**
    Zadania i uprawnienia powinny być tak podzielone, aby jedna osoba nie mogła zdobyć pełnej kontroli nad całym systemem.

6 Zgodność z wymaganiami prawnymi

ACK Cyfronet AGH dba o zapewnienie zgodności zasad postępowania z przepisami obowiązującego prawa, przyjętymi uwarunkowaniami umownymi i normatywnymi oraz wypracowanymi własnymi standardami.

W Cyfronet zostały wdrożone mechanizmy (procedury, dobre praktyki itp.) zapobiegające naruszeniom przepisów prawa powszechnie obowiązującego, w tym związanych z ochroną własności intelektualnej. Prowadzona jest bieżąca ewidencja licencji oprogramowania, co zapewnia, że pracownicy upoważnieni do instalacji oprogramowania działają w granicach praw nabytych przez Cyfronet. Nadzorowana jest także własność intelektualna powierzona lub przekazana przez osoby trzecie. Celem takiego postępowania jest zapewnienie bezpieczeństwa informacji poprzez unikanie naruszania przepisów prawa oraz zobowiązań wynikających z umów. Realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanej z identyfikacją wymagań prawnych w zakresie bezpieczeństwa informacji. Jednym z elementów realizacji celu są okresowe audyty bezpieczeństwa, których wyniki stanowią dane wejściowe do stałego doskonalenia systemu SZBI.

W ACK Cyfronet AGH politykę ochrony informacji zbudowano w oparciu o akty prawne wymienione w **Załącznik nr 11 - Akty prawne - PBI DG.**

Podstawą normalizacyjną dokumentu Polityki Bezpieczeństwa Informacji są niżej wymienione normy:

- "PN-EN ISO/IEC-27001:2022 (wersja angielska) Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania";
- "PN-ISO/IEC-27005:2014-01 Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji";
- "PN-EN ISO/IEC 27002:2022 (wersja angielska) Technika informatyczna - Praktyczne zasady zarządzania bezpieczeństwem informacji".

7 Organizacja bezpieczeństwa informacji w ACK Cyfronet AGH

7.1 Postanowienia ogólne

1. Odpowiedzialność za bezpieczeństwo informacji w Cyfronecie ponoszą wszyscy właściciele i użytkownicy systemów przetwarzania informacji zgodnie z niniejszą Polityką Bezpieczeństwa Informacji oraz pozostałymi dokumentami Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).
2. ACK Cyfronet AGH odpowiedzialny jest za zapewnienie niezbędnych zasobów dla funkcjonowania, utrzymania i doskonalenia systemu SZBI. Cyfronet zapewnia kompetentną kadrę pracowniczą do realizacji wyznaczonych zadań. Celem takiego postępowania jest ograniczenie ryzyka błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania zasobów. Elementem zapewnienia bezpieczeństwa zasobów ludzkich jest z jednej strony okresowa realizacja szkoleń z zasad spełniania wymogów bezpieczeństwa, z drugiej strony bezwzględne przestrzeganie zasady rozdziału kompetencji i indywidualnej odpowiedzialności w obszarze poszczególnych aktywów.
3. Dyrektor ACK Cyfronet AGH jest bezpośrednio odpowiedzialny za ochronę bezpieczeństwa informacji w jednostce, a w szczególności za monitorowanie poufności, integralności i dostępności posiadanych zasobów informacji, nadzorowanie przestrzegania zasad bezpieczeństwa przez podległych pracowników oraz podejmowanie stosownych działań w razie stwierdzenia wystąpienia incydentu lub sytuacji mogącej prowadzić do wystąpienia incydentu bezpieczeństwa.
4. Właściciel aktywa odpowiada za zarządzanie aktywem, w szczególności decyduje o zasadach przetwarzania informacji oraz sposobach dostępu do informacji.
5. Każdy pracownik Centrum jest zapoznawany z zasadami bezpieczeństwa oraz z aktualnymi procedurami ochrony informacji w swojej komórce organizacyjnej oraz w Centrum.

7.2 Kontekst organizacji

Zewnętrzny kontekst organizacji to instytucje nadzorujące w różnych zakresach Centrum, w tym odpowiednie wymagania dotyczące bezpieczeństwa informacji, a także inne osoby prawne lub fizyczne posiadające prawo dostępu do informacji będącej w posiadaniu Centrum.

Kontekst wewnętrzny to pracownicy i inne osoby posiadające dostęp do danych podlegających ochronie.

Szczegółowy opis kontekstu organizacji określa **Załącznik nr 12 - Kontekst organizacji - PBI DG.**

7.3 Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Na dokumentację systemu SZBI składają się:

1. Polityka Bezpieczeństwa Informacji – Dokument główny,
2. Deklaracja stosowania;
3. Księga wytycznych i procedur bezpieczeństwa;
4. Zarządzenie Dyrektora:

- nr 16/2017 w sprawie zmiany zarządzenia 4/2010 - wprowadzenie zasad bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych i finansowych w ACK Cyfronet AGH,
- nr 11/2014 w sprawie zasad dotyczących bezpieczeństwa i ochrony budynku oraz pomieszczeń ACK Cyfronet AGH,
- nr 17/2015 w sprawie zasad dotyczących bezpieczeństwa i ochrony budynku technicznego ACK Cyfronet AGH przy ul. Podole 62.

Uzupełnieniem dokumentacji systemu SZBI jest dokumentacja eksploatowanych w ACK Cyfronet AGH systemów informatycznych.

Cyfronet zapewnia nadzór nad dokumentacją systemu SZBI i jej zmianami oraz określa zasady jej udostępniania.

7.4 Struktura zarządzania bezpieczeństwem informacji

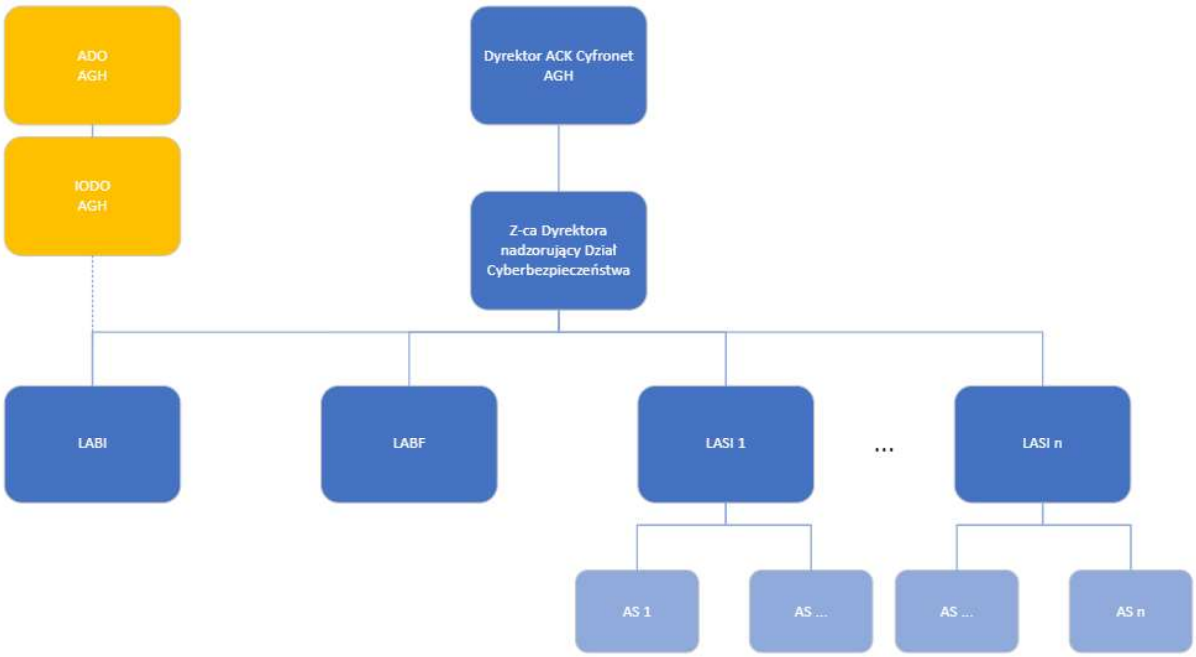
1. Podstawową zasadą przy tworzeniu struktury zarządzania bezpieczeństwem informacji jest oddzielenie funkcji wykonawczych od struktur kontrolnych i zarządzających oraz zasada niezależności i bezstronności osób/jednostek realizujących audyty bezpieczeństwa.
2. Dyrektor powołuje strukturę bezpieczeństwa informacji - **Dział Cyberbezpieczeństwa (ACK-DCB),** czyniąc go odpowiedzialnym za operacyjne wdrażanie ustalonych zasad.
3. W ACK Cyfronet AGH przetwarzanie informacji odbywa się z zachowaniem ustalonych zasad. Za nadzór nad przestrzeganiem zasad ochrony przetwarzania danych odpowiada **Lokalny Administrator Bezpieczeństwa Informacji** (LABI), natomiast za realizację technicznych aspektów – **Lokalni Administratorzy Systemów Informatycznych** (LASI).
4. Pracownicy i inni użytkownicy systemów przetwarzających informację są odpowiedzialni za bezpieczeństwo informacji w Centrum zgodnie ze swoim zakresem obowiązków i posiadanymi prawami dostępu do systemów przetwarzania danych. Każdy użytkownik zobowiązany jest do staranności w dbaniu o bezpieczeństwo powierzonych mu do przetwarzania informacji.

7.4.1 Zespół Doradczy ds. Zarządzania Bezpieczeństwem Informacji

1. Zespół Doradczy do spraw Zarządzania Bezpieczeństwem Informacji jest ciałem doradczym Dyrektora w zakresie zagadnień związanych z bezpieczeństwem przetwarzanej w Cyfronecie informacji.
   W skład Zespołu Doradczego wchodzą:
   - LABI – Lokalny Administrator Bezpieczeństwa Informacji;
   - LABF – Lokalny Administrator Bezpieczeństwa Fizycznego;
   - LASI – Lokalni Administratorzy Systemów Informatycznych;
   - Z-ca Dyrektora nadzorujący Dział Cyberbezpieczeństwa
   - Z-ca Dyrektora d/s Administracyjnych
2. Do obowiązków Zespołu Doradczego należy:
   - wdrażanie Polityki Bezpieczeństwa Informacji (PBI);
   - dokonywanie przeglądu dokumentacji SZBI oraz monitorowanie naruszeń bezpieczeństwa informacji;

- wnioskowanie o dokonywanie zmian w dokumentacji SZBI w oparciu o zdobywane doświadczenie;
- przygotowanie opinii dotyczącej akceptowalności ryzyk w procesie analizy ryzyka;
- podejmowanie przedsięwzięć zmierzających do podniesienia poziomu bezpieczeństwa informacji;
- upowszechnianie dobrych praktyk bezpieczeństwa informacji w jednostkach organizacyjnych;

7.4.2 Schemat organizacyjny Systemu Zarządzania Bezpieczeństwem Informacji



7.4.3 Główny Administrator Informacji oraz Administrator Danych Osobowych

Głównym Administratorem Informacji (GAI) oraz Administratorem Danych Osobowych (ADO) jest Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie. Funkcję GAI/ADO pełni Rektor AGH.

7.4.4 Dyrektor ACK Cyfronet AGH

Dyrektor ACK Cyfronet AGH jest odpowiedzialny za ochronę bezpieczeństwa informacji w jednostce, a w szczególności:

- akceptuje ryzyka i plany postępowania z ryzykiem powstałym w ACK Cyfronet AGH;
- uczestniczy w posiedzeniach Zespołu Doradczego ds. Zarządzania Bezpieczeństwem Informacji;
- zatwierdza zmiany w dokumentacji SZBI;
- zatwierdza decyzje podjęte przez Zespół Doradczy ds. Zarządzania Bezpieczeństwem Informacji oraz dokumenty przygotowane przez LABI, LASI i LABF, w tym harmonogramy i raporty;
- powołuje LABI, LASI i LABF,
- zatwierdza standardy przygotowane przez LABI, LASI i LABF.

7.4.5 Z-ca Dyrektora nadzorujący Dział Cyberbezpieczeństwa

Z-ca Dyrektora nadzorujący Dział Cyberbezpieczeństwa pełni rolę operacyjną, polegającą na weryfikacji planów rozwoju infrastruktury Cyberbezpieczeństwa, weryfikacji raportów bezpieczeństwa wraz z raportami ryzyk, oraz zarządza procesami naprawczymi z zakresu Cyberbezpieczeństwa.

7.4.6 Lokalny Administrator Bezpieczeństwa Informacji (LABI)

Lokalny Administrator Bezpieczeństwa Informacji (Kierownik Działu Cyberbezpieczeństwa) jest rolą operacyjną i odpowiedzialną za nadzór nad realizacją polityki bezpieczeństwa informacji w ACK Cyfronet AGH.

Lokalnego Administratora Bezpieczeństwa Informacji w ACK Cyfronet AGH wyznacza, powołuje i odwołuje Dyrektor.

Lokalny Administrator Bezpieczeństwa Informacji:

1. realizuje nadzór nad wykonywaniem Polityki Bezpieczeństwa Informacji ściśle współpracując z LASI (Lokalny Administrator Systemów Informatycznych), LABF (Lokalny Administrator Bezpieczeństwa Fizycznego), zapewnia, że SZBI jest zgodny z wymaganiami normy;
2. przedstawia Dyrekcji wyniki działania SZBI;
3. realizuje nadzór nad dokumentacją SZBI na etapie jej opracowania, weryfikacji, aktualizacji, udostępniania i przechowywania – koordynacja i nadzór merytoryczny (zgodnie z PN-ISO/IEC 27001);
4. monitoruje zmiany w prawie dotyczące zasad bezpieczeństwa informacji;
5. sprawuje nadzór i koordynuje działania związane z funkcjonowaniem i doskonaleniem SZBI;
6. ustala i wdraża procesy wymagane w SZBI (nadzór nad kontrolowaniem dostępu do aplikacji i informacji);
7. przygotowuje do zatwierdzenia dokumenty dotyczące zasad ochrony grup informacji, regulaminy i instrukcje;
8. we współpracy z IODO zapewnia przetwarzanie danych osobowych zgodnie z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych oraz innymi przepisami powszechnie obowiązującego prawa;
9. raz w roku przedstawia Dyrektorowi raport z funkcjonowania bezpieczeństwa informacji w Centrum;
10. nadzoruje działania wdrożeniowe i doskonalące (zapobiegawcze i korygujące) w SZBI;
11. organizuje przeglądy SZBI oraz nadzoruje realizację ustaleń wynikających z przeglądów;
12. organizuje szkolenia z zakresu SZBI (szkolenia dla osób upoważnionych do korzystania z informacji objętych ochroną), w tym prowadzi szkolenia nowych pracowników w zakresie zasad realizacji Polityki Bezpieczeństwa;
13. sporządza roczny harmonogram działań obejmujący kontrole wybranych zakresów SZBI (audyty bezpieczeństwa informacji), który przedkłada do zatwierdzenia Dyrektorowi;
14. analizuje raporty ze zgłoszonych incydentów o charakterze krytycznym lub istotnych zdarzeń związanych z bezpieczeństwem informacji oraz przedstawia wnioski do kierownictwa Centrum;
15. podejmuje odpowiednie działania w przypadku wykrycia naruszeń bezpieczeństwa informacji lub prób takich naruszeń;

16. w porozumieniu z właścicielami aktywów stosuje środki organizacyjne i techniczne zapewniające ochronę danych (w tym osobowych), w szczególności przed ich nieuprawnionym udostepnieniem, kradzieżą, uszkodzeniem lub zniszczeniem przez osoby nieuprawnione;
17. prowadzi rejestr:
    - Lokalnych Administratorów Systemów Informatycznych (wzór rejestru – **Załącznik nr 1 – Wzór rejestru LASI - PBI DG**);
    - Systemów i usług teleinformatycznych na podstawie danych pozyskanych od LASI (wzór rejestru – **Załącznik nr 2 – Wzór rejestru systemów i usług - PBI DG**);
    - Administratorów Systemów (wzór rejestru – **Załącznik nr 4 – Wzór rejestru AS - PBI DG**);
    - osób uprawnionych do przetwarzania danych osobowych i wydanych upoważnień **Załącznik nr 5 – Wzór rejestru osób uprawnionych do przetwarzania danych osobowych- PBI DG**);
    - aktywów informacyjnych (wzór rejestru – **Załącznik nr 2 – Wzór rejestru aktywów informacyjnych - PBI KW**)
    - certyfikatów cyfrowych (wzór rejestru – **Załącznik nr 7 – Wzór rejestru certyfikatów cyfrowych - PBI KW**)
    - osób uprawnionych do wykorzystywania sprzętu mobilnego (wzór rejestru – **Załącznik nr 12 – Wzór rejestru mobilnego– PBI KW).**
18. w porozumieniu z LABF określa zasady funkcjonowania obszarów szczególnie chronionych (laboratoria, serwerownie etc.), wykaz miejsc szczególnie istotnych dla przetwarzania informacji LABF przekazuje do ABI wg wzoru **Załącznik nr 3 – Wzór rejestru obszarów - PBI DG;**
19. sprawuje nadzór nad gospodarką certyfikatami.

7.4.7 Lokalny Administrator Bezpieczeństwa Fizycznego (LABF)

Lokalny Administrator Bezpieczeństwa Fizycznego (LABF) nadzoruje realizację standardów oraz sposób działania w obszarze bezpieczeństwa fizycznego. Współpracuje z LABI w zakresie wdrażania zaleceń.

Lokalnego Administratora Bezpieczeństwa Fizycznego w ACK Cyfronet AGH wyznacza, powołuje i odwołuje Dyrektor.

Lokalny Administrator Bezpieczeństwa Fizycznego:

1. sprawuje nadzór nad realizacją zadań bezpieczeństwa fizycznego obszarów szczególnie chronionych zgodnie z Polityka Bezpieczeństwa Informacji;
2. w porozumieniu z LABI opracowuje i przygotowuje do zatwierdzenia standardy w obszarze bezpieczeństwa fizycznego;
3. opracowuje roczny harmonogram prac obejmujących kontrole wybranych obszarów;
4. prowadzi rejestr obszarów o szczególnym znaczeniu dla funkcjonowania Centrum (wzór rejestru – **Załącznik nr 3 – Wzór rejestru obszarów - PBI DG**);
5. dokonuje przeglądu istotnych pomieszczeń (zgodnie z harmonogramem lub na wniosek osób zainteresowanych np. Dyrektor, LABI, LASI);
6. biorąc pod uwagę klasy informacji, określa minimalne zasady wyposażenia i struktury technicznej dla pomieszczeń o szczególnym znaczeniu dla funkcjonowania Centrum;
7. podejmuje działania w przypadku incydentów związanych z bezpieczeństwem obszarów chronionych w tym procedury informowania LABI o planowanych zakłóceniach np. przerwy w dostawie energii elektrycznej, spodziewane burze itp.;

8. organizuje i prowadzi ewidencję (rejestr) wejść osób obcych do pomieszczeń, w których znajdują się newralgiczne elementy systemów teleinformatycznych (wzór rejestru – **Załącznik nr 8 – Wzór rejestru wejść - PBI DG)**.

7.4.8 Lokalni Administratorzy Systemów Informatycznych (LASI)

Lokalny Administrator Systemów Informatycznych (LASI) nadzoruje techniczne aspekty realizacji polityki bezpieczeństwa informacji w wyznaczonym obszarze działania oraz określa, w porozumieniu z LABI, standardy bezpieczeństwa informacji.

Lokalnych Administratorów Systemów Informatycznych dla poszczególnych obszarów w ACK Cyfronet AGH wyznacza, powołuje i odwołuje Dyrektor.

LASI współpracuję z Lokalnym Administratorem Bezpieczeństwa Informacji (LABI) w zakresie ochrony informacji.

Do zadań LASI należy w szczególności:

1. kontrola bezpieczeństwa systemów informatycznych;
2. kontrola poprawności funkcjonowania systemów;
3. nadzór nad gospodarką licencjami oprogramowania;
4. nadzór nad nadawaniem i odbieraniem uprawnień dostępu do systemów i usług;
5. w wyznaczonym obszarze działania odpowiada za aktualność inwentaryzacji sprzętu i oprogramowania obejmującego rodzaj i konfigurację (wzór rejestru – **Załącznik nr 6 – Wzór rejestru sprzętu i oprogramowania - PBI DG**);
6. odpowiada za obsługę incydentów związanych z bezpieczeństwem systemów i informacji w zakresie powierzonych systemów informatycznych (wzór rejestru – **Załącznik nr 8 – Wzór rejestru incydentów - PBI KW**);
7. ścisła współpraca z LABI, LABF, administratorami systemów w ramach zarządzania bezpieczeństwem informacji;
8. realizacja zadań związanych z zapewnieniem ciągłości działania systemów teleinformatycznych w wyznaczonym obszarze w Centrum (w szczególności: sporządza Plan wykonania kopii zapasowych danych i systemów w wyznaczonym obszarze zgodnie z przyjętymi w Polityce Bezpieczeństwa Informacji zasadami). Realizacja wykonywania kopii jest dokumentowana (wzór planu wykonywania kopii - **Załącznik nr 11 - Kopie zapasowe – PBI KW**);
9. dla systemów nadzorowanych potwierdzenie możliwość dopuszczenia systemu do użytkowania (oddanie do eksploatacji) i przekazanie do LABI informacji o danych administratora (administratorów) systemu według wzoru celem uzupełnienia informacji (Wzór rejestru - **Załącznik nr 4 – Wzór rejestru AS - PBI DG**);
10. określenie (w porozumieniu z LABI) standardów bezpieczeństwa systemów informatycznych, w szczególności w odniesieniu do systemów o krytycznym znaczeniu dla Centrum;
11. dla systemów automatyzujących prace Centrum potwierdzenie możliwość dopuszczenia systemu do użytkowania (oddanie do eksploatacji):
    - decyzja o wprowadzeniu do eksploatacji,
    - bezpieczeństwo systemu,
    - regulamin usługi/systemu.

7.4.9 Administrator Systemu (AS)

Administrator Systemu (AS) odpowiada za administrowanie wyznaczonymi systemami/usługami/grupami urządzeń.

Administratora Systemu wyznacza, zmienia i odwołuje LASI adekwatnie do zakresu systemu.

AS współpracuje z Lokalnym Administratorem Bezpieczeństwa Informacji (LABI) w zakresie ochrony informacji.

W szczególności Administrator Systemu:

1. realizuje zadania związane z prawidłowym funkcjonowaniem nadzorowanych systemów informatycznych;
2. w porozumieniu z właścicielem usługi oraz LABI (Administrator Bezpieczeństwa Informacji) przygotowuje dokumenty niezbędne do wprowadzenia nowej usługi do eksploatacji (wzór regulaminu (opisu) – **Załącznik nr 5 – Wzór regulaminu usługi - PBI KW**; wzór planu wykonania kopii – **Załącznik nr 11 - Kopie zapasowe - PBI KW**);
3. w uzasadnionych przypadkach (wykrycie zagrożeń, nowe podatności itp.) - wnioskuje do właściciela usługi o wstrzymanie eksploatacji systemu do czasu usunięcia zagrożeń. Decyzję o ewentualnym wstrzymaniu eksploatacji systemu podejmuje właściciel aktywa dokonując stosownej analizy ryzyka. Wyżej wskazany wniosek do właściciela usługi jest odnotowywany przez LASI w Dzienniku Administratora danego systemu);
4. nadaje użytkownikom uprawnienia do korzystania z systemów informatycznych (jeśli nie ma możliwości nadania tych uprawnień centralnie), za zgodą właściciela systemu;
5. prowadzi Dziennik Administratora (wzór Dziennika - **Załącznik nr 9 - Wzór dziennika administratora – PBI KW**);
6. prowadzi rejestr użytkowników systemów, uczestniczy w procesie okresowej weryfikacji aktualności praw dostępu (Wzór rejestru – **Załącznik nr 7 – Wzór rejestru użytkowników systemu - PBI DG)**;
7. prowadzi/nadzoruje czynności serwisowe w lokalnych systemach informatycznych oraz sieciach;
8. rekomenduje konfigurację oprogramowania oraz sprzętu komputerowego (nowego i istniejącego) dla realizacji zasad bezpieczeństwa informacji, w szczególności odpowiada za rekomendacje dotyczące wycofywania z eksploatacji nieaktualnych wersji (nie wspieranych przez producentów) oprogramowania systemowego;
9. realizuje zadania związane z zapewnieniem ciągłości działania systemów teleinformatycznych w Centrum (w szczególności: wykonuje kopie zapasowe administrowanych danych i systemów zgodnie z przyjętymi w Polityce Bezpieczeństwa Informacji zasadami). Realizacja wykonywania kopii jest dokumentowana (wzór planu wykonywania kopii - **Załącznik nr 11 - Kopie zapasowe - PBI KW**);
10. prowadzi niezbędne szkolenia z zakresu wykorzystania systemów i usług, którymi administruje;
11. monitoruje i wykrywa nieautoryzowany dostęp do systemów służących do przetwarzania informacji;
12. przeprowadza cyklicznie (co najmniej raz w roku) przegląd techniczny oraz fizyczną inspekcję okablowania pod kątem podłączonych i nieautoryzowanych urządzeń oraz pod kątem dostępu do pomieszczeń z okablowaniem i paneli połączeniowych. Przegląd jest rejestrowany w Dzienniku Administratora.

7.4.10 Właściciel aktywa

Właściciel aktywa odpowiada za zarządzanie aktywami informacyjnymi, systemami je przetwarzającymi, w szczególności decyduje o zasadach przetwarzania, oczekiwanym poziomie dostępności oraz sposobach dostępu do informacji.

Właściciel aktywa określa:

1. zasady przetwarzania danych w podległych systemach - zgodnie z obowiązującą Polityką Bezpieczeństwa Informacji (nadawanie uprawnień, zasady dostępu, regulamin usługi, i inne). Właściciel aktywa (w porozumieniu z LABI oraz LASI) koordynuje przygotowanie każdej nowej usługi/systemu do wprowadzenia jej do eksploatacji;
2. cechy informacji: dostępność np. publiczna, rodzaj np. użytkowa lub techniczna, wpływ na funkcjonowanie jednostki np. krytyczna, ważna, inne cechy;
3. zasady ciągłości działania systemów i usług (m.in. w porozumieniu z LASI określa poziom oczekiwanej dostępności systemów, zasady tworzenia i czas przechowywania kopii zapasowych i inne, w tym procedury awaryjne).

7.4.11 Pracownicy (użytkownicy)

Osoby przetwarzające informacje są odpowiedzialne za bezpieczeństwo danych w ACK Cyfronet AGH zgodnie ze swoim zakresem obowiązków i posiadanych uprawnień dostępu do systemów przetwarzania informacji. Każdy użytkownik zobowiązany jest do zachowania staranności w dbaniu o bezpieczeństwo powierzonych mu do przetwarzania informacji.

W szczególności każdy pracownik (użytkownik):

1. stosuje zasady opisane w Polityce Bezpieczeństwa Informacji;
2. chroni informacje stosownie do ich wagi przed dostępem do nich przez osoby nieuprawnione;
3. zachowuje szczególną staranność przy przetwarzaniu danych, tak aby dane były przetwarzane zgodnie z prawem, merytorycznie poprawne i adekwatne do celów, w jakich są przetwarzane;
4. chroni informacje przed utratą lub nieuprawnioną modyfikacją;
5. chroni sprzęt i wszelkie nośniki informacji zawierające dane chronione;
6. przestrzega zasad ochrony haseł dostępu do systemów, w szczególności użytkownik zobowiązany jest do zmiany haseł w regularnych odstępach czasu, a w przypadku podejrzenia ujawnienia hasła osobie obcej zmiana hasła musi nastąpić niezwłocznie, zgodnie z wytycznymi w rozdziale 6.2 Księgi wytycznych i procedur;
7. zobowiązany jest do niezwłocznego informowania LASI, LABI lub bezpośredniego przełożonego o wszelkich incydentach, zdarzeniach, awariach itp. sprzętu komputerowego, oprogramowania lub nieprawidłowościach w działaniu systemów i usług.

Pracownicy zobowiązani są do informowania Działu Cyberbezpieczeństwa oraz Bezpośredniego Przełożonego o zdarzeniach mogących mieć wpływ na bezpieczeństwo przetwarzanych informacji w szczególności o zdarzeniach:

1. zniszczenia lub możliwości zniszczenia informacji chronionej;
2. ujawnienia lub możliwości ujawnienia informacji chronionej osobom nieupoważnionym;
3. nieautoryzowanej zmianie lub możliwości wprowadzenia nieautoryzowanej zmiany;
4. innych budzących podejrzenia zdarzeniach.

Zabrania się pracownikom:

1. podejmowania prób wykorzystywania obcych identyfikatorów (kont) oraz obcych metod uwierzytelnienia (haseł, certyfikatów) do pracy z systemami;
2. udostępniania własnych metod uwierzytelniania innym użytkownikom;
3. udostępniania osobom nieuprawnionym informacji chronionych, w tym danych osobowych oraz danych o infrastrukturze teleinformatycznej ACK Cyfronet AGH podlegających ochronie;
4. przetwarzania danych chronionych w sposób mogący narazić je na utratę bezpieczeństwa przez naruszenie poufności, integralności lub dostępności;
5. samodzielnej instalacji oprogramowania systemowego bez posiadania odpowiedniego zezwolenia;
6. uruchamiania aplikacji i programów, które mogą zakłócić lub destabilizować pracę systemów informatycznych ACK Cyfronet AGH;
7. przetwarzania niezabezpieczonych informacji chronionych, zwłaszcza danych osobowych, na nośnikach wymiennych.

W przypadku rozwiązania umowy, przed zakończeniem pracy każdy pracownik zobowiązany jest do zwrotu wszelkich aktywów Centrum będących w jego posiadaniu.

7.5 Zasady współpracy ze stronami zewnętrznymi

W uzasadnionych przypadkach dopuszcza się udostępniania systemów, usług i dostępu do nich osobom trzecim. Osoby trzecie, mające dostęp do informacji chronionych zobowiązane są do podpisania stosownego zobowiązania o poufności oraz, w każdym wypadku, mają obowiązek przestrzegania wszystkich zasad bezpieczeństwa – analogicznie jak pracownicy ACK Cyfronet AGH.

Współpraca ze stronami trzecimi odbywa się na podstawie odpowiednich umów lub pisemnych porozumień. Decyzję o współpracy z podmiotami zewnętrznymi podejmuje Właściciel aktywa, po uzyskaniu zgody Dyrektora lub Zastępcy Dyrektora nadzorującego dany dział. Stronom tym odbiera się prawo dostępu po ustaniu przyczyny, dla jakiej dostały uprawnienia.

W Cyfronecie wdrożono zasady ochrony informacji w odniesieniu do osób trzecich oraz podmiotów wykonujących prace na rzecz Centrum. Umowy zawierane z podmiotami zewnętrznymi winny zawierać klauzule poufności różnego stopnia szczegółowości (adekwatnie do potrzeb) niezbędne przy zawieraniu umów oraz zobowiązania do funkcjonowania zgodnie z obowiązującymi przepisami prawa, w szczególności w zakresie przestrzegania ustawy o ochronie danych osobowych. Wzory zapisów w umowach – **Załącznik nr 9 - Wzór zapisów o powierzeniu danych - PBI DG** i/lub **Załącznik nr 10 - Wzór zapisów o zachowaniu poufności - PBI DG**. Celem takiego postępowania jest zapewnienie ochrony informacji przed dostępem osób niepowołanych, przeciwdziałaniu uszkodzeniu informacji, jej wyciekowi lub innymi zakłóceniami w obiektach Centrum. Zasady związane z zapewnieniem bezpieczeństwa informacji obowiązujące strony trzecie stosuje się też w odniesieniu do wszelkich projektów realizowanych w Centrum samodzielnie lub we współpracy z innymi podmiotami.

Zasady współpracy z Policją, Jednostkami Straży Pożarnej i innymi służbami państwowymi polegają na niezbędnej, wynikającej z kontekstu ewentualnego zdarzenia wymianie informacji w zakresie niezbędnym do zapewnienia bezpieczeństwa osób i mienia oraz porządku publicznego.

O zdarzeniach wymagających bezpośredniej współpracy z ww. służbami niezwłocznie informowana jest Dyrekcja ACK Cyfronet AGH oraz Lokalny Administrator Bezpieczeństwa Informacji.

8 Zarządzanie dostępem do zasobów informacyjnych

Dostęp do informacji przechowywanych i przetwarzanych w ACK Cyfronet AGH jest poddany kontroli wynikającej z powszechnie obowiązujących przepisów prawa oraz dodatkowych wymagań bezpieczeństwa, przyjętych w Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności.

Kontrola polega na:

1. wydzieleniu obszarów przeznaczonych do przetwarzania oraz przechowywania informacji;
2. zastosowaniu odpowiednich barier fizycznych przeciwdziałających nieuprawnionemu dostępowi osób nieupoważnionych, w szczególności w przypadku przetwarzania danych osobowych;
3. stałym monitoringu głównych ciągów komunikacyjnych w budynkach Centrum;
4. zarządzaniu uprawnieniami poszczególnych użytkowników w sposób zapewniający dostęp wyłącznie do danych wymaganych do wykonywania obowiązków służbowych, jeśli dane te podlegają ochronie z jakiejkolwiek przyczyny;
5. stosowaniu bezpiecznych systemów przetwarzania informacji;
6. nadzorowaniu działalności osób trzecich, mogących wpłynąć na bezpieczeństwo informacji;
7. bieżącym informowaniu pracowników o wszelkich zmianach w zakresie regulacji dotyczących przechowywania, przetwarzania i udostępniania informacji.

Adekwatność i skuteczność stosowanych w Centrum środków kontroli dostępu do informacji podlega bieżącej weryfikacji w ramach audytów wewnętrznych, zmian dokumentacji i metod postępowania wynikających z ewolucji uregulowań prawnych oraz systemów przetwarzania danych, a także reagowania na zagrożenia ujawnione przez inne strony.

9 Zarządzanie ryzykiem

ACK Cyfronet AGH zarządza swoimi aktywami informacyjnymi poprzez zapewnienie im wymaganego poziomu bezpieczeństwa. Aktywa informacyjne są identyfikowane i klasyfikowane zgodnie ze stawianymi im wymaganiami w zakresie ochrony.

Ważnym elementem zarządzania aktywami i bezpieczeństwem informacji jest przeprowadzanie okresowej analizy ryzyka i opracowania planów postępowania z ryzykiem. Okresową analizę ryzyka przeprowadza właściciel aktywa. Jej wyniki przekazuje do LABI. Analiza ryzyka stanowi podstawę podejmowania wszelkich działań w zakresie doskonalenia ochrony zasobów informacyjnych Centrum. Na podstawie wyników analizy ryzyka opracowywane są plany postępowania z ryzykiem dla aktywów o ryzykach większych niż ustalony poziom ryzyka akceptowalnego.

Niezależnie od okresowych przeglądów, ryzyka są szacowane po zmianach mających wpływ na system bezpieczeństwa informacji.

10 Monitorowanie poziomu bezpieczeństwa

10.1 Bezpieczeństwo fizyczne sprzętu i okablowania, konfiguracji i eksploatacji infrastruktury teleinformatycznej

W Cyfronecie przyjęto następujące zasady dotyczące bezpieczeństwa sprzętu i okablowania, konfiguracji i eksploatacji:

1. **Zasada bezpieczeństwa fizycznego**.
   Kontrolę fizycznych wejść, zabezpieczenie biur, pokoi i urządzeń, ochronę przed zagrożeniami zewnętrznymi i środowiskowymi, pracę w obszarach zabezpieczonych, nadzór nad obszarami ogólnie dostępnymi.
2. **Zasada bezpieczeństwa sprzętu i okablowania**.
   Rozmieszczenie i ochronę sprzętu, urządzeń wspomagających, bezpieczeństwo okablowania, utrzymanie sprzętu, bezpieczeństwo sprzętu znajdującego się poza terenem Centrum, bezpieczne usuwanie sprzętu, bezpieczną eksploatację urządzeń przenośnych.
3. **Zasada konfiguracji i eksploatacji sieci**.
   Stosowanie środków ochrony przed błędami konfiguracji, złośliwym oprogramowaniem, zagrożeniami dla dostępności, integralności i poufności danych. Obejmuje środki kontroli sieci, bezpieczeństwo usług sieciowych, polityki i zasady dotyczące wymiany informacji, przesyłania wiadomości drogą elektroniczną, regulaminy korzystania z usług sieciowych, identyfikację sprzętu i oprogramowania, kontrolę połączeń sieciowych, routing, nadzorowanie słabości technicznych.

10.2 Bezpieczeństwo związane z wykorzystaniem zasobów

W ACK Cyfronet AGH w trakcie eksploatacji systemów (usług) w sposób ciągły monitoruje się wykorzystanie podstawowych zasobów sprzętowych oraz parametrów pracy. Na podstawie obserwowanych trendów wykorzystania zasobów można prognozować z pewnym wyprzedzeniem konieczność zwiększenia dostępnych zasobów.

10.3 Bezpieczeństwo związane z eksploatacją systemów

Administratorzy systemów (usług) na bieżąco monitorują wykorzystanie systemów przez użytkowników, w szczególności pod kątem prób nieuprawnionego dostępu do systemów, w tym też różnorodne próby wykradania haseł dostępu.

11 Monitorowanie zmian

Wszelkie zmiany mogące wpływać na ryzyka są na bieżąco przeglądane i uwzględniane w działalności Centrum. Przeglądowi podlegają:

1. zagrożenia,
2. podatności,
3. ryzyka,
4. poziom akceptowalności ryzyk,
5. zabezpieczenia i cele zabezpieczeń.

12 Zarządzanie incydentami

1. Każdy pracownik w przypadku zidentyfikowania nieprawidłowego działania systemu potencjalnie mającego wpływ na bezpieczeństwo informacji niezwłocznie winien powiadomić o tym przełożonego lub LABI.
2. Obsługę incydentów w powierzonym zakresie realizuje LASI we współpracy z LABI oraz LABF.
3. Szczególną uwagę należy zwrócić na zdarzenia wskazujące na nieoczekiwane działania systemu mające wpływ na poufność, dostępność i integralność informacji takie jak:
   - utrata danych, usługi lub funkcjonalności,
   - przeciążenie lub niepoprawne działanie systemu,
   - błędy ludzkie mające wpływ na bezpieczeństwo informacji,
   - niezgodności z politykami lub zaleceniami,
   - naruszenie ustaleń związanych z bezpieczeństwem fizycznym,
   - niekontrolowane zmiany systemu
   - naruszenie praw dostępu.
4. Awarie lub inne nienormalne zachowania systemu mogą wskazywać na atak lub rzeczywiste naruszenie bezpieczeństwa i winny być zawsze traktowane jako zdarzenia związane z bezpieczeństwem informacji.
5. Każdorazowe zidentyfikowanie incydentu mającego wpływ na bezpieczeństwo przetwarzanej informacji w ACK Cyfronet AGH jest rejestrowane oraz wykonywana jest wstępna ocena wpływu incydentu na bezpieczeństwo. Po wstępnej analizie podejmowane są niezwłocznie działania mające na celu usunięcie skutków i przyczyn incydentu.
6. Rejestr incydentów jest systematycznie analizowany i poddawany przeglądowi przez LABI oraz Komitet ds. Bezpieczeństwa Informacji (Wzór rejestru – **Załącznik nr 8 – Wzór rejestru incydentów - PBI KW**).

13 Rozwój i bezpieczna eksploatacja systemów informatycznych

Rozwój i eksploatacja systemów informatycznych w ACK Cyfronet AGH, w tym systemów i aplikacji własnych lub pozyskanych od partnerów zewnętrznych jest prowadzony w sposób nadzorowany z uwzględnieniem odpowiedniego poziomu bezpieczeństwa.
ACK Cyfronet AGH uwzględnia w procesie rozwoju i eksploatacji systemów następujące, wymagane czynniki:

1. Spełnienie wymogów bezpieczeństwa podczas zakupu lub wdrażania nowego systemu.
2. Dopuszczenie nowego systemu do fazy produkcyjnej poprzedzone jest fazą testowania.
3. W przypadku aplikacji podjęcie starań umożliwiających dostęp do kodów źródłowych (o ile jest to jest możliwe).
4. Stosowanie procedur kontroli zmian.
5. Dostosowanie wdrażanych systemów do potrzeb interoperacyjności zgodnie z wymogami. Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności.
6. Umożliwienie wymiany danych z zastosowaniem standardowych metod kodowania znaków i dozwolonych formatów plików.
7. Spełnienie wymagań dotyczących prezentacji danych z uwzględnieniem potrzeb osób niepełnosprawnych.
8. Opiekę LASI nad systemami.

14 Zarządzanie ciągłością działania

ACK Cyfronet AGH dba o zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem danych. Celem takiego postępowania jest przeciwdziałanie przerwom w działalności oraz ochrona krytycznych aktywów informacyjnych przed rozległymi awariami lub katastrofami. Realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z zarządzeniem ciągłością działania tak, aby ograniczać do akceptowalnego poziomu skutki wypadków i awarii.

W ramach zapewnienia ciągłości działania realizuje się identyfikację istotnych aktywów informacyjnych oraz zapewnia się wdrożenie mechanizmów organizacyjnych i technicznych wystarczających dla spełnienia wymagań bezpieczeństwa informacji. W szczególności istotnym elementem jest wdrożenie planów i procedur utrzymania lub odtworzenia funkcjonowania systemów, zapewniających dostępność informacji na akceptowalnym poziomie i w wymaganym czasie po wystąpieniu przerwy lub awarii krytycznych systemów.

Istotnym elementem zapewnienia ciągłości jest wdrożenie zasad szacowania ryzyka i postępowania ze zidentyfikowanymi ryzykami mającymi wpływ na bezpieczeństwo przetwarzanej informacji.
Szczegółowe informacje znajdują się w dokumencie **Polityka zarządzania ciągłością działania Centrum**, który stanowi opis zasad zarządzania awaryjnego, kryzysowego i bieżącego w ACK Cyfronet AGH.

15 Zarządzanie zmianami

ACK Cyfronet AGH, mając na uwadze konieczność szybkiego dostosowywania się do wymagań otoczenia, częste zmiany przepisów prawnych oraz dążenie do wzrostu efektywności, zapewnia metody postępowania dla skutecznej i terminowej obsługi zmian w infrastrukturze teleinformatycznej przy utrzymaniu pożądanego poziomu bezpieczeństwa przetwarzanych danych i ograniczeniu ryzyka negatywnego wpływu zmiany na obsługę teleinformatyczną organizacji.

Proces zarządzania zmianą w Centrum przebiega w następujących etapach:

1. ustalenie celu zmiany;
2. rozważenie wielkości i ważności zmiany dla Cyfronetu i odbiorców usług;
3. określenie momentów krytycznych we wdrożeniu zmiany;
4. zainicjowanie zmiany, przeprowadzenie testów, wdrożenie w systemie produkcyjnym;
5. aktywne włączenie pracowników Centrum w proces zmiany;
6. monitorowanie i raportowanie kolejnych kroków wdrożenia zmiany;
7. zakończenie wdrażania zmiany.

Proces zarządzania zmianami jest dokumentowany za pomocą wewnętrznego systemu informatycznego.

16 Postanowienia końcowe

ACK Cyfronet AGH wymaga zapoznania się pracowników z dokumentami Polityki Bezpieczeństwa Informacji. Za zapoznanie się pracowników z dokumentami odpowiada kierownik każdej komórki organizacyjnej Cyfronetu. Naruszenia świadome bądź przypadkowe Polityki Bezpieczeństwa Informacji (wraz z wszystkimi dokumentami zależnymi) powoduje skutki prawne zgodnie z Regulaminem Pracy, a w przypadkach zastrzeżonych przez ustawodawcę - karne wynikające z odpowiedzialności określonej przez przepisy prawa.

17 Wykaz załączników

Wzory rejestrów wskazane w załącznikach do Polityki Bezpieczeństwa Informacji mogą być prowadzone w wersji papierowej lub elektronicznej.

Załącznik	**Opis**
Załącznik nr 1 – Wzór rejestru LASI - PBI DG	Rejestr LASI Rejestr prowadzi LABI
Załącznik nr 2 – Wzór rejestru usług - PBI DG	Rejestr systemów/usług Rejestr prowadzi LABI Dane dla LABI przygotowuje i przekazuje AS we współpracy z właściwym LASI
Załącznik nr 3 – Wzór rejestru obszarów - PBI DG	Rejestr obszarów (pomieszczeń) o szczególnym znaczeniu dla funkcjonowania ACK Cyfronet AGH w procesie przetwarzania danych Rejestr prowadzi LABF
Załącznik nr 4 – Wzór rejestru AS - PBI DG	Rejestr Administratorów Systemów (AS) Rejestr prowadzi LASI
Załącznik nr 5 – Wzór rejestru osób uprawnionych do przetwarzania danych osobowych - PBI DG	Rejestr osób uprawnionych do przetwarzania danych osobowych Rejestr prowadzi LABI
Załącznik nr 6 – Wzór rejestru sprzętu i oprogramowania - PBI DG	Rejestr sprzętu i oprogramowania z elementami konfiguracji Rejestr prowadzi LASI
Załącznik nr 7 – Wzór rejestru użytkowników systemu - PBI DG	Rejestr użytkowników systemu/usługi Rejestr prowadzi AS
Załącznik nr 8 – Wzór rejestru wejść - PBI DG	Rejestr wejść Rejestr prowadzi LABF
Załącznik nr 9 – Wzór zapisów o powierzeniu danych - PBI DG	Wzór zapisów o powierzeniu danych osobowych
Załącznik nr 10 – Wzór zapisów o zachowaniu poufności - PBI DG	Wzór zapisów umownych o zachowaniu poufności
Załącznik nr 11 – Akty prawne - PBI DG	Akty prawne
Załącznik nr 12 – Kontekst organizacji - PBI DG	Kontekst organizacji
Załącznik nr 13 – Cele bezpieczeństwa informacji	Cele bezpieczeństwa informacji/SZBI
załącznik nr 14 – Pomiar skuteczności zabezpieczeń	Pomiar skuteczności zabezpieczeń

18 Historia zmian

Nr zmiany	Data zmiany	Opis dokonanej zmiany	Obowiązująca wersja

Załącznik nr 1. Wzór rejestru LASI

Lp.	Nazwisko i imię	Dane kontaktowe	Obszar działania	Data wprowadzenia	Data ustania uprawnień	Uwagi

---

Rejestr prowadzony jest przez Lokalnego Administratora Bezpieczeństwa Informacji (LABI)

Załącznik nr 2. Wzór rejestru systemów i usług teleinformatycznych

Lp.	Nazwa ujednolicona	Krótki opis usługi	Właściciel	Zasięg usługi	Ocena istotności*	Administratorzy usługi	Dział realizujący usługę	Lokalizacja serwera (wirtualny)	Uwagi

---

Nazwa ujednolicona*: nazwa usługi poprzedzona skrótem Działu np. DKDM.PLGRID*

* (Krytyczna, Wysoka, Średnia, Niska, Nieistotna)

Załącznik nr 3. Wzór rejestru obszarów (pomieszczeń) o szczególnym znaczeniu dla funkcjonowania Centrum w procesie przetwarzania danych

Lokalizacja	Rodzaj pomieszczenia	Dział	Osoba kontaktowa	Infrastruktura techniczna i zabezpieczenia *	Uwagi

*(Z) – zabezpieczenia - (D) – dozór całodobowy, (KD) – kontrola dostępu, (A) – alarm, (K) – kraty w oknach, (DK) –drzwi zamykane na klucz, (KL) – klimatyzacja, (SP) – sygnalizacja PPOŻ, (GAS) –gaśnice, (SF)- Sejf, (SO) – Sejf Ogniotrwały, (SK)- szafa zamykana na klucz, inne zabezpieczenia

---

Rejestr prowadzony jest przez Lokalnego Administratora Bezpieczeństwa Fizycznego (LABF).

Załącznik nr 4. Wzór rejestru Administratorów Systemów (AS)

Lokalny Administrator Systemów Informatycznych (imię i nazwisko) ……..

Lp.	Dział	Nazwisko Imię	Dane kontaktowe	Nazwa systemu/usługi	Data nadania uprawnień	Data ustania uprawnień	Uwagi

---

Rejestr jest prowadzony przez właściwego Lokalnego Administratora Systemów Informatycznych (LASI)

Załącznik nr 5. Wzór rejestru osób uprawnionych do przetwarzania danych osobowych

<table>
<tr><td>RRRR</td><td>Imię i nazwisko</td><td colspan="2">ACK-...</td><td colspan="2">...</td><td colspan="2">.....</td></tr>
<tr><td>(rok)</td><td>(referent)</td><td colspan="2">(symbol kom.org.)</td><td colspan="2">(oznacz. teczki)</td><td colspan="2">(tytuł teczki wg wykazu akt)</td></tr>
<tr><td rowspan="2">Lp.</td><td rowspan="2">Sprawa (krótka treść)</td><td colspan="2">Od kogo wpłynęła</td><td colspan="2">Data</td><td rowspan="2">Uwagi (sposób załatwienia)</td></tr>
<tr><td>znak pisma</td><td>z dnia</td><td>wszczęcia sprawy</td><td>ostatecznego załatwienia</td></tr>
<tr><td rowspan="2">1.</td><td rowspan="2">Upoważnienie do przetwarzania danych osobowych dla</td><td colspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="2">2.</td><td rowspan="2">Upoważnienie do przetwarzania danych osobowych dla</td><td colspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="2">3.</td><td rowspan="2">Upoważnienie do przetwarzania danych osobowych dla</td><td colspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td></td><td></td></tr>
</table>

Rejestr prowadzony jest przez Lokalnego Administratora Bezpieczeństwa Informacji

Załącznik nr 6. Wzór rejestru sprzętu i oprogramowania z elementami konfiguracji

Lokalny Administrator Systemów Informatycznych (imię i nazwisko) …….

I. Rejestr sprzętu wraz z konfiguracją:

Nazwa	Istotność	Lokalizacja	Producent	Model	Opis wraz z konfiguracją	Numer inwentarzowy	Data zakupu	Koniec gwarancji	Uwagi

II. Licencje oprogramowania:

Nazwa	Rodzaj licencji	Licencjodawca	Ilość licencji	Opis licencji	Ważna do	Osoba korzystająca z licencji*	Numer licencji	Uwagi

* W przypadku licencji wielostanowiskowych należy podać Administratora Systemu.

Rejestr prowadzony jest przez Lokalnego Administratora Systemów Informatycznych (LASI).

Rejestr jest prowadzony w postaci elektronicznej.

W rejestrze sprzętu uwzględnia się zapisy dotyczące sprzętu z istotnością, co najmniej **Krytyczna, Wysoka, Średnia.**

Załącznik nr 7. Wzór rejestru użytkowników systemu/usługi

Administrator Systemu (imię i nazwisko) …….

System (nazwa) ……

Użytkownik	Identyfikator (login)	Rola w systemie	Data nadania uprawnień	Data odebrania uprawnień	Status	Uwagi

---

Rejestr prowadzony jest przez Administratora Systemu (AS)

Załącznik nr 8. Wzór rejestru wejść osób obcych do pomieszczenia chronionego

Lp.	Data	Imię i nazwisko	Pomieszczenie	Godzina wejścia	Godzina wyjścia	Powód wizyty	Uwagi

---

Rejestr jest prowadzony przez Lokalnego Administratora Bezpieczeństwa Fizycznego (LABF)

Załącznik nr 9. Wzór zapisów umownych o powierzeniu danych osobowych

UMOWA W SPRAWIE POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w Krakowie w dniu …… r. pomiędzy:
……..,
reprezentowanym/-ą przez:

- …… - ……,
- …… - ……,

zwanym/-ą dalej „**Administratorem**”,

a

Akademią Górniczo-Hutniczą im. St. Staszica w Krakowie, Akademickim Centrum Komputerowym Cyfronet AGH, ul. Nawojki 11, 30-950 Kraków, NIP: 675-000-19-23, REGON: 000001577-00022**,** reprezentowaną przez

- ……,

zwaną dalej „**Podmiotem Przetwarzającym**”,

zwanymi dalej: „**Stronami”,**
zwana dalej: „**Umową**”

§ 1
PRZEDMIOT UMOWY

1. W związku z zawarciem przez Strony w dniu …….. roku umowy …… (zwanej dalej **„Umową główną”**) oraz działając na podstawie art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej **„Rozporządzeniem”**) Administrator powierza Podmiotowi Przetwarzającemu dane osobowe do przetwarzania w zakresie i na zasadach określonych w niniejszej Umowie.
2. Administrator oświadcza, że jest administratorem w rozumieniu przepisów Rozporządzenia i przetwarza dane osobowe zgodnie z obowiązującymi przepisami prawa.
3. Na podstawie Umowy Podmiot Przetwarzający zobowiązuje się przetwarzać dane osobowe wyłącznie w następującym zakresie i na następujących zasadach:
   a) …… (przedmiot przetwarzania),
   b) dane osobowe dotyczące (kategoria osób, których dane dotyczą):
      i. ……..,
      ii. ……..,
      iii. ……..;
   c) dane osobowe obejmujące (rodzaj danych):
      i. ……..,
      ii. ……..,
      iii. ……..,
      iv. ……..,
   d) przy wykorzystaniu ……., wykonując takie operacje jak: ……. (charakter przetwarzania),
   e) w celu realizacji Umowy głównej (cel przetwarzania),
   f) w okresie obowiązywania Umowy Głównej (czas trwania przetwarzania).
4. Przetwarzanie danych osobowych przez Podmiot Przetwarzający odbywać się będzie wyłącznie na udokumentowane polecenie Administratora.
5. Za udokumentowane polecenie przetwarzania danych Strony uznają:
   a) niniejszą Umowę,
   b) Umowę główną,
   c) inne udokumentowane polecenia, w tym przekazane za pośrednictwem wiadomości e-mail.

§ 2
OŚWIADCZENIA STRON

1. Podmiot Przetwarzający oświadcza, iż jest podmiotem znającym specyfikę procesu przetwarzania danych i że są mu znane przepisy, na podstawie których może przetwarzać dane osobowe, w szczególności przepisy Rozporządzenia.
2. Podmiot Przetwarzający zobowiązuje się przetwarzać dane zgodnie z obowiązującymi przepisami prawa oraz Umową a także dochować należytej staranności przy przetwarzaniu powierzonych mu danych osobowych.
3. Podmiot Przetwarzający oświadcza, iż stosuje środki bezpieczeństwa, które zapewniają należytą ochronę danych osobowych i spełniają wymogi, o których mowa w art. 32 Rozporządzenia. Jednocześnie Podmiot Przetwarzający, w razie uzasadnionej konieczności, zmodyfikuje odpowiednio stosowane przez siebie środki bezpieczeństwa w taki sposób, by zachowane były standardy bezpieczeństwa adekwatne do rodzaju przetwarzanych danych i związanego z procesem przetwarzania danych osobowych ryzyka.
4. Podmiot Przetwarzający zapewnia, że w procesie przetwarzania danych osobowych w ramach wykonywania Umowy będą brały udział wyłącznie osoby imiennie upoważnione do przetwarzania danych osobowych oraz przeszkolone z zakresu przepisów dotyczących ochrony danych osobowych. Tym samym Podmiot Przetwarzający zobowiązuje się nadać tym osobom stosowne upoważnienia oraz wydawać w imieniu Administratora stosowne polecenia co do przetwarzania danych osobowych przetwarzanych dla Administratora.
5. Podmiot Przetwarzający zobowiązuje się zapewnić ochronę przetwarzanych danych osobowych poprzez zobowiązanie osób upoważnionych do przetwarzania danych osobowych w ramach wykonywania Umowy do zachowania tajemnicy, o której mowa w art. 28 ust. 3 lit. b) Rozporządzenia, zarówno w trakcie ich zatrudnienia (lub istnienia innego stosunku współpracy) jak również po jego ustaniu.
6. Administrator oświadcza, że wypełnia wobec osób, których dane powierza Podmiotowi Przetwarzającemu do przetwarzania obowiązek informacyjny wynikający z art. 13 i 14 Rozporządzenia.

§ 3
ZASADY WSPÓŁPRACY

1. Strony zobowiązują się do wzajemnej współpracy w zakresie przetwarzania danych objętych Umową, w szczególności Strony zobowiązują się do współpracy w zakresie realizacji obowiązku udzielania odpowiedzi na zapytania osób, których dane osobowe są przetwarzane oraz wywiązywania się z obowiązków, o których mowa w art. 32-36 Rozporządzenia.
2. Podmiot Przetwarzający zobowiązuje się niezwłocznie zawiadomić Administratora o każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba że zakaz zawiadomienia wynika z przepisów prawa oraz o każdym żądaniu otrzymanym od osoby, której dane przetwarza.
3. Podmiot Przetwarzający udostępnia Administratorowi niezbędne informacje w celu wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.
4. Podmiot Przetwarzający umożliwia osobie lub osobom upoważnionym przez Administratora przeprowadzanie audytów, w tym inspekcji, dotyczących sposobu wykonania Umowy, a także udziela niezbędnej pomocy przy ich przeprowadzaniu. Zarówno audyt jak i inspekcja będą przeprowadzane – z wyłączeniem przypadków wymagających takich czynności niezwłocznie, wskutek wykrycia nieprawidłowości lub na polecenie organu nadzorującego – co do zasady nie częściej niż 2 razy w roku.
5. O skorzystaniu z prawa przeprowadzenia audytu lub inspekcji Administrator powinien uprzedzić Podmiot Przetwarzający w miarę możliwości co najmniej z 14-dniowym wyprzedzeniem. Administrator informuje w takim przypadku o okresie planowanej kontroli oraz o zakresie czynności kontrolnych kierując w tym celu do Podmiotu Przetwarzającego pisemne zawiadomienie.
6. Czynności, o których mowa w ust. 4, powinny zostać przeprowadzone z uwzględnieniem godzin pracy Podmiotu Przetwarzającego, w sposób możliwie niezakłócający pracy.

7. Podmiot Przetwarzający zobowiązuje się do usunięcia wszelkich uchybień stwierdzonych podczas audytu i opisanych w końcowym protokole. Usunięcie uchybień powinno nastąpić niezwłocznie, nie później jednak niż w terminie 30 dni od zakończenia audytu i przedstawienia przez Administratora końcowego protokołu.
8. Podmiot Przetwarzający, w przypadku stwierdzenia naruszenia lub uzasadnionego podejrzenia naruszenia ochrony danych osobowych, które na mocy Umowy przetwarza zobowiązany jest niezwłocznie, nie później niż w przeciągu 24 godzin zwykłych od stwierdzenia naruszenia, poinformować Administratora o danym zdarzeniu oraz przekazać Administratorowi wszelkie informacje niezbędne do dokonania przez Administratora zgłoszenia naruszenia Prezesowi Urzędu Ochrony Danych Osobowych, o których to informacjach mowa w art. 33 ust. 3 Rozporządzenia. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić we wskazanym powyżej czasie, Podmiot Przetwarzający może je udzielać sukcesywnie bez zbędnej zwłoki.
9. Podmiot Przetwarzający niezwłocznie informuje Administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie Rozporządzenia lub innych przepisów prawa dotyczących ochrony danych, obowiązujących w Polsce lub wydanych przez Unię Europejską.

§ 4
PODPOWIERZENIE DANYCH OSOBOWYCH

1. Podmiot Przetwarzający może powierzyć dane osobowe objęte Umową – wyłącznie w celu wykonania Umowy – do dalszego przetwarzania innym podmiotom jedynie po uzyskaniu uprzedniej pisemnej zgody Administratora.
2. Przekazanie powierzonych danych do państwa trzeciego lub organizacji międzynarodowej może nastąpić jedynie na pisemne polecenie Administratora, chyba że obowiązek taki nakłada na Podmiot Przetwarzający prawo polskie lub prawo Unii Europejskiej. W takim przypadku, przed rozpoczęciem przetwarzania, Podmiot Przetwarzający informuje Administratora o tym obowiązku, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podmiot, któremu zostanie powierzone przetwarzanie danych osobowych w ramach podpowierzenia, winien spełniać te wymogi, do spełnienia których zobowiązany jest Podmiot Przetwarzający na podstawie niniejszej Umowy, a także dawać gwarancję należytego wykonania obowiązków ochrony danych osobowych.
4. Podmiot Przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podmiocie, któremu zostało podpowierzone przetwarzanie danych osobowych, obowiązków ochrony danych osobowych.

§ 5
CZAS OBOWIĄZYWANIA UMOWY

1. Umowa zostaje zawarta na czas od dnia jej zawarcia do dnia zakończenia obowiązywania Umowy głównej.
2. Po zakończeniu obowiązywania Umowy, Podmiot Przetwarzający – zależnie od decyzji Administratora – zobowiązany jest do zwrotu albo do usunięcia w sposób uniemożliwiający odtworzenie wszelkich danych osobowych uzyskanych w związku z realizacją Umowy oraz usunięcia w sposób uniemożliwiający odtworzenie ich kopii najpóźniej w terminie 30 dni od dnia zakończenia obowiązywania Umowy, chyba że prawo polskie lub prawo Unii Europejskiej nakazują przechowywanie danych osobowych.

§ 6
ZASADY ZACHOWANIA POUFNOŚCI

1. Strony zobowiązują się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Drugiej Strony i od współpracujących z nią osób a jednocześnie uzyskanych w związku z realizacją Umowy oraz uzyskanych w jakikolwiek inny sposób, zamierzony lub przypadkowy, w formie ustnej, pisemnej lub elektronicznej, a które to informację, dane, materiały, dokumenty i dane osobowe są związane z Umową (dalej zwane **„Informacjami Poufnymi”**).

2. Strony oświadczają, że w związku z zobowiązaniem do zachowania w tajemnicy Informacji Poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Drugiej Strony w innym celu niż wykonanie Umowy, chyba że konieczność ich ujawnienia wynika z obowiązujących przepisów lub Umowy.
3. Podmiot Przetwarzający zobowiązuje się do ujawnienia Informacji Poufnych jedynie tym osobom, którym będą one niezbędne do wykonywania powierzonych im czynności w ramach realizacji Umowy i tylko w takim zakresie, w jakim odbiorca Informacji Poufnych musi mieć do nich dostęp dla celów realizacji zadania wynikającego z tytułu realizacji Umowy.
4. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, aby środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania Informacji Poufnych gwarantowały ich bezpieczeństwo, w tym w szczególności bezpieczeństwo danych osobowych powierzonych do przetwarzania, przed dostępem osób trzecich nieuprawnionych do zapoznania się z ich treścią.
5. Obowiązek zachowania w tajemnicy Informacji Poufnych obowiązuje także po zakończeniu obowiązywania Umowy przez okres zachowania przez Informacje Poufne wartości gospodarczej, nie krócej jednak niż przez 3 lata.

§ 7
OSOBY DO KONTAKTU

1. W związku z realizacją Umowy Strony ustalają następujące osoby do kontaktu:
   a) za Administratora: ……,
      tel.: ……, e-mail: ……..
   b) za Podmiot Przetwarzający: ……
      tel.: …….. e-mail: …….
2. W przypadku potrzeby zmiany danych osób, o których mowa w ust. 1, Strona dokonująca zmiany zawiadamia niezwłocznie o niej Drugą Stronę na piśmie niezwłocznie, nie później niż w terminie 7 dni od dnia dokonania zmiany. W razie niedopełnienia tej powinności informacje przekazane osobie ustalonej w Umowie uznaje się za przekazane prawidłowo i bez naruszenia Umowy.

§ 8
POSTANOWIENIA KOŃCOWE

1. Strony oświadczają, że wypełniły/wypełnią wobec osób, których dane przywołały w niniejszej Umowie oraz osób, których dane kontaktowe udostępnią w celu realizacji Umowy obowiązek informacyjny wynikający z art. 13 i 14 Rozporządzenia.
2. Strony oświadczają, iż w przypadku, gdy którekolwiek z postanowień Umowy, z mocy prawa lub ostatecznego albo prawomocnego orzeczenia sądu lub jakiegokolwiek organu administracyjnego, zostaną uznane za nieważne lub nieskuteczne, pozostałe postanowienia Umowy zachowują pełną moc i skuteczność. Postanowienia Umowy nieważne lub nieskuteczne zostaną zastąpione postanowieniami ważnymi w świetle prawa i skutecznymi.
3. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
4. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
5. W sprawach nieuregulowanych w Umowie zastosowanie będą miały przepisy powszechnie obowiązującego prawa, a w szczególności Kodeksu cywilnego oraz Rozporządzenia.
6. Sądem właściwym dla rozpatrzenia sporów wynikających z Umowy będzie sąd właściwy miejscowo dla Podmiotu Przetwarzającego.

……	……
(za Administratora)	(za Podmiot Przetwarzający)

Załącznik nr 10. Wzór zapisów umownych o zachowaniu poufności

UMOWA
O ZACHOWANIU POUFNOŚCI

zawarta pomiędzy:

Akademią Górniczo-Hutniczą w Krakowie
Akademickim Centrum Komputerowym Cyfronet AGH
ul. Nawojki 11, 30-950 Kraków
numer NIP: 6750001923
które reprezentuje:
Dyrektor – Prof. dr hab. inż. Kazimierz Wiatr
zwanym dalej „**Cyfronet”** a

…….
……
którą reprezentuje:
……
zwaną dalej: „**……**”
zwanymi dalej łącznie „**Stronami**” lub indywidualnie **„Stroną”**.

Strony umowy zwane są dalej także „**Stroną Ujawniającą**”, jeżeli udostępniają innej Stronie albo Stronom informacje poufne, albo „**Stroną Otrzymującą**”, jeżeli uzyskują informacje poufne.

Zważywszy na to, iż Strony zamierzają podjąć współpracę , a co za tym idzie udostępniają lub będą udostępniać wzajemnie informacje poufne, zawierają niniejszą umowę, której przedmiotem jest określenie i stosowanie procedur mających na celu ochronę informacji poufnych, w myśl obowiązujących przepisów.

§ 1
Informacje Poufne

Na potrzeby niniejszej Umowy przez **”Informacje Poufne”** rozumie się wszelkie informacje, w szczególności określone w § 2 ust. 1 niniejszej umowy, niezależnie od ich postaci i formy przekazania, które zostały udostępnione przez jedną ze Stron (Stronę Ujawniającą) drugiej Stronie (Stronie Otrzymującej) w związku z podjętą współpracą.

§ 2
Warunki zachowania poufności

1. Strony zobowiązują się:
   a) zachować w ścisłej tajemnicy wszelkie dane, materiały, informacje, w szczególności wszelkie informacje ujawnione przez Stronę Ujawniającą drugiej Stronie umowy (Stronie Otrzymującej) w trakcie podjętej współpracy lub w związku z tą współpracą, w tym również w trakcie prowadzenia negocjacji mających na celu rozpoczęcie współpracy, a także informacje, do których Strona Otrzymująca mimowolnie lub w inny sposób uzyskała dostęp np. podczas spotkań, wizyt w zakładach, laboratoriach i/lub siedzibach drugiej Strony, w szczególności dotyczące organizacji, technologii, działalności, dane dotyczące kontrahentów, pracowników, biznesowe, techniczne, ekonomiczne, finansowe, handlowe, prawne, inne informacje posiadające wartość gospodarczą, wszelkie informacje dotyczące Strony Ujawniającej, nie podane do wiadomości publicznej, a uzyskane teraz lub w przyszłości w związku z podjętą współpracą, a także informacje, których ujawnienie lub wykorzystanie mogłoby narazić Strony lub ich kontrahentów na szkodę – niezależnie od formy przekazania tych informacji i ich źródła;

b) wykorzystywać Informacje, o których mowa w ust. 1. lit. a) wyłącznie w celach określonych ustaleniami dokonanymi przez Strony w związku z podjętą współpracą;
c) przekazywać Informacje, o których mowa w ust. 1. lit. a) jedynie tym pracownikom, współpracownikom, którym będą one niezbędne do realizacji powierzonych im zadań w związku z podjętą przez Strony współpracą, w zakresie niezbędnym do ich realizacji, z zastrzeżeniem, że osoby te są związane obowiązkiem zachowania poufności w stopniu co najmniej odpowiadającym postanowieniom niniejszej umowy;
d) podjąć wszelkie niezbędne kroki dla zapewnienia, że żadna z osób otrzymujących Informacje w myśl ust. 1. lit. c) nie ujawni tych informacji, ani ich źródła, zarówno w całości, jak i w części, stronom trzecim bez uzyskania uprzedniego wyraźnego upoważnienia na piśmie od Strony, której Informacja lub źródło Informacji dotyczy;
e) nie kopiować, nie powielać ani w jakikolwiek sposób nie rozpowszechniać jakichkolwiek Informacji określonych w ust. 1. lit. a) lub ich części, z wyjątkiem uzasadnionej potrzeby do celów określonych w ust. 1. lit. b). Wszelkie wykonane kopie będą określone jako należące do Strony Ujawniającej i traktowane jako poufne;
f) dołożyć wszelkich starań w celu zapewnienia, aby środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania Informacji, o których mowa w ust. 1. lit. a) gwarantowały ich bezpieczeństwo przed dostępem osób trzecich nieuprawnionych do zapoznania się z ich treścią.

2. Postanowienia ust. 1. nie będą miały zastosowania w stosunku do tych Informacji uzyskanych od drugiej Strony, które:
   a) są opublikowane, powszechnie znane lub urzędowo podane do publicznej wiadomości bez naruszenia postanowień niniejszej umowy;
   b) są znane danej Stronie umowy przed przystąpieniem do współpracy/podpisaniem niniejszej umowy lub zostały przekazane przez osobę trzecią, bez naruszenia jakichkolwiek zobowiązań do ich nie ujawniania w stosunku do Stron;
   c) zostaną ujawnione przez jedną ze Stron za uprzednią pisemną zgodą drugiej Strony;
   d) których obowiązek ujawnienia wynika z przepisów prawa, w tym ustawy o dostępie do informacji publicznej, decyzji sądów, decyzji władz państwowych lub samorządowych wydanych na podstawie właściwych przepisów prawa lub w związku z toczącym się postępowaniem kontrolnym, sądowym, administracyjnym lub przed sądem polubownym, w takim wypadku Strona zobowiązana do ich ujawnienia jest zobowiązana do niezwłocznego poinformowania drugiej Strony o ich ujawnieniu, chyba że powiadomienie drugiej Strony w danym wypadku było niewykonalne, nieuzasadnione lub sprzeczne z prawem oraz podjęcia wszelkich prawnie dozwolonych działań zmierzających do zminimalizowania zakresu przekazywanych informacji, w szczególności żądać wyłączenia jawności;
   e) które zostały niezależnie i samodzielnie opracowane przez Stronę bez dostępu lub wykorzystania Informacji Poufnych.
3. Strona ujawniająca Informacje Poufne i powołująca się na okoliczności wskazane w ust. 2. jest zobowiązana do ich udowodnienia.

§ 3
Czas obowiązywania; rozwiązanie umowy

1. Zobowiązania wynikające z postanowień niniejszej umowy wiążą Strony na czas współpracy Stron oraz przez okres 5 lat od dnia ustania tej współpracy.
2. Rozwiązanie niniejszej umowy z jakiegokolwiek powodu nie zwolni Stron z odpowiedzialności, która w chwili rozwiązania powstała już w stosunku do drugiej Strony lub która może powstać w odniesieniu do działań lub zaniechań z okresu przed rozwiązaniem niniejszej umowy.
3. W przypadku zakończenia współpracy lub rozwiązania niniejszej umowy oraz na każde pisemne wezwanie Strony Ujawniającej, Strona Otrzymująca zobowiązana będzie do niezwłocznego zwrotu wszystkich dokumentów i informacji zawierających Informacje Poufne, z zastrzeżeniem prawa Strony Otrzymującej do zachowania jednej kopii Informacji Poufnych, w ścisłej poufności, wyłącznie w celu wykonania swoich zobowiązań wynikających z przepisów prawa lub z niniejszej

umowy. Zwrot dokumentów i informacji nie zwalnia Strony Otrzymującej z obowiązku zachowania w poufności powierzonych jej Informacji Poufnych na zasadach określonych w niniejszej umowie.

§ 4
Prawo do Informacji Poufnych

1. Wszelkie prawa do Informacji Poufnych w stosunkach pomiędzy Stronami przysługują Stronie Ujawniającej, o ile Strony wyraźnie nie postanowiły inaczej na piśmie pod rygorem nieważności.
2. Prawa do utworów przygotowanych z wykorzystaniem Informacji Poufnych przysługują Stronie, która przygotowała taki utwór, co nie uchybia obowiązkowi uzyskania zgody drugiej Strony na ujawnienie Informacji Poufnych w tym utworze.

§ 5
Postanowienia końcowe

1. Strony oświadczają, że ani niniejsza umowa, ani też przewidziane niniejszą umową ujawnienie jakichkolwiek Informacji Poufnych przez jedną Stronę drugiej Stronie, nie stanowi udzielenia licencji w rozumieniu ustawy z dnia 30 czerwca 2000 r. Prawo własności przemysłowej (t.j. Dz. U. z 2021 r., poz. 324 z późn. zm.) oraz ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2021 r., poz. 1062 z późn. zm.), ani przeniesienia na Stronę Otrzymującą praw autorskich, patentów, zgłoszeń patentowych, znaków towarowych, tajemnic handlowych i know-how.
2. Każda ze Stron odpowiada za zachowanie poufności Informacji zgodnie z postanowieniami niniejszej umowy przez swoich pracowników i współpracowników jak za działania i zaniechania własne.
3. Strona Otrzymująca, która ujawni Informację Poufną drugiej Strony wbrew postanowieniom umowy, zwalnia tę Stronę (Stronę Ujawniającą Informację Poufną) od odpowiedzialności wobec osób trzecich za wszelkie skutki takiego ujawnienia, jak i za samo ujawnienie.
4. W przypadku naruszenia postanowień niniejszej umowy Strony mogą w każdym momencie żądać niezwłocznego zaniechania wykonania jakichkolwiek czynności związanych z prowadzoną współpracą.
5. W przypadku powstania szkody na skutek naruszenia jakiegokolwiek postanowienia niniejszej umowy przez którąkolwiek ze Stron, Strony mogą zgłaszać roszczenia odszkodowawcze zgodnie z ogólnymi zasadami prawa. Strony wyłączają względem siebie odpowiedzialność z tytułu utraconych korzyści.
6. Niewykonanie przez którąkolwiek ze Stron przysługujących jej praw na wypadek naruszenia postanowień niniejszej umowy przez drugą Stronę nie będzie rozumiane, jako zrzeczenie się takich praw w przypadku późniejszych naruszeń ani jakichkolwiek innych praw przewidzianych niniejszą umową.
7. Żadna Strona nie może dokonać przeniesienia praw lub obowiązków wynikających z umowy, ani zwolnić się z tych obowiązków bez uprzedniej zgody drugiej Strony udzielonej w formie pisemnej pod rygorem nieważności.
8. Żadna ze Stron nie może używać nazwy lub logo drugiej Strony w publikacjach i przekazach o charakterze reklamowym, bez uzyskania uprzedniej zgody drugiej Strony wyrażonej w formie pisemnej pod rygorem nieważności.
9. Żadna Strona nie będzie zabiegać ani podejmować działań zmierzających do zatrudnienia na podstawie jakiegokolwiek tytułu, w szczególności (lecz nie wyłącznie) na podstawie umowy o pracę, zlecenia, o dzieło, kontraktu menadżerskiego (bezpośrednio ani za pośrednictwem podmiotów powiązanych lub osób trzecich) pracowników drugiej Strony przez okres, o którym mowa w § 3 ust. 1 niniejszej umowy, bez uzyskania uprzedniej zgody drugiej Strony wyrażonej w formie pisemnej pod rygorem nieważności. W przypadku naruszenia przez Stronę postanowień niniejszego punktu, Strona ta zapłaci na rzecz drugiej Strony karę umowną w wysokości …….. PLN (słownie …… złotych) za każde naruszenie. Zapłata kary umownej nie pozbawia drugiej Strony prawa dochodzenia odszkodowania przewyższającego wysokość kary umownej, na zasadach ogólnych. Powyższe nie będzie miało zastosowania do sytuacji, w której pracownik

Strony odpowiada na publiczne ogłoszenie zamieszczone przez drugą Stronę, w szczególności w Internecie lub w prasie.

10. Do niniejszej umowy zastosowanie mają przepisy prawa polskiego.
11. Wszelkie spory wynikające z niniejszej umowy lub w związku z nią będą rozstrzygane przez sąd właściwy dla siedziby Cyfronet.
12. Wszelkie zawiadomienia i oświadczenia oraz inna korespondencja przewidziane w niniejszej umowie przekazywane drugiej Stronie będą w formie pisemnej w języku polskim i będą doręczane osobiście lub listem poleconym z potwierdzeniem odbioru na adres odbiorcy wskazany w niniejszej umowie, lub na taki inny adres, który Strona może wskazać poprzez zawiadomienie dokonane zgodnie z postanowieniami niniejszego ustępu.
13. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
14. Umowa zostaje zawarta w postaci elektronicznej opatrzonej elektronicznym podpisem kwalifikowanym.
15. Datą zawarcia niniejszej umowy jest data złożenia podpisu przez ostatnią z osób wskazanych w komparycji umowy.

.....	.....
……	Cyfronet

Załącznik nr 11. Rejestr aktów prawnych

Rejestr aktów prawnych dotyczących SZBI		
Przepisy ogólne		
L.p.	**Akt prawny**	**Dziennik ustaw**
1.	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych	Dz.U. 2018 poz. 1000
2.	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (RODO)	Dz.U.UE.L.2016.119.1
3.	Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych	Dz.U. 1994 nr 24 poz. 83
4.	Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej	Dz.U. 2001 nr 112 poz. 1198
5.	Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne	Dz.U. 2005 nr 64 poz. 565
6.	Rozporządzenie Rady Ministrów z dnia z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych	Dz.U. 2012 poz. 526
7.	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa	Dz.U. 2018 poz. 1560
8.	Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych	Dz.U. 2016 poz. 904

Załącznik nr 12. Kontekst organizacji

Źródło czynników	Rodzaj czynników	Czy ma zastosowanie	Opis czynnika lub odwołanie do dokumentacji	Zmiany w odniesieniu do poprzedniej wersji
Czynniki zewnętrzne				
Środowisko organizacji - międzynarodowe, krajowe, regionalne lub lokalne	Kulturowe	TAK	Współpraca zagraniczna	Nie dotyczy
	Społeczne	NIE		Nie dotyczy
	Polityczne	NIE		Nie dotyczy
	Prawne	TAK	Jest wiele przepisów określających wymagania w branży. Istnieją normy dotyczące zapewnienia dostępności i ciągłości działania.	Nie dotyczy
	Regulacyjne	TAK	Istnieją umowy o współpracę z dostawcami zewnętrznymi	Nie dotyczy
	Finansowe	TAK	Usługi komercyjne	Nie dotyczy
	Technologiczne	TAK	Musi być zapewniony sprzęt IT, serwery, zasilanie	Nie dotyczy
	Ekonomiczne	TAK	usługi komercyjne	Nie dotyczy
	Naturalne	TAK	Siedziba ACK Cyfronet AGH znajduje się w budynku biurowym, będącym własnością AGH.	Nie dotyczy
	Konkurencyjne	TAK	Istnieje konkurencja na rynku.	Nie dotyczy
Wpływ na cele	Kluczowe Czynniki	TAK	Dostępność serwerów zewnętrznych i usług internetowych. Nowa technologia wymaga zwiększonych nakładów na promocję. Niezawodność działania. Rotacja programistów. Rozwój produktów. Bezpieczeństwo systemów.	Nie dotyczy
	Trendy	NIE		Nie dotyczy

Interesariusze zewnętrzni	Relacje	TAK	Klienci, dostawcy, wymagania branżowe.	Nie dotyczy
	Postrzeganie	TAK	Jakość dostarczanych rozwiązań, terminowość.	Nie dotyczy
	Wartości	NIE		Nie dotyczy
Czynniki wewnętrzne				
Zarządzanie	Zarządzanie	TAK	Wdrożenie i certyfikowanie systemu zarządzania bezpieczeństwem informacji wg. ISO27001	Nie dotyczy
Struktura organizacyjna	Struktura Organizacyjna	TAK	Podział zadań, strategia i cele, potencjał organizacji, relacje z interesariuszami wew. oraz zewn.; PBI DG	Nie dotyczy
Role i odpowiedzialności	Role i Odpowiedzialności	TAK	Zakresy obowiązków, opis funkcji w PBI DG	Nie dotyczy
Polityki bezpieczeństwa informacji	Polityki Bezpieczeństwa Informacji	TAK	Polityka ochrony danych osobowych; Polityki SZBI	Nie dotyczy
Cele dot. bezpieczeństwa informacji	Cele Dot. Bezpieczeństwa Informacji	TAK	Ochrona technologii, danych Klientów i Dostawców zdobywanie wiarygodności kontrahentów	Nie dotyczy
Strategie	Strategie	TAK	Utrzymywanie marki solidnego, innowacyjnego dostawcy w branży	Nie dotyczy
Zdolność organizacji - zasoby i wiedza	Kapitał	NIE		Nie dotyczy
	Czas	NIE		Nie dotyczy
	Zasoby Ludzkie	TAK	Zarząd, pracownicy firmy, podwykonawcy zewnętrzni	Nie dotyczy
	Procesy	TAK	Dokumentacja wewnętrzna	Nie dotyczy
	Systemy	TAK	Systemy świadczące usługi dla klientów są rozwiązaniami własnymi Centrum	Nie dotyczy

	Technologie	TAK	Użyte technologie gwarantują świadczenie usługi na wysokim poziomie przy utrzymaniu wysokiego stopnia SLA	Nie dotyczy
Systemy informacyjne	Systemy Informacyjne	TAK	Instrukcja zarządzania systemami IT	Nie dotyczy
Przepływy informacji	Przepływy Informacji	TAK	Przepływ informacji reguluje Regulamin Organizacyjny	Nie dotyczy
Procesy decyzyjne	Procesy decyzyjne	TAK	Szybki proces decyzyjny (decyduje Dyrektor lub Dyrekcja zgodnie z posiadanymi upoważnieniami)	Nie dotyczy
Interesariusze wew.	Relacje	TAK	Struktura organizacyjna ACK Cyfronet AGH określa zależności pomiędzy poszczególnymi działami	Nie dotyczy
	Postrzeganie	TAK	Przejrzysta struktura organizacyjna	Nie dotyczy
	Wartości	TAK	Rzetelność, wysokie kompetencje, nastawienie na klienta, jakość i terminowość	Nie dotyczy
Kultura organizacyjna	Kultura Organizacyjna	TAK	Współpraca zorientowana na terminową realizację zadań	Nie dotyczy
Przyjęte przez organizację	Standardy	TAK	RODO, PZP, Dyscyplina Finansów Publicznych	Nie dotyczy
	Dobre Praktyki	TAK	ITSM, AGILE, BCP, ITIL	Nie dotyczy
	Modele	NIE		Nie dotyczy
Wymagania kontraktowe	Wymagania Kontraktowe	TAK	Przestrzeganie zaleceń wynikających z przepisów PZP	Nie dotyczy

Interesariusze zewnętrzni

Interesariusz	Pełna nazwa	Regulacje prawne mające wpływ na organizację	Czy ma zastosowanie w PBI
UODO	Urząd Ochrony Danych Osobowych	Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. 2019 poz. 125)	TAK
		Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. 2014, poz. 1934)	NIE
		Rozporządzenie ministra spraw wewnętrznych i administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2004 r. Nr 94, poz. 923) i Rozporządzenie ministra spraw wewnętrznych i administracji z dnia 11 maja 2011 r. zmieniające rozporządzenie w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2011 r. Nr 103, poz. 601)	NIE
		Rozporządzenie ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)	TAK

		USTAWA Z dn.10.05.2018 o ochronie danych osobowychROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)	TAK
Konsultanci	Konsultanci, Współpracownicy	umowa o zachowaniu poufności	TAK
		umowa o świadczenie usług	TAK
JC	Jednostka Certyfikująca	Norma ISO/IEC 27001 Norma ISO/IEC 27018	NIE
Księgowość, kadry i płace	Dostawca systemu księgowego	Polityka Bezpieczeństwa Informacji, umowa o współpracy – powierzenie przetwarzania danych	NIE
Dostawcy mediów telekomunikacyjnych, Dostawcy oprogramowania, rozwiązań chmurowych, Dostawcy Sprzętu IT	Dostawcy mediów telekomunikacyjnych, Dostawcy oprogramowania, rozwiązań chmurowych, Dostawcy Sprzętu IT	Umowy dostaw i konserwacji sprzętu	TAK
Dostawcy prądu, Dostawcy sprzętu i konserwacja sprzętu	Dostawcy prądu, Dostawcy sprzętu i konserwacja sprzętu	Umowy dostaw i konserwacji sprzętu	TAK

Interesariusze wewnętrzni

Interesariusz	Powiązania wewnętrzne	Regulacje wewnętrzne	Interesariusze zewnętrzni	Czy ma zastosowanie w PBI
ADO	Dyrekcja, Kierownicy działów	Polityka Bezpieczeństwa Informacji, Polityka bezpieczeństwa chmury	UODO, Klienci, Konsultanci, Jednostka Certyfikująca, zewnętrzna firma księgowa	TAK

Auditor wewnętrzny	Dyrekcja	Polityka bezpieczeństwa, Polityka bezpieczeństwa chmury	nie dotyczy	TAK
Programiści IT, Testerzy	Dyrekcja, Kierownicy działów	Wewnętrzne procedury i instrukcje	Dostawcy mediów telekomunikacyjnych, Dostawcy oprogramowania, rozwiązań chmurowych, Dostawcy Sprzętu IT, Serwis sprzętu IT	TAK

Załącznik nr 13. Cele bezpieczeństwa informacji

Cel	Odnośnik z Polityki SZBI	Działanie	Miernik/ weryfikacja	Zasoby	Termin realizacji działania	Odpowiedzialny za zrealizowanie działania
Zapewnienie prawidłowego funkcjonowania SZBI	postępowanie zgodnie z obowiązującymi prawami i normami w zakresie bezpieczeństwa informacji i innymi wymaganiami oraz wewnętrznymi regułami organizacji;	Weryfikacja na podstawie pomiaru skuteczności zabezpieczeń – określenie i uzupełnienie braków, podjęcie działań korygujących, bądź wdrożenie dodatkowych zabezpieczeń.	Osiągnięcie akceptowalnych wartości w Szczegółowy Pomiar Skuteczności Zabezpieczeń		31.12.2024	Lokalny Administrator Bezpieczeństwa Informacji
Zapewnienie wiedzy i świadomości w zakresie bezpieczeństwa informacji wśród pracowników organizacji	upowszechnianie w całej organizacji świadomości dotyczącej wymagań Klienta, bezpieczeństwa danych osobowych i bezpieczeństwa informacji	Przeprowadzenie okresowego szkolenia z zakresu SZBI.	90% przeszkolonych pracowników		31.12.2024	Lokalny Administrator Bezpieczeństwa Informacji
Wzrost skuteczności SZBI	ciągłe doskonalenie skuteczności Systemu Zarządzania Bezpieczeństwem Informacji.	Otrzymanie certyfikatu ISO 27001	Tak/Nie		30.10.2024	Dyrekcja Centrum
Zachowanie poufności danych klientów	zapewnienie bezpieczeństwa danych powierzonych nam przez klientów	Analiza wykrytych incydentów	100% incydentów z wyjaśnionymi przyczynami i wdrożonymi działaniami korygującymi		12.2024	Lokalny Administrator Systemów Informatycznych

Załącznik nr 14. Pomiar skuteczności zabezpieczeń

Data Pomiaru	**DD.MM.RRRR**	**Okres** [w miesiącach]	**OD-DO**						
Pkt normy	**Zabezpieczenie**	**Dział realizujący**	**Sposób pomiaru skuteczności grup zabezpieczeń**	**Wskaźnik skuteczności**	**Częstość pomiaru**	**Forma zapisu/ Miejsce przechowywania**	**Weryfikacja**	**Wskaźnik**	**Wartość po której należy podjąć działania korygujące**
5 Kontrole organizacyjne									
5.1	Polityki bezpieczeństwa informacji	DCB	Okresowy przegląd Polityki bezpieczeństwa w ramach przeglądów zarządzania.	Adekwatność i aktualność polityki bezpieczeń-stwa – ilość zrealizowanych /zaplanowa-nych przeglądów	raz w roku	Rejestr incydentów	Dokonano weryfikacji zapisów Polityki bezpieczeń-stwa. Stwierdzono że zapisy Polityki są nieaktualne i wymagają zmian.	**n/d**	**n/d**
5.9	Spis informacji i innych powiązanych aktywów	Właściwy w stosunku do obszaru LASI	Okresowa (raz w roku) inwentaryzacja	% różnic stanu faktycznego do aktualnej ewidencji	raz w roku	n/d	Aktywa są zinwentary-zowane.	**n/d**	**n/d**

5.15	Kontrola dostępu	Właściwy w stosunku do obszaru LASI	Przegląd zapisów dotyczących uprawnień pracowników	% zgodności istniejących kont/ dostępów/ uprawnień użytkowników z rzeczywistością	raz w roku	Rejestr	100,00%	**100%**	**95%**
5.15	Kontrola dostępu	Właściwy w stosunku do obszaru LASI	Analiza incydentów	% incydentów z ustalonymi przyczynami do nich wszystkich	raz w roku	Rejestr	brak zdarzeń	**n/d**	**90%**
5.22	Monitorowanie, przegląd i zarządzanie zmianami usług dostawców	Właściwy w stosunku do obszaru LASI	Weryfikacja realizacji SLA	% zrealizowanych działań zgodnie z SLA	raz w roku	_	brak zdarzeń w analizowa-nym okresie	**n/d**	**95,00%**
5.26	Reakcja na incydenty związane z bezpieczeństwe m informacji	DCB	Przegląd skuteczności podjętych działań korygujących i zapobiegawczych	% zrealizowanych działań do zaakceptowan ych,	raz w roku	Rejestr incydentów Pełnomocnik System ticketowy Administrator	Zgodnie z rejestrem incydentów prowadzo-nym przez Pełnomoc-nika	**n/d**	**90%**
5.31	Wymogi prawne, ustawowe, regulacyjne i umowne	DCB	Przegląd wymagań prawnych - aktualność wymagań	% nieaktualnych przepisów w zestawieniu wymagań prawnych – bez aktualizacji	raz w roku	_	100,00%	**0%**	**0,01%**

6 Kontrola ludzi

6.3	Świadomość bezpieczeństwa informacji, edukacja i szkolenia	DCB	Weryfikacja liczby przeszkolonych pracowników	%przeszkolonych pracowników do wszystkich pracowników	raz w roku	listy szkoleń	90%	**100%**	**80%**
6.6	Umowy o zachowaniu poufności lub nieujawnianiu informacji	Dyrekcja Centrum	Określenie wymagań co do umów	% umów z określonymi wymaganiami	raz w roku	Rejestr umów		**75%**	**70%**

7 Kontrole fizyczne

7.2	Wejście fizyczne	LABF	Przegląd zapisów dotyczących uprawnień pracowników	% zgodności istniejących kont/ dostępów/ uprawnień użytkowników z rzeczywistością	raz w roku	Rejestr	W analizowa-nym okresie nie stwierdzono incydentów	**0**	**jakikolwiek incydent**
7.5	Ochrona przed zagrożeniami fizycznymi i środowiskowymi	LABF	Przegląd zapisów dotyczących legalności urządzeń	%zalegalizowanych urządzań	raz w roku	Rejestr	W analizowa-nym okresie nie stwierdzono incydentów	**100%**	**90%**

8 Kontrole technologiczne

8.7	Ochrona przed złośliwym oprogramowaniem	DCB	Aktualność oprogramowania antywirusowego	% aktualnego oprogramowania (baza wirusów)	raz w roku	Rejestr	100,00%	**100%**	**95,00%**

8.8	Zarządzanie lukami technicznymi	DCB	Analiza łat i aktualizacji	Ilość łat i aktualizacji, które były niezbędne do funkcjonowania oprogramowania	raz w roku	Rejestr	100,00%	**100%**	**90%**
8.15	Logowanie	Właściwy w stosunku do obszaru LASI	Przegląd zapisów/ logów z systemów zabezpieczających: firewall, antywirus itp.	% nieautoryzowanych prób wejść/wyjść do udanych wejść;	raz w roku	Rejestr	brak zdarzeń	**0%**	**jakikolwiek incydent**

	wartość dopuszczalna		brak działań	
	wartość graniczna		działania zapobiegawcze	
	wartość niedopuszczalna		natychmiastowe działania korygujące	