



SŁOWNIK DEFINICJI I SKRÓTÓW

ZINTEGROWANY SYSTEM ZARZĄDZANIA

SPIS TREŚCI

1. Skróty.....	3
2. Definicje.....	6

1. Skróty

SKRÓT	PEŁNA NAZWA
AB	Administrator Bezpieczeństwa
AD	Active Directory
ADO	Administrator Danych Osobowych
BCP	(ang. <i>Business Continuity Plan</i>) Plan Ciągłości Działania
CeZ, Centrum	Centrum e-Zdrowia
COB	Wydział Centrum Operacji Bezpieczeństwa w Departamencie Bezpieczeństwa
DI	Dyrektor Główny
DII	Dyrektor Pionu Architektury i Usług e-Zdrowia,
DIII	Dyrektor Pionu Rozwoju SIM i Wdrożeń
DIV	Dyrektor Pionu Eksploatacji i Bezpieczeństwa Systemów Teleinformatycznych
DV	Dyrektor Generalny
DB	Departament Bezpieczeństwa
DFK	Departament Finansowo-Kadrowy
DRP	(ang. <i>Disaster Recovery Plan</i>) plan odtwarzania po awarii
EWP	Ewidencja wjazdów do Polski
EZD	System do elektronicznego zarządzania dokumentacją obowiązujący w CeZ
HR	Wydział Kadr
ICT	(ang. <i>Information and Communication Technologies</i>) technologie informacyjno-komunikacyjne
IOC	(ang. <i>Indicators of Compromise</i>) Wskaźnik Kompromitacji
IOD	Inspektor Ochrony Danych
IP	Informacja Publiczna
IT	Infrastruktura Teleinformatyczna
IW	Informacja Wewnętrzna

Słownik definicji i skrótów

Wersja dokumentu:	1.1	Klauzula:	Do użytku publicznego	Strona 3 z 16
-------------------	-----	-----------	-----------------------	---------------

JIRA	Narzędzie do śledzenia zgłoszeń i zarządzania projektami dla zespołów
JIRA SD	JIRA Service Desk – Narzędzie do śledzenia i zarządzania zadaniami wsparcia technicznego obowiązujący w CeZ
LPD	Lokalny Punkt Dostępu
NDA	(ang. <i>Non-Disclosure Agreement</i>) Umowa o zachowaniu poufności
OMS	Opiekun Merytoryczny Systemu
OO3	Opiekun Osoby Trzeciej
OS3	Opiekun Strony Trzeciej
OTS	Opiekun Techniczny Systemu
OUK	Operator Usługi Kluczowej ¹
P1	Platforma P1
P3M	Standard zarządzania projektami w CeZ ²
PBI	Polityka Bezpieczeństwa Informacji
POIN	Pełnomocnik ds. ochrony informacji niejawnych
RODO	Ogólne rozporządzenie o ochronie danych ³ . Rozporządzenie unijne zawierające przepisy o ochronie osób fizycznych w związku z przetwarzaniem oraz o swobodnym przepływie danych osobowych
RPO	(ang. <i>Recovery Point Objective</i>) Docelowy Punkt Odtworzenia
RTO	(ang. <i>Recovery Time Objective</i>) Docelowy Czas Odtworzenia
SIM	System Informacji Medycznych
SKD	System Kontroli Dostępu
SLA	(ang. <i>Service Level Agreement</i>) Poziom Warunków Świadczonych Usług
SMZ	System Monitorowania Zagrożeń

¹ Zgodnie z Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (UoKSC) art. 5

² Standard zarządzania projektami CeZ (P3M) <https://confluence.csioz.gov.pl/display/p3m> (wyszukano 13.09.2023)

³ RODO – 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

SoA	(ang. <i>SoA – Statement of Applicability</i>) Deklaracja Stosowania w ramach Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z normą ISO 27001
SZBI	System Zarządzania Bezpieczeństwem Informacji
SZCD	System Zarządzania Ciągłością Działania
TC	Tajemnica Centrum
WI	Wydział Infrastruktury
WO	Wydział Organizacyjny
WWI	Wydział Wsparcia Informatycznego
ZSZ	Zintegrowany System Zarządzania

2. Definicje

TERMIN	OPIS
ACTIVE DIRECTORY (AD)	Usługa katalogowa (hierarchiczna baza danych) dla systemów Windows – będąca implementacją protokołu LDAP.
ADMINISTRATOR BEZPIECZEŃSTWA	Pracownik lub współpracownik CeZ odpowiedzialny za konfigurację narzędzi z obszaru bezpieczeństwa.
ADMINISTRATOR DANYCH OSOBOWYCH (ADO)	Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych ⁴ .
ADMINISTRATOR IT	Pracownik/współpracownik/wykonawca zewnętrzny odpowiedzialny za utrzymanie systemu użytkowego (aplikacji, baz danych, rejestru, usługi, systemów operacyjnych, uprawnień, itp) zgodnie z wymaganiami funkcjonalnymi Właściciela Biznesowego oraz określonymi wymogami нефункциональными (np. wymaganiami bezpieczeństwa i przepisów prawa). Zgodnie z procedurami może pełnić jedną lub wiele ról m.in: Administratora Oprogramowania, Administratora Aplikacji, Administratora Merytorycznego Aplikacji, Administratora Technicznego, Administratora Tożsamości, Opiekuna Merytorycznego Systemu, Opiekuna Technicznego Systemu.
AKTYWA	Wszystko co ma wartość dla CeZ, w szczególności informacje oraz mienie.
ARCHIWIZACJA	Trwałe zabezpieczenie dokumentów, plików w formie elektronicznej lub fizycznej w celu ich długotrwałego przechowywania np. archiwizowanie dokumentów papierowych, logów, obrazów maszyn (VM), kodu źródłowego itp.
AUDYT POZAPLANOWY	Audyt przeprowadzany w związku z żądaniem interesariuszy zewnętrznych, niekorzystnymi zmianami procesu, istotnymi niezgodnościami procesu, istotnymi zmianami organizacyjnymi.
AUDYT WEWNĘTRZNY	Systematyczny, niezależny i udokumentowany proces mający na celu określenie stopnia zgodności przyjętych kryteriów oceny funkcjonowania SZBI ze stanem faktycznym.
AUDYTOR WEWNĘTRZNY	Pracownik posiadający odpowiednie kompetencje do przeprowadzania audytów wewnętrznych, powołany przez Dyrektora CeZ`.
AUTENTYCZNOŚĆ	Atrybut bezpieczeństwa informacji dotyczący właściwości określającej, że jest ona wiarygodna.

⁴ Op. Cit. RODO art. 4 ust. 7

COMMUNITY SUPPORT	Spółecznościowa grupa wsparcia - oznaczają takie wsparcie, które jest realizowane przez członków danej społeczności, np. skupionej wokół danej dystrybucji linuxa.
CYBERBEZPIECZEŃSTWO	odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy ⁵ .
CZAS TRWANIA INCYDENTU	Czas jaki upłynął od chwili powzięcia informacji o incydencie bezpieczeństwa do chwili decyzji o zakończeniu jego obsługi.
DEVELOPER	Patrz – Programista.
DOCELOWY CZAS ODTWORZENIA (RTO)	(ang. <i>Recovery Time Objective</i>) określa czas potrzebny do przywrócenia systemu po wystąpieniu incydentu.
DOCELOWY PUNKT ODTWORZENIA (RPO)	(ang. <i>Recovery Point Objective</i>) określa okres następujący po incydencie, wskazujący na maksymalną ilość danych, które mogą zostać utracone, gdy usługa jest przywracana po przerwie w działaniu.
DOKUMENT	Informacja i przekazujący ją nośnik (wersja papierowa lub elektroniczna).
DOKUMENT WEWNĘTRZNY	Dokument, który został opracowany w CeZ, w szczególności: zarządzenia, procedury, instrukcje i regulaminy.
DOKUMENT ZEWNĘTRZNY	Dokument, który powstał poza CeZ, w szczególności: ustawy, rozporządzenia, normy.
DOKUMENTACJA SZBI	Wszelka dokumentacja systemowa (polityki, procedury, instrukcje) niezbędna do prawidłowego funkcjonowania SZBI.
DOSTĘPNOŚĆ	Atrybut bezpieczeństwa informacji zapewniający że informacja jest dostępna uprawnionym, wtedy kiedy jest potrzebna.
DOSTĘPNOŚĆ DANYCH	Właściwość danych określająca, konieczność zapewnienia dostępu do nich kiedy są one potrzebne.
DZIAŁANIE KORYGUJĄCE	Działanie w celu wyeliminowania przyczyny wykrytej niezgodności lub innej niepożądanego sytuacji.
ELEKTRONICZNE ZARZĄDZANIE DOKUMENTACJĄ (EZD)	(EZD, EZD PUW) system do elektronicznego zarządzania dokumentacją obowiązujący w CeZ. (https://ezd.cez.gov.pl/)
EWIDENCJA WJAZDÓW DO POLSKI (EWP)	System nadzoru nad chorobami zakaźnymi, w tym w czasie epidemii.
HARMONOGRAM AUDYTÓW	Zestaw jednego lub więcej audytów zaplanowanych w schemacie czasowym i prowadzonych w określonym celu.

⁵ Op. Cit. UoKSC art. 2 pkt 4

HASŁO	Ciąg znaków literowych, cyfrowych lub innych znaków specjalnych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
HASŁO TYMCZASOWE	Hasło przekazywane przez Service Desk, bądź Administratora IT danego Systemu na potrzeby pierwszego logowania, bądź ustanowienia nowego hasła na żądanie Użytkownika.
INCYDENT BEZPIECZEŃSTWA INFORMACJI (INCYDENT BEZPIECZEŃSTWA)	Pojedyncze zdarzenie lub seria niepożądanych, lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji ⁶ .
INCYDENT	Zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo ⁷ .
INCYDENT ISTOTNY	Incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz. Urz. UE L 26 z 31.01.2018, str. 48), zwanego dalej "rozporządzeniem wykonawczym 2018/151" ⁸ .
INCYDENT KRYTYCZNY	Incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV ⁹ .
INCYDENT POWAŻNY	Incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej ¹⁰ .
INFORMACJA WEWNĘTRZNA	Informacje, których naruszenie w wyniku przypadkowego lub złośliwego działania może mieć średni wpływ na działalność i cele CeZ.
INFORMACJA PUBLICZNA	Informacje, których naruszenie w wyniku przypadkowego lub złośliwego działania może mieć znikomy lub zerowy wpływ na działalność i cele CeZ.

⁶ Zgodnie z normą ISO 27001:2017

⁷ Op. Cit. UoKSC art. 2 pkt 5

⁸ Op. Cit. UoKSC art. 2 pkt 8

⁹ Op. Cit. UoKSC art. 2 pkt 6

¹⁰ Op. Cit. UoKSC art. 2 pkt 7

INFORMACJE POUFNE	Wszelkie informacje, materiały, dokumenty, dostarczone lub udostępnione pracownikowi przez pracodawcę lub inne podmioty oraz wytworzone przez pracownika w ramach realizacji umowy, a także o których wiedzę pracownik Są to informacje, które obowiązują zarówno przed, jak i po zawarciu umowy, w jakiegokolwiek formie. Obejmują informacje dotyczące pracodawcy lub innych podmiotów, w szczególności dotyczą danych osobowych. Informacjami poufnymi nie są dokumenty lub informacje podane do publicznej wiadomości w sposób inny niż na skutek naruszenia postanowień umowy lub innych zobowiązań do zachowania poufności, które wynikają z umów lub przepisów prawa.
INFRASTRUKTURA TELEINFORMATYCZNA (IT)	Zespół urządzeń i łączy transmisyjnych obejmujący w szczególności platformy sprzętowe (w tym: serwery fizyczne i wirtualne, macierze, stacje robocze oraz firmware), sieć teleinformatyczną (w tym: routery, przełączniki, zapory sieciowe oraz inne urządzenia sieciowe), oprogramowanie systemowe (w tym systemy operacyjne i systemy zarządzania bazami danych) oraz inne elementy umożliwiające bezawaryjną i bezpieczną pracę ww. zasobów (w tym zasilacze UPS, generatory prądotwórcze, urządzenia klimatyzacyjne), także te wykorzystywane w ośrodkach zapasowych.
INSPEKTOR OCHRONY DANYCH (IOD)	Osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna w szczególności za zapewnienie przestrzegania przepisów o ochronie danych osobowych, w rozumieniu art. 37 – 39 RODO.
INTEGRALNOŚĆ	Atrybut bezpieczeństwa informacji dotyczący właściwości określającej, że żadna jej część nie została zniszczona lub zmodyfikowana przez nieuprawnione osoby.
JIRA SERVICE DESK (JIRA SD)	JIRA Software – system do śledzenia i zarządzania zadaniami wsparcia technicznego obowiązujący w CeZ. (https://jirasd.csioz.gov.pl/servicedesk/customer/portals).
JIRA (JIRA SOFTWARE (JIRA))	JIRA Software – system śledzenia i zarządzania zadaniami obowiązujący w CeZ. (https://jira.csioz.gov.pl/).
KANCELISTA	Osoba upoważniona do dostępu do punktu ewidencyjnego oraz odpowiedzialna za przyjmowanie dokumentacji wpływającej do punktu ewidencyjnego.
KARTA DOSTĘPU	Karta zbliżeniowa uprawniająca do wejścia do wyznaczonych stref na terenie CeZ, oraz pobierania kluczy z depozytora.
KIEROWNIK PROJEKTU (KP)	Osoba posiadająca uprawnienia do bieżącego prowadzenia projektu, w ramach uprawnień określonych przez Komitet Sterujący (KS) i regulamin organizacyjny ¹¹ .

¹¹ Op. Cit. P3M <https://confluence.csioz.gov.pl/display/P3M/Opis+roli+Kierownik+Projektu> (wyszukano 13.09.2023 r.)

Słownik definicji i skrótów				
Wersja dokumentu:	1.1	Klauzula:	Do użytku publicznego	Strona 9 z 16

KONTO ADMINISTRATORA	Konto Administratora IT (systemu operacyjnego, bazy danych, aplikacji) posiadającego uprawnienia do administrowania danym zasobem w określonym obszarze odpowiedzialności.
KONTO TECHNICZNE	Konto funkcjonujące w środowisku teleinformatycznym jedynie w celu zapewnienia ich prawidłowego funkcjonowania i w związku z tym nie przypisane żadnej osobie, lecz jedynie konkretnemu zasobowi.
KONTO UPRIWILEJOWANE	Konto Techniczne lub Konto Administratorskie / Administratora.
KONTO UŻYTKOWNIKA	Zbiór zasobów i uprawnień w ramach środowiska teleinformatycznego przypisanych identyfikatorowi użytkownika i wykorzystywany przez użytkownika do realizacji zadań biznesowych.
KOORDYNATOR OUK	Koordinator Operatora Usług Kluczowych, pracownik Departamentu Bezpieczeństwa odpowiedzialny za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
KOORDYNATOR SYSTEMU ZGŁOSZEŃ	Pracownik Departamentu Bezpieczeństwa odpowiedzialny w ramach realizowanych zadań za obsługę systemu zgłoszeniowego.
KSIĘGA SYSTEMU	Dokument, w którym określono Zintegrowany System Zarządzania.
LOKALNY PUNKT DOSTĘPU	Lokalne, wydzielone pomieszczenie z infrastrukturą teleinformatyczną zapewniające dostęp do usług.
MIENIE	Materiały, urządzenia, które nie stanowią wyposażenia mobilnego (z wyłączeniem telefonów komórkowych, laptopów itp.).
NARUSZENIE OCHRONY DANYCH OSOBOWYCH	Naruszenie bezpieczeństwa (incydent bezpieczeństwa) prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych ¹²
NIEZGODNOŚĆ	Niespełnienie wymagania.
OBSŁUGA INCYDENTU	Wszystkie czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczanie skutków incydentu.
OBSŁUGUJĄCY INCYDENT	(ang. <i>incident handler</i>) pracownik Departamentu Bezpieczeństwa (w szczególności Pełnomocnik ds. ZSZ, Koordynator OUK) bądź Inspektor Ochrony Danych, odpowiedzialny za obsługę zgłoszeń z danej kategorii bezpieczeństwa informacji.

¹² Op. Cit. RODO art. 4 pkt 12

OPIEKUN MERYTORYCZNY SYSTEMU (OMS)	Pracownik/współpracownik/wykonawca zewnętrzny, wyznaczony w uzgodnieniu z Właścicielem Biznesowym Systemu do nadzoru merytorycznego nad rozwojem i utrzymaniem systemu (aplikacji, rejestru, usługi, systemów operacyjnych, itd) oraz do konsultowania z Właścicielem Biznesowym Systemu spraw wykraczających poza standardowe uzgodnienia (SLA, funkcjonalność, budżet, bezpieczeństwo itd.). Rolę tę może również wypełniać Administrator Aplikacji lub Administrator IT w zależności od specyfiki systemu.
OPIEKUN OSOBY TRZECIEJ (OO3)	Wskazany przedstawiciel CeZ odpowiedzialny za nadzór nad osobą trzecią (np. opiekun merytoryczny spraw związanych z daną osobą, opiekun umowy).
OPIEKUN STRONY TRZECIEJ (OS3)	Wskazany przedstawiciel CeZ odpowiedzialny za nadzór nad stroną trzecią w tym umowy z nią zawarte.
OPIEKUN TECHNICZNY SYSTEMU (OTS)	Osoba odpowiedzialna za koordynowanie zarządzania technicznego systemem, w tym za uzgodnienie (z Właścicielem Biznesowym Systemu i Opiekunem Merytorycznym Systemu) oraz przygotowanie wymagań i procedur eksploatacyjnych (SLA, RPO, RTO) i operacyjnych. Rolę tę może również wypełniać Administrator Aplikacji lub Administrator IT w zależności od specyfiki Systemu.
OSOBA TRZECIA	<p>Osoba fizyczna, osoba prawna lub jednostka organizacyjna nie posiadająca osobowości prawnej współpracujące współpracująca z CeZ na podstawie odrębnej umowy, bądź na mocy ustawy lub rozporządzenia regulujących zasady tej współpracy (np. Główny Inspektorat Farmaceutyczny). Osobą Trzecią są:</p> <ul style="list-style-type: none"> ▪ podmioty uprawnione, w szczególności podmioty nadzorowane przez Ministerstwo Zdrowia współpracujące przy wykonywaniu zadań i obowiązków na mocy przepisów prawa powszechnego, w szczególności pracownicy tych podmiotów, ▪ podmioty współpracujące z CeZ na podstawie umów partnerskich, w szczególności pracownicy tych podmiotów, ▪ podmioty współpracujące z CeZ w celu wsparcia realizowanych przez CeZ zadań, w szczególności pracownicy tych podmiotów zwani także dalej współpracownikami, ▪ dostawcy współpracujący przy wdrażaniu, eksploatacji i utrzymaniu środowiska teleinformatycznego, w szczególności pracownicy tych podmiotów, ▪ podmioty świadczące na rzecz CeZ inne usługi np. audyt, doradztwo itp., w szczególności pracownicy tych podmiotów.
PEŁNOMOCNIK DS. OCHRONY INFORMACJI NIEJAWNYCH (POIN)	Osoba, która odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych w CeZ, upoważniona do dostępu do punktu ewidencyjnego oraz nadzorująca procedury postępowania z dokumentacją wpływającą do punktu ewidencyjnego.
PEŁNOMOCNIK DS. ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA	Osoba, która odpowiada za prowadzenie całokształtu spraw związanych z opracowaniem, wdrożeniem i doskonaleniem Zintegrowanego Systemu Zarządzania.

PLAN CIĄGŁOŚCI DZIAŁANIA (BCP)	(ang. <i>Business Continuity Plan</i>) Udokumentowana informacja, która ukierunkowuje organizację na reagowanie na zakłócenia oraz wznowienie, odzyskanie i przywrócenie dostaw wyrobów i usług zgodnie z jej celami w zakresie ciągłości działania.
PLAN ODTWARZANIA PO AWARII	(ang. <i>Disaster Recovery Plan</i>) Lista czynności koniecznych do wykonania po incydencie, zmierzająca do wznowienia, odzyskania i przywrócenia dostaw wyrobów i usług zgodnie z jej celami w zakresie ciągłości działania (stanowi element Planu Ciągłości Działania).
PLATFORMA P1	Elektroniczna Platforma Gromadzenia, Analizy i Udostępniania zasobów cyfrowych o Zdarzeniach Medycznych ¹³ . (https://ezdrowie.gov.pl/)
PODATNOŚĆ	Słabość aktywu lub zabezpieczenia, która może być wykorzystana przez co najmniej jedno zagrożenie.
POLITYKA BEZPIECZEŃSTWA INFORMACJI (PBI)	Wyrażona przez dyrekcję ogólna intencja i kierunki działań dotyczące bezpieczeństwa informacji.
POUFNOŚĆ	Atrybut bezpieczeństwa informacji, który dotyczy właściwości określającej, że nie jest ona udostępniana osobom do tego nieupoważnionym.
POZIOM WARUNKÓW ŚWIADCZONYCH USŁUG (SLA)	(ang. <i>Service Level Agreement</i>), Zapisy w umowach dotyczące poziomu oraz warunków świadczonych usług z zakresu IT. Zawarte w umowie zapisy stanowią dla klienta gwarancję jakości wykonanych przez zleceniobiorcę działań.
PRACOWNIK	Osoba fizyczna zatrudniona w CeZ na podstawie umowy o pracę.
PROCEDURA	Opisuje proces lub grupę procesów oraz sposób ich nadzorowania w CeZ (to jest procesu lub grupy procesów), ustala cel, zakres stosowania, konieczne definicje (pojęcia lub terminy), odpowiedzialność, tryb postępowania (kolejność czynności w realizowanym procesie) oraz wskazuje powiązania z innymi dokumentami np. zarządzeniami, instrukcjami stosowanymi w danym procesie oraz określa niezbędne formularze.
PROCEDURA OPERACYJNA	Udokumentowana procedura opisująca działania i czynności w ramach realizowanych zadań przez komórkę organizacyjną, z wyłączeniem procedury systemowej.
PROCEDURA SYSTEMOWA	Udokumentowana procedura literalnie wymagana normą ISO 22301 i/lub ISO 27001.

¹³ Op. Cit. P3M <https://confluence.csioz.gov.pl/display/P3MAB/P1+-+Elektroniczna+Platforma+Gromadzenia> (wyszukano 13.09.2023)

PROGRAMISTA (DEVELOPER)	Osoba odpowiedzialna za wytwarzanie systemów informatycznych, ich rozwój oraz dbanie, aby wytwarzane funkcjonalności były zgodne z założeniami ¹⁴ .
PRZEŁOŻONY	Osoba odpowiedzialna za nadzór nad podległymi pracownikami.
PUNKT EWIDENCYJNY	Wyodrębnione miejsce dotyczące ochrony informacji niejawnych, podległa pełnomocnikowi ds. ochrony informacji niejawnych. Punkt ewidencyjny obsługiwany jest przez wyznaczonych pracowników, odpowiedzialnych za właściwe rejestrowanie, przechowywanie, obieg i wydawanie materiałów uprawnionym osobom.
RECERTYFIKACJA	Proces przeglądu kont użytkowników i ich uprawnień w wybranych systemach oraz usuwania na tej podstawie nieprawidłowości.
RĘKOJMIA ZACHOWANIA TAJEMNICY	Zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego ¹⁵ .
ROZLICZALNOŚĆ	Możliwość weryfikacji kto i kiedy miał dostęp do danych informacji.
RYZYO	Kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji.
SERVICE DESK	Usługa zapewniana użytkownikom przez Wydział Infrastruktury, której celem jest rozwiązywanie problemów dotyczących infrastruktury IT zarządzanej przez CeZ. (https://jirasd.csioz.gov.pl/servicedesk/customer/portals).
STACJA PRZESIADKOWA	Serwer przesiadkowy (tzw. jump host) to system zdalnego połączenia, który pozwala użytkownikowi zyskać dostęp do szczególnie chronionych usług.
STANDARD ZARZĄDZANIA PROJEKTAMI (P3M)	Standard P3M ¹⁶ umożliwiający: <ul style="list-style-type: none"> ▪ ustanowienie i doskonalenie spójnego podejścia do zarządzania projektami, programami, portfolio oraz analizy biznesowej, ▪ ustanowienie ram zarządczych dla każdego projektu, programu, portfolio, ▪ ustanowienie i doskonalenie wspólnego środowiska informatycznego do zarządzania projektami programami i portfolio, ▪ współdzielenie doświadczeń i najlepszych praktyk.

¹⁴ OP. Cit. P3M <https://confluence.csioz.gov.pl/display/P3M/Opis+roli+Programista> (wyszukano 13.09.2023)

¹⁵ Ustawa z dn. 5 sierpnia 2010 r. o ochronie informacji niejawnych art. 2 pkt 2

¹⁶ Op. Cit. P3M <https://confluence.csioz.gov.pl/display/p3m> (wyszukano 13.09.2023)

Słownik definicji i skrótów				
Wersja dokumentu:	1.1	Klauzula:	Do użytku publicznego	Strona 13 z 16

STREFA DOSTĘPU	Strefa na terenie siedziby CeZ, w której pracownicy i współpracownicy lub osoby z zewnątrz (goście) poruszają się za pomocą posiadanych kart zbliżeniowych. Wydzielono cztery strefy dostępu: ogólnodostępna, z ograniczonym dostępem, szczególnie chroniona, zastrzeżona.
STREFA OGÓLNODOSTĘPNA	Strefa na terenie siedziby CeZ, do której mają dostęp wszyscy pracownicy i współpracownicy oraz osoby z zewnątrz.
STREFA SZCZEGÓLNIE CHRONIONA	Strefa na terenie siedziby CeZ, która podlega szczególnej ochronie. Dostęp do strefy posiadają osoby upoważnione.
STREFA Z OGRANICZONYM DOSTĘPEM	Strefa na terenie siedziby CeZ, do której dostęp posiadają osoby do tego upoważnione.
STREFA ZASTRZEŻONA	Strefa na terenie siedziby CeZ, która podlega szczególnej ochronie i ewidencji wejść/wyjść. Dostęp do strefy posiadają osoby upoważnione, a nieupoważnione przebywają w strefie osób upoważnionych oraz w ich towarzystwie. Wejście do strefy jest odnotowywane w książce wejść/wyjść.
SYSTEM INFORMACJI MEDYCZNEJ	System teleinformatyczny, który służy przetwarzaniu danych dotyczących: udzielonych, udzielanych i planowanych świadczeń opieki zdrowotnej, udostępnianych przez systemy teleinformatyczne usługodawców. ¹⁷
SYSTEM INFORMATYCZNY	Aplikacja komputerowa (w tym aplikacja mobilna), usługa chmurowa lub zbiór powiązanych komponentów programowych, którego celem jest przetwarzanie danych.
SYSTEM KONTROLI DOSTĘPU (SKD)	System zabezpieczający przed wejściem przez osoby nieuprawnione na teren obiektu oraz do poszczególnych pomieszczeń poprzez zastosowanie rozwiązań typu bramki, czytniki, karty dostępu.
SYSTEM MONITOROWANIA ZAGROŻEŃ	System, który ma na celu: usprawnienie dostępu do informacji o zapobieganiu skutkom niepożądanych zdarzeń mających wpływ na zdrowie i życie ludzi, poprawę efektywności działań w zakresie zapobiegania skutkom niepożądanych zdarzeń oraz zapewnić monitorowanie sektora ochrony zdrowia w zakresie zagrożeń.
SZACOWANIE RYZYKA	Ostatni etap analizy ryzyka. Polega na obliczeniu ryzyka utraty bezpieczeństwa przez informacje, które są przetwarzane i przechowywane w systemie.

¹⁷ Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia art. 10 ust. 1

SZCZEGÓLNE KATEGORIE DANYCH OSOBOWYCH	Zgodnie z RODO do szczególnych kategorii danych osobowych zalicza się: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.
ŚRODOWISKO TELEINFORMATYCZNE	Infrastruktura teleinformatyczna wraz z wykorzystującymi ją systemami informatycznymi oraz eksploatowane w CeZ systemy informatyczne, które wspierają jego działalność. Oparte są na infrastrukturze teleinformatycznej, zapewnianej przez podmioty zewnętrzne.
TAJEMNICA CENTRUM (TAJEMNICA CeZ)	Informacje, których naruszenie w wyniku przypadkowego lub złośliwego działania miałooby duży wpływ na działalność i cele CeZ.
TOŻSAMOŚĆ	Zbiór unikalnych faktów, cech oraz danych personalnych (w szczególności imię i nazwisko, numer identyfikacyjny PESEL, NIP, data urodzenia) pozwalających na jednoznaczne zidentyfikowanie konkretnej osoby, uznawanych przez państwo dla celów regulacyjnych (prawnych) oraz innych „oficjalnych spraw”.
TOŻSAMOŚĆ CYFROWA	Zestaw danych, które w sposób unikalny opisują osobę i jej tożsamość, oraz zawierają informację na temat jej powiązań w systemach informatycznych.
UMOWA O ZACHOWANIU POUFNOŚCI (NDA)	(ang. <i>Non-Disclosure Agreement</i>) Umowa, na mocy której strony zobowiązują się do zachowania w tajemnicy ściśle określonych informacji (na przykład tajemnicy przedsiębiorstwa).
USŁUGA KLUCZOWA	Usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymieniona w wykazie usług kluczowych.
UŻYTKOWNIK	Osoba, która posiada określony zakres uprawnień i dostępów do środowiska teleinformatycznego.
WŁAŚCICIEL BIZNESOWY PROJEKTU	Osoba, która ponosi ostateczną odpowiedzialność za projekt, będąc wspieraną przez Głównych Użytkowników oraz dyrektora CeZ, dostawcę, przewodniczącego Komitetu Sterującego (za Standardem P3M ¹⁸).
WŁAŚCICIEL BIZNESOWY SYSTEMU	Osoba odpowiedzialna merytorycznie za określony zakres działań CeZ bądź podmiotu zewnętrznego, dla wsparcia którego świadczona jest usługa informatyczna.

¹⁸ Op. Cit. P3M <https://confluence.csioz.gov.pl/pages/viewpage.action?pageId=328579> (wyszukano 13.09.2023)

WŁAŚCICIEL INFORMACJI	Kierownik komórki organizacyjnej bądź samodzielne stanowisko, odpowiedzialny za merytoryczną treść określonych informacji oraz za udział w podejmowaniu decyzji dotyczących w zakresie należących do niego informacji. Kierownik komórki decyduje o poziomach zabezpieczeń tych informacji oraz o miejscach i sposobach ich przetwarzania.
WSKAŹNIK KOMPROMITACJI (IOC)	(ang. <i>Indicators of Compromise</i>) Oznaka wskazująca na możliwość naruszenia bezpieczeństwa.
WSPÓŁPRACOWNIK	Osoba reprezentująca podmiot zewnętrzny, współpracująca z CeZ na podstawie odrębnej umowy cywilno-prawnej (np. umowy o świadczenie usług).
WYKONAWCA (ZEWNĘTRZNY)	Podmiot gospodarczy powiązany umową formalnie-prawną z CeZ, realizujący dostawy lub świadczący usługi na rzecz CeZ.
WYMAGANIA	Określone potrzeby lub oczekiwania, które zostały ustalone, przyjęte zwyczajowo lub są obowiązkowe.
ZABEZPIECZENIE	Środek, który obniża ryzyko.
ZAGROŻENIE	Potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w systemie lub organizacji.
ZASADA NIEPRZECHODNIOŚCI PRAW	Zgodnie z zasadą nabyte przez użytkownika prawa dostępu są nieprzechodnie, czyli nie ma prawa on ich ujawniać, udostępniać innym użytkownikom.
ZASADA WIEDZY NIEZBĘDNEJ	Zgodnie z tą zasadą informacje mogą być przetwarzane wyłącznie przez osoby sprawdzone (dające rękojmię zachowania tajemnicy) i przeszkolone z zakresu bezpieczeństwa informacji.
ZDARZENIE BEZPIECZEŃSTWA	Zdarzenie związane z bezpieczeństwem informacji jest określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.
ZINTEGROWANY SYSTEM ZARZĄDZANIA (ZSZ)	System, w skład którego wchodzi System Zarządzania Bezpieczeństwem Informacji (SZBI) zgodny z wymaganiami normy PN-ISO/IEC 27001 oraz System Zarządzania Ciągłością Działania (SZCD).