

PROCEDURA OGÓLNA ZARZĄDZANIA INCYDENTAMI CYBERBEZPIECZEŃSTWA W GK PGE

PROG 00116/B

Sygn.: PGE/CENT/DSIT/3.2

Data zatwierdzenia: 2022/04/04

Obowiązuje od: 2022/04/14

I CEL I ZAKRES

- 1.1 Celem Procedury jest zapewnienie efektywnego zarządzania Incydentami związanymi z Cyberbezpieczeństwem w GK PGE, w tym przede wszystkim:
 - a. skutecznego i szybkiego wykrywania oraz reagowania na wystąpienia Incydentów Cyberbezpieczeństwa, a przez to możliwie największego ograniczenia ich negatywnych skutków,
 - b. gromadzenia materiałów analitycznych dających największą szansę na ustalenie przyczyny Incydentu Cyberbezpieczeństwa oraz jego sprawców,
 - c. poprawnego gromadzenia Materiałów Dowodowych mogących służyć jako dowód w szczególności w ewentualnych postępowaniach karnych, cywilnych (w tym postępowaniach przygotowawczych oraz przed sądami) oraz postępowaniach dyscyplinarnych,
 - d. rejestrowania, klasyfikowania, priorytetyzacji, analizowania, podejmowania działań naprawczych i ograniczających skutki Incydentu,
 - e. podniesienia skuteczności zabezpieczeń poprzez analizę historii Incydentów Cyberbezpieczeństwa, wyszukiwania powiązań między Incydentami, usuwania przyczyn ich wystąpienia,
 - f. definiowanie i wdrażanie działań korygujących mających na celu zapobieżenie wystąpienia analogicznego Incydentu Cyberbezpieczeństwa w przyszłości.
- 1.2 Procedura obejmuje swoim zakresem Zdarzenia związane z Incydentami Cyberbezpieczeństwa mającymi miejsce w:
 - a. Systemach Teleinformatycznych z obszaru ICT,
 - b. obszarze Systemów OT.
- 1.3 Procedura nie obejmuje swoim zakresem monitorowania dostępności, ciągłości usług i obsługi Sytuacji Krytycznych, za wyjątkiem sytuacji, gdzie ma miejsce podejrzenie Incydentu Cyberbezpieczeństwa.

II ODPOWIEDZIALNOŚĆ

- 2.1 Za stosowanie niniejszej Procedury odpowiedzialni są:
 - 2.1.1 Kierujący komórką właściwą ds. strategii ICT w PGE Polska Grupa Energetyczna S.A., który jednocześnie odpowiada za aktualizację Procedury.
 - 2.1.2 Pracownicy oraz Osoby Trzecie, realizujący określone działania na rzecz Spółek GK PGE – ich zakres odpowiedzialności został określony w [Załącz. 5](#).
 - 2.1.3 Kierujący komórką właściwą ds. compliance w PGE Polska Grupa Energetyczna S.A. w zakresie przekazywania Zgłoszeń Incydentów niezgodności z obszaru cyberbezpieczeństwa zarejestrowanych zgodnie z *PROG 00095 Procedura Ogólna – Zgłaszanie i postępowanie ze Zgłoszeniami Incydentów niezgodności w GK*.
- 2.2 Wszelkie odstępstwa od Procedury muszą być zaakceptowane przez Kierującego komórką właściwą ds. strategii ICT w PGE S.A.

III DOKUMENTY POWIĄZANE

- 3.1 *REGL 00082 Polityka Organizacji Teleinformatyki w Grupie Kapitałowej PGE*
- 3.2 *PROG 00035 Procedura Ogólna – Wytyczne w zakresie ochrony danych osobowych w GK PGE*
- 3.3 *PROG 00037 Procedura Ogólna – Wytyczne w zakresie Klasyfikacji i ochrony informacji w Grupie Kapitałowej PGE*
- 3.4 *PROG 00038 Procedura Ogólna – Wytyczne w zakresie opracowywania planów zapewnienia ciągłości działania w GK PGE*
- 3.5 *PROG 00039 Procedura Ogólna bezpieczeństwa teleinformatycznego*
- 3.6 *PROG 00103 Procedura Ogólna – korzystania z zasobów teleinformatycznych ICT w GK PGE*
- 3.7 *PROG 00095 Procedura Ogólna – Zgłaszanie i postępowanie ze Zgłoszeniami Incydentów niezgodności w GK PGE oraz ochrona Sygnalistów*
- 3.8 *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*

IV ZAŁĄCZNIKI

- 4.1 [Załącz. 1](#) Kryteria klasyfikacji Incydentów Cyberbezpieczeństwa
- 4.2 [Załącz. 2](#) Karta komunikacji Incydentów Cyberbezpieczeństwa

- 4.3 [Załącznik 3](#) Wytyczne w zakresie zabezpieczania Materiału Dowodowego Incydentów Cyberbezpieczeństwa
- 4.4 [Załącznik 4](#) Karta Zabezpieczenia Materiału Dowodowego
- 4.5 [Załącznik 5](#) Macierz RACI i zadania poszczególnych ról
- 4.6 [Załącznik 6](#) Karta informacyjna ODO

V SKRÓTY I DEFINICJE

GK PGE; PGE, PGE S.A.;

Centrala; Grupa PGE / Grupa; Jednostka Biznesowa; Komórka organizacyjna / komórka; Pracodawca; Pracownik; Proces biznesowy / Proces; Przetwarzanie informacji; Spółka GK PGE, Spółka, Spółki; Tajemnica Spółki;

Skróty użyte na potrzeby niniejszego dokumentu:

CERT	- (ang. Computer Emergency Response Team) – zespół reagowania na awarie komputerowe (będące wynikiem Incydentów Cyberbezpieczeństwa)
CIO	- (ang. Chief Information Officer) – rola pełniona przez Kierującego komórką właściwą ds. strategii ICT w PGE S.A. Odpowiada za operacyjne zarządzanie Funkcją ICT w GK PGE
CSIRT GOV	- Zespół Reagowania na Incydenty Cyberbezpieczeństwa działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego (definicja na podstawie ustawy o KSC)
DLP	- (ang. Data Loss Prevention) – ogólna nazwa technologii informatycznych wspomagających ochronę danych w postaci elektronicznej przed kradzieżą lub przypadkowymi wyciekami. Rozwiązanie informatyczne, oprogramowanie służące do ochrony danych przed wyciekiem.
DSIT	- komórka właściwa ds. strategii IT PGE S.A.
IOD	- Inspektor Ochrony Danych, wyznaczony przez ADO
ICT	- (ang. Information and Communication Technologies) - teleinformatyka
ITSM	- system informatyczny wykorzystywany do zarządzania usługami IT
KSC	- Krajowy System Cyberbezpieczeństwa, określony w Ustawie o KSC
ODO	- Ochrona Danych Osobowych
OT	- (ang. Operational Technology)
PGE-CERT	- Komórka organizacyjna w strukturach PGE Systemy S.A., świadcząca usługi monitorowania Cyberbezpieczeństwa i Obsługi incydentów
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 (ogólne rozporządzenie o ochronie danych)
SIEM	- (ang. Security Information and Event Management) – system do zarządzania informacją i Zdarzeniami cyberbezpieczeństwa umożliwiający scentralizowane zarządzanie, gromadzenie i analizę informacji pochodzących z różnych źródeł, m.in. logów, wpisów w dziennikach systemowych czy wszelkich innych aplikacjach funkcjonujących w organizacji pozwalający zwiększyć Bezpieczeństwo Informacji oraz infrastruktury poprzez wczesne wykrywanie nadużyć i Incydentów Bezpieczeństwa w GK PGE
SLA	- (ang. Service Level Agreement) umowa o gwarantowanym poziomie świadczenia usług
SOM	- (ang. Security Operations Management) – zestaw narzędzi teleinformatycznych pozwalający na kompleksową Obsługę Incydentów Cyberbezpieczeństwa za pomocą jednej platformy integrującej się z innymi systemami, pełniący rolę centralnego punktu informacji i zbioru wszystkich Incydentów Cyberbezpieczeństwa w organizacji

Definicje pojęć użyte na potrzeby niniejszego dokumentu:

- 5.1 **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 (Rozporządzenie o Ochronie Danych Osobowych RODO Art. 4 pkt 7). W przypadku Spółek wchodzących w skład Grupy Kapitałowej PGE, Administratorem Danych Osobowych jest samodzielnie każda Spółka GK PGE.
- 5.2 **Administrator Systemu (Administrator)** – Pracownik GK PGE lub Osoba Trzecia posiadająca odpowiedni poziom uprawnień i odpowiedzialności za System Teleinformatyczny lub element infrastruktury teleinformatycznej. Osoba ta zarządza i sprawuje nadzór nad Systemem Teleinformatycznym lub innym elementem infrastruktury teleinformatycznej od strony technicznej.

- 5.3 **Bezpieczeństwo Informacji** – zapewnienie Poufności, Integralności i Dostępności informacji dla przetwarzanych informacji, czyli zabezpieczanie jej przed nieautoryzowanym dostępem, zmianą, utratą, uszkodzeniem, zniszczeniem lub zatajeniem.
- 5.4 **Centrala** – Spółka (jeżeli nie posiada ona oddziałów) lub komórka organizacyjna Spółki realizująca zadania operacyjne w miejscu siedziby Spółki (jeżeli Spółka posiada oddziały).
- 5.5 **Centrum Usług Wspólnych ICT (CUW ICT)** – podmiot, którego celem jest świadczenie Usług ICT na rzecz pozostałych Spółek GK PGE.
- 5.6 **Cyberbezpieczeństwo** – odporność systemów informacyjnych na działania naruszające Poufność, Integralność, Dostępność i Autentyczność przetwarzanych Danych lub związanych z nimi usług oferowanych przez te Systemy.
- 5.7 **Cyberprzestrzeń** – oznacza przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami.
- 5.8 **Dane** – danymi (ang. data) jest wszystko to, co jest lub może być przetwarzane umysłowo lub komputerowo. W szczególności Danymi są informacje przetwarzane w Systemach Teleinformatycznych lub przechowywane na Nośnikach Informacji wraz z informacjami konfiguracyjnymi Zasobów ICT.
- 5.9 **Dane Osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której Dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
- 5.10 **Dostępność** – właściwość bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu.
- 5.11 **Dowód Elektroniczny** – informacje przechowywane lub przesyłane w formie elektronicznej, które mogą mieć znaczenie jako Materiał Dowodowy. Przykładem Dowodów Elektronicznych mogą być zapisy elektroniczne przechowywane w pamięci operacyjnej oraz dysku twardym komputera (np. informacje zawarte w pamięci „ulotnej” RAM Dokumenty Elektroniczne, korespondencja elektroniczna, zapisy dzienników Zdarzeń z programów komputerowych, zapisy urządzeń kontroli dostępu, nagrania z kamer przemysłowych, zapisy z systemu SKD, adresy IP, wirusy świadczące o kradzieży cyfrowej tożsamości użytkownika) oraz metadane (daty plików lub inne właściwości) z tym zapisem związane.
- 5.12 **Dyrektor ICT Spółki** – osoba zarządzająca obszarem ICT w Spółce GK PGE.
- 5.13 **False Positive** – Zdarzenie fałszywie pozytywne, określające, że zidentyfikowane Zdarzenie nie jest w rzeczywistości potwierdzone lub jego znaczenie jest nieistotne.
- 5.14 **Główny Architekt Bezpieczeństwa ICT i OT** – pracownik Komórki Organizacyjnej właściwej ds. Strategii ICT GK PGE, odpowiedzialny za nadzór nad obszarem Cyberbezpieczeństwa ICT oraz OT w GK PGE.
- 5.15 **Grupa PGE / Grupa** – PGE oraz Spółki objęte zakresem zastosowania Kodeksu Grupy PGE na podstawie Art. 7 Kodeksu Grupy PGE.
- 5.16 **Grupa Kapitałowa PGE (GK lub GK PGE)** – PGE oraz Spółki względem których PGE posiada status spółki dominującej w rozumieniu artykułu 4 § 1 pkt 4 Kodeksu spółek handlowych.
- 5.17 **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. W tym również rozliczalności, naruszenia zasad i przepisów obowiązujących w GK PGE w zakresie Bezpieczeństwa Informacji.
- 5.18 **Incydent Cyberbezpieczeństwa (Incydent)** – zdarzenie, które ma lub może mieć niekorzystny wpływ na Cyberbezpieczeństwo w tym na Bezpieczeństwo Informacji.
- 5.19 **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 GOV**.
- 5.20 **Incydent poważny** – Incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia Usługi Kluczowej (definicja na podstawie ustawy o KSC).
- 5.21 **Inspektor Ochrony Danych (IOD)** – Inspektor Ochrony Danych lub specjalista ds. ochrony Danych lub inna osoba wyznaczona w Spółce, w celu wykonywania zadań określonych w art. 39 RODO.
- 5.22 **Integralność** – właściwość polegająca na zapewnieniu dokładności i kompletności informacji.
- 5.23 **Jednostka Biznesowa (JB)** – Spółka, wyodrębniona Jednostka organizacyjna lub obszar zarządczy w wielu Spółkach, realizujący określone zadania na rzecz Grupy PGE lub jej części .
- 5.24 **Karta Incydentu Cyberbezpieczeństwa** – ustrukturyzowane informacje o Incydencie.

- 5.25 **Karta informacyjna ODO** – Ustrukturyzowana informacja o Incydencie w zakresie ODO pozwalająca na zgłoszenie naruszenia.
- 5.26 **Karta komunikacji** – model przepływu komunikacji przy zaistnieniu Incydentu Cyberbezpieczeństwa bądź Zdarzenia mającego znamiona Incydentu Cyberbezpieczeństwa, wraz z macierzą kontaktów w poszczególnych Komórkach i Jednostkach Biznesowych.
- 5.27 **Komórka organizacyjna / komórka** – jedno lub wieloosobowe ciało powołane do wykonywania określonych części zadań w Jednostce organizacyjnej, mające ustalone miejsce w jej strukturze organizacyjnej. Komórka może być: departament, biuro, zespół, wydział, dział, sekcja lub inna komórka wewnętrzna w Spółce lub Oddziale Spółki.
- 5.28 **Komórka właściwa ds. cyberbezpieczeństwa OT w Centrali Spółki** – komórka wydzielona w strukturze organizacyjnej Centrali Spółki, odpowiedzialna za realizację zadań powierzonych jej w ramach niniejszej Procedury oraz pozostałych regulacji dotyczących obszaru cyberbezpieczeństwa ujętych w DSZ Spółki.
- 5.29 **Komórka właściwa ds. cyberbezpieczeństwa OT w Oddziale Spółki** – komórka wydzielona w strukturze organizacyjnej Oddziału Spółki, odpowiedzialna za realizację zadań powierzonych jej w ramach niniejszej Procedury oraz pozostałych regulacji dotyczących obszaru cyberbezpieczeństwa ujętych w DSZ Spółki i DSZ Oddziału.
- 5.30 **Kontraktor** – osoba, niebędącą Osobą Trzecią, realizująca zadania na rzecz Spółki na innej podstawie niż umowa o pracę.
- 5.31 **Materiał Dowodowy** – wszelkie informacje mogące wskazywać na miejsce, czas, źródło, sposób, sprawcę oraz skutek wystąpienia Incydentu Bezpieczeństwa, m.in. w postaci Dowodu Elektronicznego.
- 5.32 **Naruszenie ochrony Danych osobowych / naruszenie** – naruszenie bezpieczeństwa ochrony Danych 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.
- 5.33 **Nośnik informacji / Nośnik** – wszelkiego rodzaju Nośniki danych, używane w procesie Przetwarzania Informacji, w szczególności dyski twarde, płyty CD/DVD/BR, taśmy DLT/DDS, pamięci przenośne, dyski magneto-optyczne, papier.
- 5.34 **Obsługa incydentu** – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków Incydentu (definicja na podstawie ustawy o KSC).
- 5.35 **Operator Usługi Kluczowej** – podmiot, wobec którego organ właściwy do spraw Cyberbezpieczeństwa wydał decyzję administracyjną o uznaniu go za Operatora Usługi Kluczowej.
- 5.36 **Osoba Trzecia** – Osoba Trzecia osoba udostępniona przez dostawcę, która nie może posiadać Dostępów odpowiadających Pracownikowi a realizująca określone zadania na rzecz Spółki. Osoba Trzecia to również: praktykanci, stażyści, wolontariusze i inne osoby realizujące zadania na rzecz Spółki, niebędące Kontraktorem.
- 5.37 **Osoba odpowiedzialna za kontakty z podmiotami KSC** – osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami Krajowego Systemu Cyberbezpieczeństwa, wyznaczona przez Operatora Usługi Kluczowej.
- 5.38 **Podatność** – właściwość systemu informacyjnego, która może być wykorzystana przez Zagrożenie cyberbezpieczeństwa.
- 5.39 **Poufność** – właściwość, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.
- 5.40 **Pracodawca** – Spółka lub Oddział Spółki zatrudniający Pracowników w ramach stosunku pracy reprezentowany przez Zarząd lub inne osoby uprawnione do dokonywania w imieniu Pracodawcy czynności w sprawach z zakresu prawa pracy, na podstawie pełnomocnictw lub innych wewnętrznych aktów prawnych obowiązujących w Spółce.
- 5.41 **Pracownik** – osoba, z którą Pracodawca nawiązał stosunek pracy w rozumieniu art. 22 Kodeksu pracy, nie obejmuje osób wykonujących pracę na innej podstawie niż stosunek pracy.
- 5.42 **Procedura** – PROG 00116/B Procedura Ogólna Zarządzania Incidentami Cyberbezpieczeństwa w GK PGE S.A., niniejszy dokument.
- 5.43 **Proces biznesowy / Proces** – logicznie uporządkowany łańcuch działań wzajemnie powiązanych lub wzajemnie oddziałujących, zwykle przebiegający przez wiele Jednostek organizacyjnych / komórek / stanowisk w organizacji, których celem jest uzyskanie produktu spełniającego oczekiwania interesariuszy, w tym klienta wewnętrznego i/lub zewnętrznego. Proces realizuje cel biznesowy organizacji.
- 5.44 **Przetwarzanie informacji** – jakiejkolwiek operacje wykonywane na informacji, w szczególności takie jak ich zbieranie, utrwalanie, przechowywanie, opracowywanie, modyfikowanie, udostępnianie, przesyłanie i usuwanie.

- 5.45 **Raport Incydentów Cyberbezpieczeństwa** – statystyczne zestawienie informacji z zadanego okresu o Incydentach Cyberbezpieczeństwa sporządzony na podstawie Kart Incydentów Cyberbezpieczeństwa.
- 5.46 **Rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
- 5.47 **Spółka GK PGE, Spółka, Spółki** – Podmiot / podmioty prawa handlowego wchodzące w skład Grupy Kapitałowej PGE.
- 5.48 **Standardowy Incydent Cyberbezpieczeństwa** – Incydent Cyberbezpieczeństwa, dla którego istnieją sprawdzone i udokumentowane metody zbierania informacji i rozwiązania.
- 5.49 **System Teleinformatyczny / informacyjny (System)** – zespół środków technicznych wraz z oprogramowaniem tworzący logiczną i nierozzerwalną całość wyodrębnioną ze względu na dostarczaną funkcjonalność przy założeniu, że głównym jego celem jest Przetwarzanie Informacji.
- 5.50 **Systemy ICT** – systemy realizujące Funkcje ICT niebędące Systemami OT, wspierające realizację celów biznesowych określanych przez Spółki.
- 5.51 **Systemy OT (ang. Operational Technology)** – Systemy Teleinformatyczne, które realizują w Spółce funkcje zarządzania, sterowania, regulacji, pomiaru, monitoringu, bezpieczeństwa (lub kilku tych funkcji łącznie) dla procesów technologicznych i przemysłowych realizowanych w ramach infrastruktury przemysłowej GK PGE wraz z Systemami teletransmisji, niezbędnymi do ich działania.
- 5.52 **Sytuacja Krytyczna** – Zdarzenie uniemożliwiające lub poważnie utrudniające normalne działanie Spółki GK PGE przez czas dłuższy niż 4 godziny, a w przypadku operacyjnej działalności handlowej przez czas dłuższy niż 1 godzina, zarówno zakłócenie, jak i awaria.
- 5.53 **Tajemnica Spółki** – oznacza tajemnicę przedsiębiorstwa zgodnie z art. 11 ust 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, przez co rozumie się informacje techniczne, technologiczne, organizacyjne Spółki lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w Poufności.
- 5.54 **Usługa Kluczowa** – usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych.
- 5.55 **Ustawa o Krajowym Systemie Cyberbezpieczeństwa /ustawa o KSC** – ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
- 5.56 **Właściciel Incydentu Cyberbezpieczeństwa** – rola pełniona przez wyznaczonych Pracowników. Odpowiada za klasyfikację, wyjaśnienie i rozwiązanie Incydentu Cyberbezpieczeństwa.
- 5.57 **Zagrożenie cyberbezpieczeństwa** – potencjalna przyczyna wystąpienia Incydentu.
- 5.58 **Zarządzanie incydemem** – Obsługa incydentu, wyszukiwanie powiązań między Incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z Obsługi incydentu.
- 5.59 **Zdarzenie** – wystąpienie lub zmiana konkretnego zestawu okoliczności.

VI REALIZACJA

6.1 POSTANOWIENIA OGÓLNE

- 6.1.1 W przypadkach, w których Incydent Cyberbezpieczeństwa może narazić ludzi na utratę życia lub zdrowia, lub narazić Spółkę na starty finansowe, uszkodzenie lub zniszczenie urządzeń albo może niekorzystnie wpłynąć na świadczenie Usługi Kluczowej, do decyzji Spółki, po dostarczeniu informacji na temat Incydentu zebranych podczas Obsługi incydentu pozostawia się wybór działań zmierzających do minimalizacji potencjalnych skutków. Po zakończeniu realizacji działań wykonywanych bez zbędnej zwłoki w celu minimalizacji skutków Incydentu, wymagane jest zarejestrowanie podjętych działań w SOM.
- 6.1.2 PGE-CERT świadczy usługi wsparcia w zakresie monitorowania Cyberbezpieczeństwa i Obsługi incydentów w Systemach ICT.
- 6.1.3 Pracownicy lub Kontraktorzy PGE-CERT nie posiadają dostępu do Systemów OT i nie podejmują działań prowadzących do usunięcia Incydentu w Systemach OT.
- 6.1.4 PGE-CERT świadczy usługi wsparcia w zakresie monitorowania Cyberbezpieczeństwa i Obsługi incydentów we wskazanych przez Jednostki Biznesowe Systemach OT na warunkach uzgodnionych z poszczególnymi Jednostkami Biznesowymi wykorzystującymi te systemy. Uzgodnione warunki zapisane są w umowach SLA.
- 6.1.5 PGE-CERT odpowiada za ciągłość działania Obsługi Incydentów Cyberbezpieczeństwa.
- 6.1.6 PGE-CERT w razie potrzeby zabezpiecza Materiał Dowodowy zgodnie z [Załącz.3 Wytyczne w zakresie zabezpieczania Materiału Dowodowego Incydentów Cyberbezpieczeństwa](#). W szczególnych przypadkach PGE-CERT może zwrócić się o pomoc w zabezpieczeniu Materiału Dowodowego do upoważnionych

- Pracowników Spółki (np. do Administratora Systemu). Przy zabezpieczaniu Materiału Dowodowego wykorzystywane są formularze określone w [Załącznik 4 Karta Zabezpieczenia Materiału Dowodowego](#).
- 6.1.7 PGE-CERT przy współpracy i na zlecenie Komórki właściwej ds. strategii ICT w Centrali Spółki realizuje uzgodnione czynności związane z analizą śledczą oraz analizę wykrytych / zaobserwowanych Zagrożeń w ramach zabezpieczonego Materiału Dowodowego.
- 6.1.8 Opiekunem zabezpieczonego materiału i zebranych informacji w toku Obsługi incydentów Cyberbezpieczeństwa przez PGE-CERT jest Kierujący komórką właściwą ds. cyberbezpieczeństwa w PGE Systemy S.A., który zapewnia:
- a. dostępność dokumentów wyłącznie dla osób upoważnionych zgodnie z realizowanymi przez nie zadaniami i za zgodą Spółki, w której wystąpił Incydent,
 - b. ochronę informacji przed niewłaściwym użyciem lub utratą Integralności,
 - c. oznaczanie kolejnych wersji dokumentów umożliwiające określenie zmian dokonanych w tych dokumentach.
- 6.1.9 PGE-CERT ma dostęp do istniejącej i systematycznie aktualizowanej informacji określającej granice Cyberprzestrzeni GK PGE, zarówno w kontekście ICT jak i OT. Informacje o granicach Cyberprzestrzeni GK PGE to adresacje sieci oraz styków z sieciami publicznymi (używane obecnie i posiadane, ale nieuruchomione obecnie), świadczone usługi komercyjne.
- 6.1.10 PGE-CERT jest centralnym punktem gromadzenia informacji o Incydentach Cyberbezpieczeństwa w GK PGE.
- 6.1.11 Kierujący komórką właściwą ds. strategii ICT w PGE S.A. utrzymuje aktualną macierz kontaktów z Karty komunikacji w sposób zapewniający ochronę na poziomie wymaganym dla Danych Osobowych oraz umożliwiającym udostępnienie upoważnionym osobom w razie zaistnienia takiej potrzeby.
- 6.1.12 W SOM zarządzanym przez PGE-CERT, rejestrowany jest każdy Incydent Cyberbezpieczeństwa przez upoważnionego Pracownika reprezentującego:
- a. PGE-CERT lub,
 - b. Komórkę właściwą ds. cyberbezpieczeństwa OT w Oddziale Spółki lub,
 - c. Komórkę właściwą ds. cyberbezpieczeństwa OT w Centrali Spółki.
- 6.1.13 Nie podlegają obowiązkowi rejestrowania w systemie SOM Zdarzenia z obszaru OT wynikające z bieżącej operacyjnej obsługi Systemów automatyki przemysłowej, jeżeli nie stwarzają bezpośredniego lub pośredniego zagrożenia świadczenia Usługi Kluczowej, co do których wprowadzono niezwłocznie działania naprawcze w celu ich wyeliminowania.
- 6.1.14 Zdarzenie opisane w powyższym punkcie podlega jednak zgłoszeniu, jeżeli w toku jego obsługi zaszło podejrzenie, że jego przyczyną mogło być wystąpienie czynnika z zakresu Cyberbezpieczeństwa (np. zdalna ingerencja).
- 6.1.15 PGE-CERT we współpracy z Osobą odpowiedzialną za kontakty z podmiotami KSC oraz Komórką właściwą ds. cyberbezpieczeństwa OT w Centrali Spółki (wraz z funkcjonalnie podlegającymi im Komórkami właściwymi ds. cyberbezpieczeństwa OT w Oddziałach Spółki) realizuje zadania zbierania informacji o Zagrożeniach cyberbezpieczeństwa i Podatnościach Systemu informacyjnego wykorzystywanego w obszarze OT, a w szczególności wykorzystywanych do świadczenia Usługi Kluczowej. W przypadku, gdy w systemie przetwarzane są dane osobowe – informacje przekazywane są również do IOD w celu aktualizacji poziomu ryzyka dla ochrony danych osobowych.
- 6.1.16 Upoważnieni Pracownicy Spółki, do których zwrócił się Pracownik zespołu PGE-CERT w ramach Obsługi incydentu Cyberbezpieczeństwa, obowiązani są do współpracy i niezwłocznego udzielania wymaganych informacji.
- 6.1.17 PGE-CERT oraz osoby z Komórki właściwej ds. cyberbezpieczeństwa OT w Centrali Spółki są upoważnione (w zakresie infrastruktury teleinformatycznej) do:
- 6.1.17.1 Monitorowania zdarzeń systemowych i przepływów sieciowych w Spółkach zagregowanych w SIEM. Monitorowanie dotyczy obszaru informatyki i automatyki.
 - 6.1.17.2 Reagowania na Incydenty Cyberbezpieczeństwa:
 - a. samodzielnie w Systemach utrzymywanych w PGE Systemy,
 - b. samodzielnie w zakresie przyjętych przez Spółki instrukcji,
 - c. zlecania działań zaradczych Administratorom poszczególnych Spółek zgodnie z wewnętrznymi regulacjami Spółek oraz weryfikacji realizacji działań przez Administratorów,
 - d. zlecania działań działom pomocy teleinformatycznej (helpdesk/servicedesk).
 - 6.1.17.3 Zbierania informacji od Spółek dotyczących cyberbezpieczeństwa, w tym o obowiązujących procedurach i Systemach Teleinformatycznych.
 - 6.1.17.4 Komunikacji:

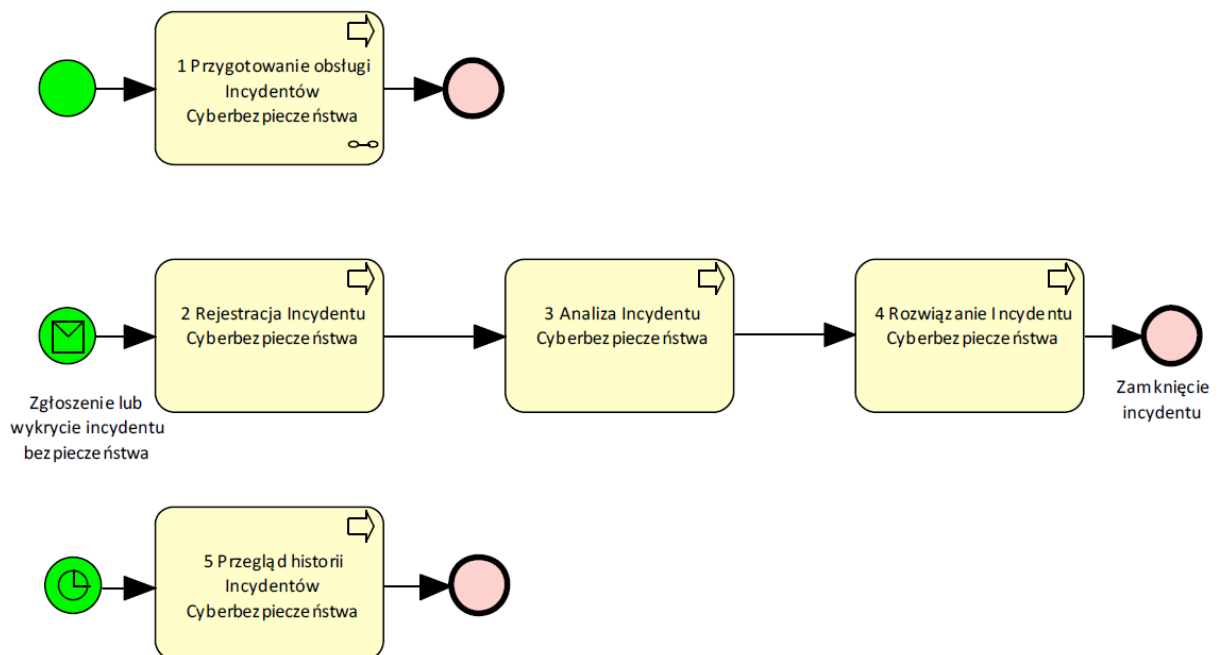
- a. zwracania się do wszystkich komórek Spółek GK o przekazywanie informacji niezbędnych do obsłużenia zarejestrowanych Incydentów,
 - b. prowadzenia korespondencji o występujących Zagrożeniach i sposobach postępowania,
 - c. współpracy operacyjnej z innymi zespołami cyberbezpieczeństwa, wewnętrznymi jak i zewnętrznymi.
- 6.1.17.5 Wyszukiwania i testowania w zakresie Cyberbezpieczeństwa publicznie dostępnych serwisów.
- 6.1.17.6 Rekomendowania zaleceń dotyczących poprawy Cyberbezpieczeństwa.
- 6.1.18 W przypadku incydentów mogących skutkować naruszeniem bezpieczeństwa przetwarzania Danych Osobowych IOD jest upoważniony do reagowania oraz zlecania działań zaradczych.
- 6.1.19 Przetwarzanie danych związanych z Incydentami Cyberbezpieczeństwa realizowane jest z zapewnieniem Bezpieczeństwa Informacji i Rozliczalności.
- 6.1.19.1 Pracownik, Osoba Trzecia bądź użytkownik Systemów Teleinformatycznych należących do GK PGE, który podejrzewa zaistnienie Incydentu Cyberbezpieczeństwa, bądź jest w posiadaniu informacji o Incydencie Cyberbezpieczeństwa zobowiązany jest zgłosić Zdarzenie i przekazać posiadane informacje do PGE-CERT poprzez jeden z kanałów:
- a. e-mail na adres: cert@gkpge.pl,
 - b. zgłoszenie na Service Desk,
 - c. zgłoszenie telefonicznie na dedykowany numer Obsługi Incydentów Cyberbezpieczeństwa PGE-CERT dostępny na stronie intranetowej <https://pgesystemy.pl/CERT-PL>,
Dodatkowo Spółki z GK PGE mogą zgłaszać Zdarzenia poprzez:
 - d. rejestrację Zdarzenia Cyberbezpieczeństwa w SOM,
 - e. w obszarze OT zgodnie z regulacjami szczegółowymi obowiązującymi w Spółce.
- 6.1.19.2 Kierujący komórką właściwą ds. compliance w PGE S.A. niezwłocznie po otrzymaniu zgłoszenia o podejrzeniu zaistnienia incydentu niezgodności w obszarze cyberbezpieczeństwa przekazuje informację poprzez jeden z kanałów wymienionych w pkt 6.1.19.1 ppkt a lub b.
- 6.1.19.3 Wymiana pozostałych informacji (poza zgłoszeniem) dotyczących Incydentów Cyberbezpieczeństwa powinna odbywać się z wykorzystaniem zabezpieczeń kryptograficznych, jedynie w gronie osób upoważnionych zgodnie z Kartą komunikacji oraz z regulacjami obowiązującymi w Spółkach.
- 6.1.20 Incydenty krytyczne mogą przekształcić się w Sytuację Krytyczną.
- 6.1.21 Incydenty Cyberbezpieczeństwa, które zostały zakwalifikowane jako „Sytuacja Krytyczna” są obsługiwane zgodnie z odpowiednimi procedurami Spółek utworzonymi na podstawie *PROG 00038 Procedura Ogólna - Wytyczne w zakresie opracowywania planów zapewnienia ciągłości działania w GK PGE*.
- 6.1.22 PGE-CERT oraz Spółka będąca Operatorem Usługi Kluczowej odpowiada za przekazanie do CSIRT GOV informacji o Incydencie Cyberbezpieczeństwa zaklasyfikowanego, jako Incydent poważny.
- 6.1.23 Wymaga się tworzenie funkcyjnych adresów email (grup dystrybucyjnych lub skrzynek) dla poszczególnych ról dla usprawnienia kontaktów. W szczególności dotyczy to ról wymienionych w tabeli kontaktów w Karcie komunikacji. PGE-CERT będzie wykorzystywał te adresy jako dodatkowy kontakt. Zarządzanie członkami takiej grupy dystrybucyjnej będzie leżało po stronie Spółki.

6.2 ROLE

- 6.2.1 W Zarządzaniu Incydentami Cyberbezpieczeństwa uczestniczą w szczególności następujące role:
- a. CIO,
 - b. Główny Architekt Bezpieczeństwa ICT i OT,
 - c. Osoba odpowiedzialna za kontakty z podmiotami KSC,
 - d. Inspektor Ochrony Danych (IOD),
 - e. Dyrektor ICT Spółki,
 - f. Kierujący komórką właściwą ds. cyberbezpieczeństwa w PGE Systemy S.A.,
 - g. Kierownik PGE-CERT,
 - h. PGE-CERT,
 - i. Ekspert Obsługi Incydentów Cyberbezpieczeństwa,
 - j. Administrator Systemu ICT,
 - k. Właściciel Systemu OT,
 - l. Komórka właściwa ds. cyberbezpieczeństwa OT w Centrali Spółki,
 - m. Komórka właściwa ds. cyberbezpieczeństwa OT w Oddziale Spółki,
 - n. Administrator Systemu OT.
- 6.2.2 Role wymienione w pkt 6.2.1 powyżej, przedstawione są w [Załączniku 5](#) *Macierz RACI i zadania poszczególnych ról*.

6.3 PRZEBIEG DZIAŁAŃ REALIZOWANYCH W RAMACH PROCEDURY

6.3.1 Mapa przebiegu działań w ramach Procedury.



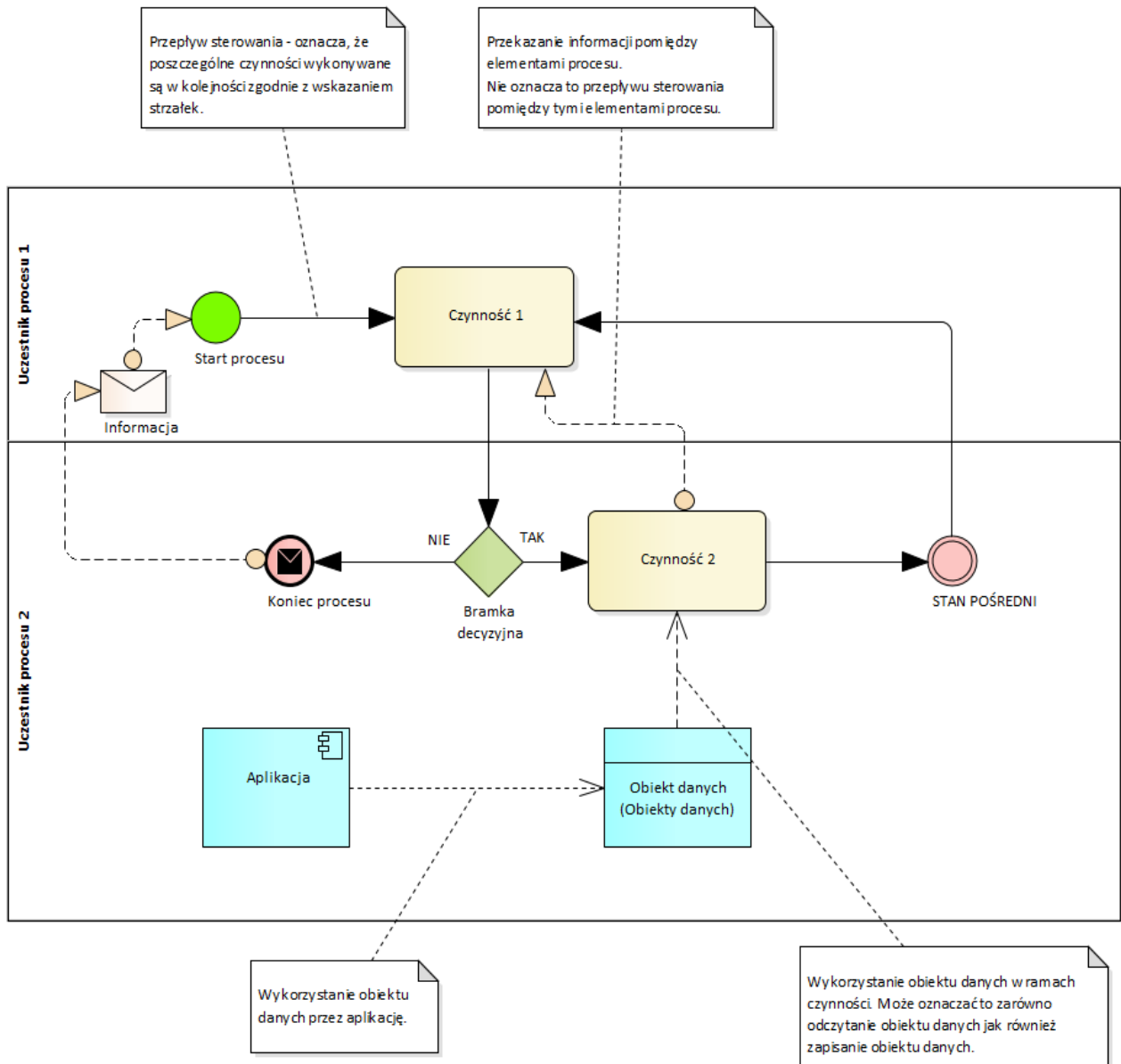
Rysunek 1 Mapa przebiegu działań Zarządzania incydentami Cyberbezpieczeństwa w GK PGE

UWAGA: diagramy w Procedurze zostały opracowane z wykorzystaniem notacji przyjętej do modelowania architektury korporacyjnej GK PGE.

6.3.1.1 Zarządzanie Incydentami Cyberbezpieczeństwa, opracowane z uwzględnieniem najlepszych praktyk w tym zakresie, realizowane jest w 3 aspektach:

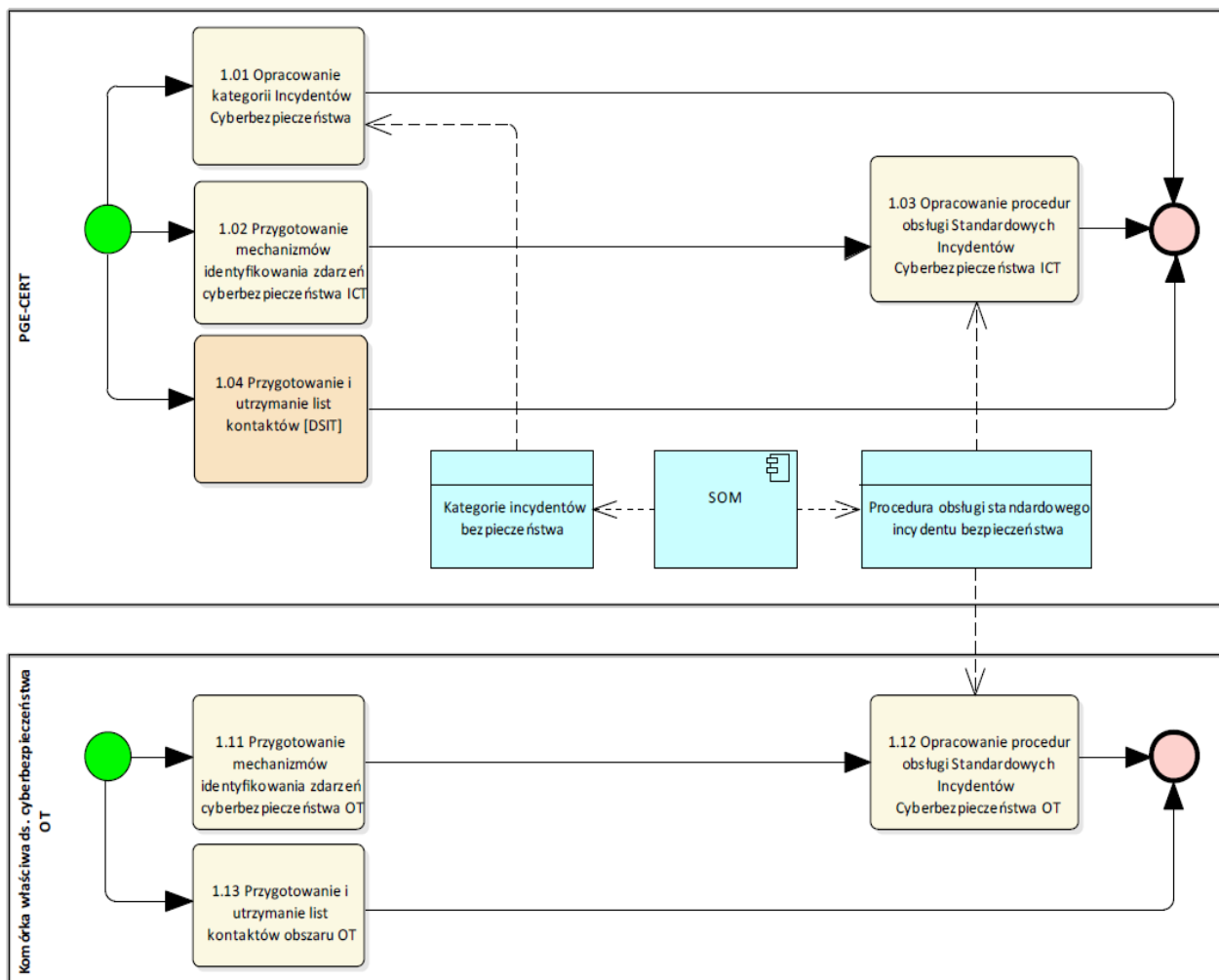
- działania związane z przygotowaniem Obsługi Incydentów Cyberbezpieczeństwa, których celem jest zapewnienie właściwego przygotowania do reagowania na Incydent Cyberbezpieczeństwa,
- działania związane z rejestracją, analizą i rozwiązaniem Incydentów Cyberbezpieczeństwa, których wspólnym celem jest zapewnienie szybkiej, właściwej, skoordynowanej i efektywnej odpowiedzi na Incydent Cyberbezpieczeństwa,
- działania związane z przeglądem historii Incydentów, których celem jest zapewnienie analizy obsłużonych Incydentów Cyberbezpieczeństwa i zaplanowanie działań w celu redukcji ryzyka w przyszłości.

6.3.1.2 Znaczenie elementów umieszczonych na diagramach Obsługi Incydentu Cyberbezpieczeństwa.



Rysunek 2 Przykładowy diagram wraz z wyjaśnieniem opisującym elementy.

6.3.2 Przygotowanie Obsługi Incydentów Cyberbezpieczeństwa.



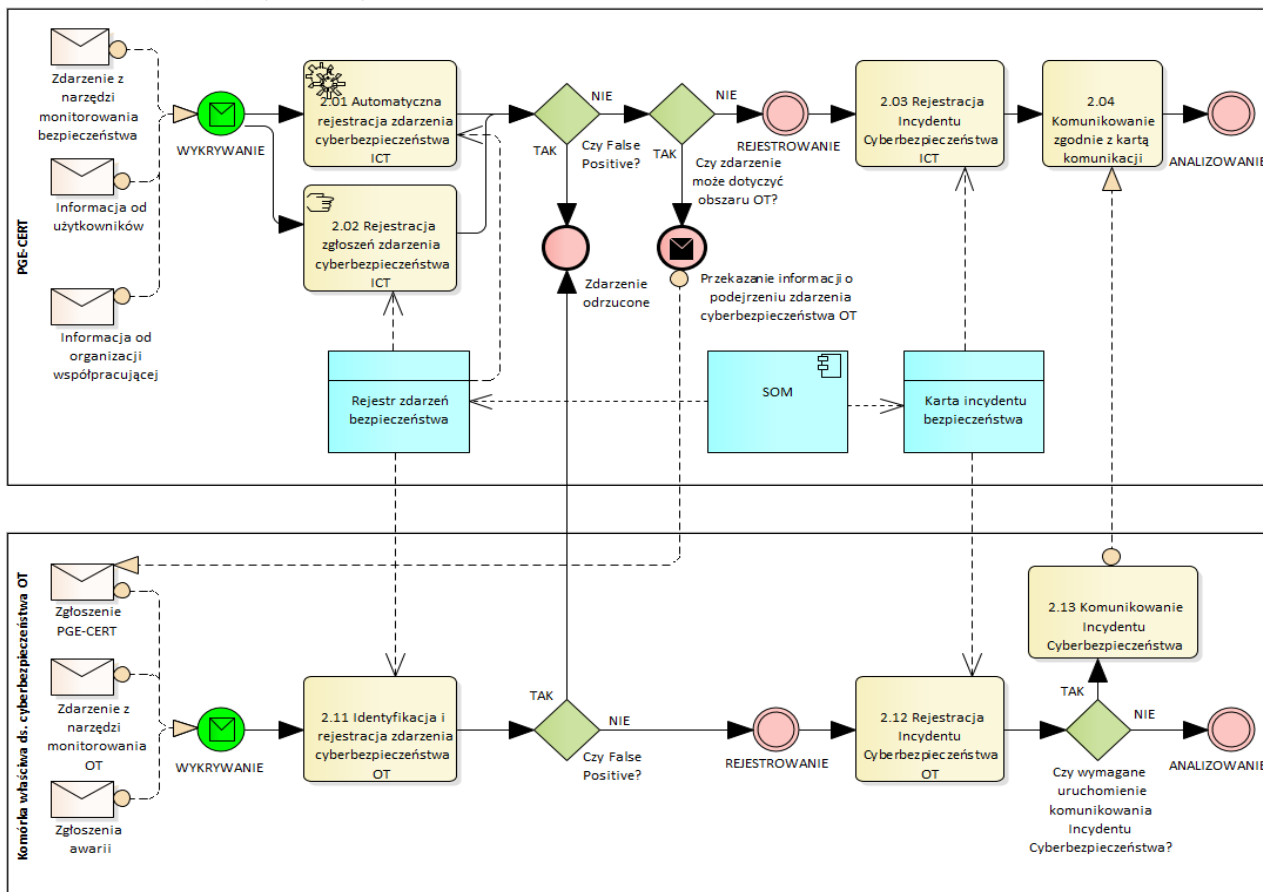
Rysunek 3 Przygotowanie Obsługi Incydentów Cyberbezpieczeństwa

UWAGA: diagram przedstawia działania wykonywane przez poszczególne role oraz komponenty aplikacyjne, które stanowią narzędzie wspierające realizację Procedury, tj. system SOM oraz 2 obiekty danych przetwarzanych przez system SOM. Na diagramie używana jest rola Komórka właściwa ds. cyberbezpieczeństwa OT, którą należy rozumieć jako Komórka właściwa ds. cyberbezpieczeństwa OT w Centrali Spółki lub Komórka właściwa ds. cyberbezpieczeństwa OT w Oddziale Spółki, gdy wewnętrzne regulacje Spółki przekazują odpowiednie kompetencje do Oddziału Spółki.

ID czynności	Rola	Nazwa czynności	Opis czynności
1.01	PGE-CERT Komórka właściwa ds. cyberbezpieczeństwa OT w Centrali Spółki	Opracowanie kategorii Incydentów Cyberbezpieczeństwa	Działanie polega na regularnej weryfikacji kategoryzacji Incydentów Cyberbezpieczeństwa oraz dostosowanie go w miarę potrzeb. Kategorie Incydentów Cyberbezpieczeństwa będą częścią kategorii Incydentów bezpieczeństwa.
1.02	PGE-CERT	Przygotowanie mechanizmów identyfikowania Zdarzeń Cyberbezpieczeństwa ICT	Działanie obejmuje przygotowanie mechanizmów służących monitorowaniu i identyfikacji Zdarzeń Cyberbezpieczeństwa.
1.03	PGE-CERT	Opracowanie procedur obsługi Standardowych Incydentów Cyberbezpieczeństwa ICT	Opracowanie i aktualizacja procedur reagowania na Standardowe Incydenty Cyberbezpieczeństwa. Procedury mają umożliwiać osobie niebędącej ekspertem w dziedzinie reagowania na Incydenty Cyberbezpieczeństwa, przeprowadzenie Obsługi incydentu o znanej kategorii.
1.04	DSIT	Przygotowanie i utrzymanie list kontaktów	DSIT prowadzi listy kontaktów osób wskazanych do kontaktu dla Pracowników PGE-CERT:

ID czynności	Rola	Nazwa czynności	Opis czynności
			<ol style="list-style-type: none"> 1. Dyrektorów ICT 2. Pracowników reprezentujących Komórki właściwe ds. cyberbezpieczeństwa OT w Centrali Spółki, 3. Pracowników reprezentujących Komórki właściwe ds. cyberbezpieczeństwa OT w Oddziale Spółki, 4. IOD. <p>Listy kontaktów powinny obejmować co najmniej:</p> <ol style="list-style-type: none"> 1. Spółkę 2. Rolę w Spółce (np. Dyrektor ICT) 3. Stanowisko 4. Imię i nazwisko 5. Email 6. Telefon <p>Kontakty email powinny obejmować funkcyjne adresy email (grup dystrybucyjne lub skrzynki funkcyjne).</p>
1.11	Komórka właściwa ds. cyberbezpieczeństwa OT w Centrali Spółki	Przygotowanie mechanizmów identyfikowania Zdarzeń Cyberbezpieczeństwa OT	Działanie obejmuje przygotowanie mechanizmów służących monitorowaniu i identyfikacji Zdarzeń Cyberbezpieczeństwa OT
1.12	Komórka właściwa ds. cyberbezpieczeństwa OT w Centrali Spółki	Opracowanie procedur obsługi Standardowych Incydentów Cyberbezpieczeństwa OT	Opracowanie i aktualizacja procedur reagowania na Standardowe Incydenty Cyberbezpieczeństwa w OT. Procedury mają umożliwiać osobie niebędącej ekspertem w dziedzinie reagowania na Incydenty Cyberbezpieczeństwa w OT, przeprowadzenie Obsługi incydentu o znanej kategorii.
1.13	Komórka właściwa ds. cyberbezpieczeństwa OT w Centrali Spółki	Przygotowanie i utrzymanie list kontaktów obszaru OT	Przygotowanie i utrzymywanie list kontaktów do osób zaangażowanych w Obsługę Incydentów Cyberbezpieczeństwa w obszarze OT Spółki.

6.3.3 Rejestracja Incydentu Cyberbezpieczeństwa.

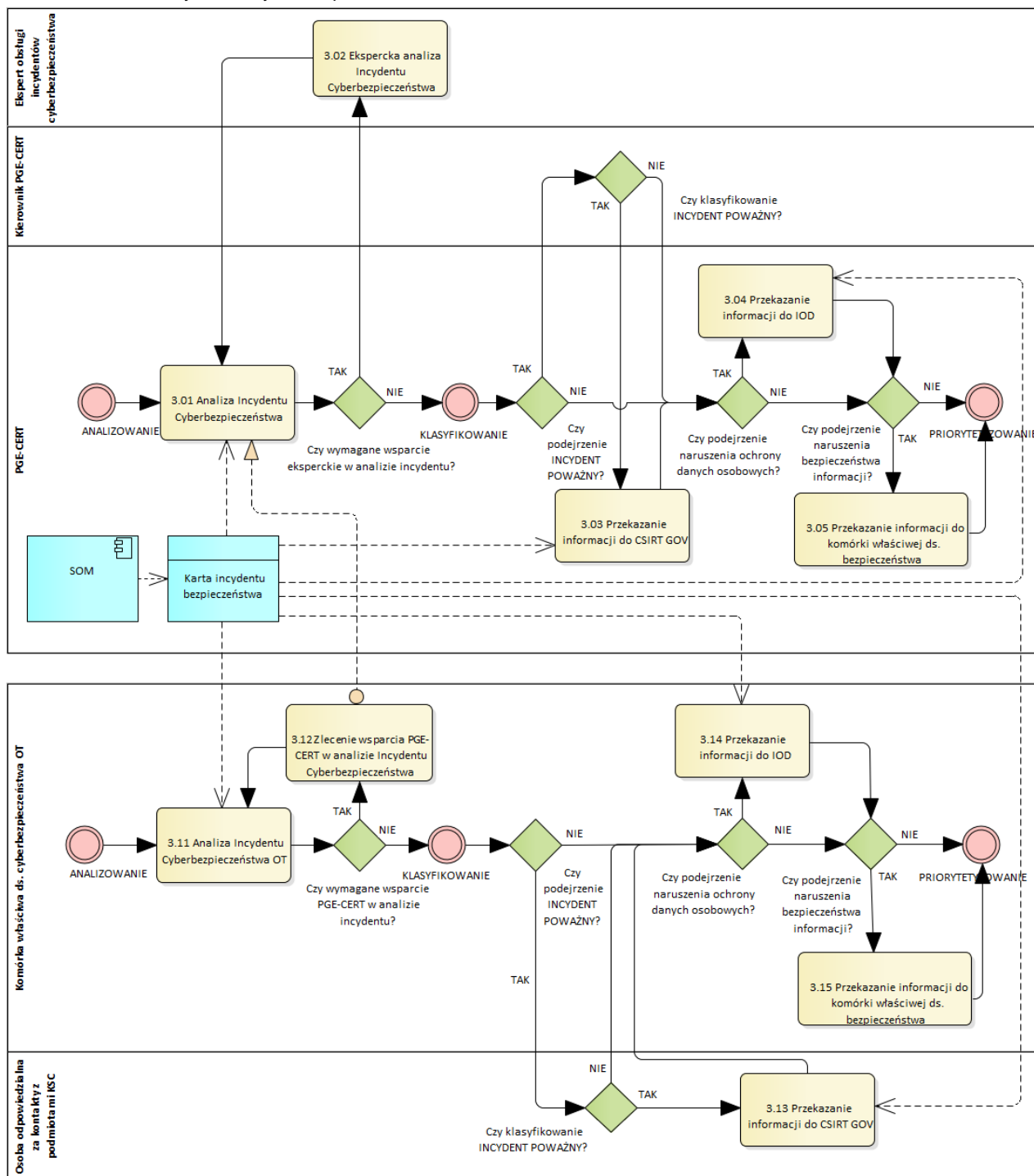


Rysunek 4 Rejestracja Incydentu Cyberbezpieczeństwa

ID czynności	Rola	Nazwa czynności	Opis czynności
2.01	PGE-CERT	Automatyczna rejestracja Zdarzenia Cyberbezpieczeństwa ICT	Automatyczna rejestracja Zdarzenia Cyberbezpieczeństwa ICT poprzez integrację narzędzi monitorowania z SOM.
2.02	PGE-CERT	Rejestracja zgłoszeń Zdarzenia Cyberbezpieczeństwa ICT	Ręczna rejestracja Zdarzenia Cyberbezpieczeństwa w SOM, realizowana w przypadkach zgłoszenia Zdarzenia przez użytkowników oraz inne strony, np. współpracujące organizacje lub w przypadku Incydentu Cyberbezpieczeństwa, który wystąpi w systemie niezintegrowanym z SOM.
2.03	PGE-CERT	Rejestracja Incydentu Cyberbezpieczeństwa	<p>Uzupełnienie podstawowych informacji odnośnie Incydentu Cyberbezpieczeństwa:</p> <ul style="list-style-type: none"> - Typ Incydentu - Priorytet - Kategoria (na podstawie Załącznik 1 Kryteria klasyfikacji Incydentów Cyberbezpieczeństwa, parametr opcjonalny na tym etapie). <p>W trakcie rejestracji dokonana jest weryfikacja, czy Zdarzenie jest duplikatem lub jest powiązane z innym już istniejącym Incydentem Cyberbezpieczeństwa. Jeżeli tak, to jest dowiązywane do tego Incydentu Cyberbezpieczeństwa i zarządzane łącznie jako jeden Incydent Cyberbezpieczeństwa.</p>

ID czynności	Rola	Nazwa czynności	Opis czynności
2.04	PGE-CERT	Komunikowanie zgodnie z Kartą komunikacji	Przekazanie informacji o potencjalnej potrzebie eskalacji Incydentu Cyberbezpieczeństwa w obszarze ICT. Komunikowaniu podlegają w szczególności Incydeny Cyberbezpieczeństwa z kategorii podejrzeń Naruszenia ochrony Danych Osobowych, naruszeń pracowniczych, Incydeny zgłoszone przez CSIRT GOV, Incydeny zgłaszane jako POWAŻNE. Komunikowanie wystąpienia Incydentu ma być realizowane zgodnie z Kartą komunikacji (Załącznik 2 – Karta komunikacji Incydentów Cyberbezpieczeństwa), w szczególności biorąc pod uwagę wskazanie kiedy ma nastąpić komunikowanie.
2.11	Komórka właściwa ds. cyberbezpieczeństwa OT w Centrali Spółki Komórka właściwa ds. cyberbezpieczeństwa OT w Oddziale Spółki	Identyfikacja i rejestracja Zdarzenia Cyberbezpieczeństwa OT	Wszelkie działania po stronie Systemów OT zmierzające do zidentyfikowania Zdarzeń o charakterze Cyberbezpieczeństwa oraz ich zarejestrowaniu w zbiorze Zdarzeń prowadzonym w SOM.
2.12	Komórka właściwa ds. cyberbezpieczeństwa OT w Centrali Spółki Komórka właściwa ds. cyberbezpieczeństwa OT w Oddziale Spółki	Rejestracja Incydentu Cyberbezpieczeństwa OT	Patrz adekwatnie do Rejestracja Incydentu Cyberbezpieczeństwa (ID czynności: 2.03 w niniejszej tabeli).
2.13	Komórka właściwa ds. cyberbezpieczeństwa OT w Centrali Spółki Komórka właściwa ds. cyberbezpieczeństwa OT w Oddziale Spółki	Komunikowanie zgodnie z Kartą komunikacji	Uruchomienie komunikowania Incydentu Cyberbezpieczeństwa – poprzez przekazanie do PGE-CERT informacji niezbędnych do komunikowania.

6.3.4 Analiza Incydentu Cyberbezpieczeństwa.



Rysunek 5 Analiza Incydentu Cyberbezpieczeństwa

ID czynności	Rola	Nazwa czynności	Opis czynności
3.01	PGE-CERT	Analiza Incydentu Cyberbezpieczeństwa	Analiza obejmuje przypisanie Kategorii Incydentu. Incydent Cyberbezpieczeństwa jest obsługiwany przez specjalistę PGE-CERT. Organizacja pracy PGE-CERT jest regulowana wewnętrznymi procedurami PGE-CERT.
3.02	Ekspert Obsługi Incydentów Cyberbezpieczeństwa	Eksperska analiza Incydentu Cyberbezpieczeństwa	Analiza wykonywana przez zewnętrznych ekspertów, na podstawie umów PGE-CERT.
3.03	PGE-CERT	Przekazanie informacji do CSIRT GOV	Przekazanie do właściwego CSIRT informacji o Incydencie Cyberbezpieczeństwa zaklasyfikowanym jako Incydent poważny

ID czynności	Rola	Nazwa czynności	Opis czynności
			niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia.
3.04	PGE-CERT	Przekazanie informacji do IOD	Przekazanie informacji o podejrzeniu Naruszenia ochrony Danych Osobowych do właściwego IOD.
3.05	PGE-CERT	Przekazanie informacji do komórki właściwej ds. bezpieczeństwa	Przekazanie informacji o podejrzeniu naruszenia Bezpieczeństwa Informacji do właściwej komórki ds. bezpieczeństwa.
3.11	Komórka właściwa ds. cyberbezpieczeństwa OT w Centrali Spółki Komórka właściwa ds. cyberbezpieczeństwa OT w Oddziale Spółki	Analiza Incydentu Cyberbezpieczeństwa OT	Analiza obejmuje przypisanie Kategorii Incydentu. Analiza jest realizowana w oparciu o zdefiniowane procedury obsługi Standardowego Incydentu Cyberbezpieczeństwa dla środowisk OT, a w przypadkach nieopisanych procedurami podejmowane są działania adekwatne do sytuacji.
3.12	Komórka właściwa ds. cyberbezpieczeństwa OT w Centrali Spółki Komórka właściwa ds. cyberbezpieczeństwa OT w Oddziale Spółki	Zlecenie wsparcia PGE-CERT w analizie Incydentu Cyberbezpieczeństwa	Zlecenie wsparcia przez PGE-CERT analizy Incydentu Cyberbezpieczeństwa.
3.13	Osoba odpowiedzialna za kontakty z podmiotami KSC	Przekazanie informacji do CSIRT GOV	Przekazanie do właściwego CSIRT informacji o Incydencie Cyberbezpieczeństwa zaklasyfikowanym jako Incydent poważny niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia.
3.14	Komórka właściwa ds. cyberbezpieczeństwa OT w Centrali Spółki Komórka właściwa ds. cyberbezpieczeństwa OT w Oddziale Spółki	Przekazanie informacji do IOD	Przekazanie informacji o podejrzeniu Naruszenia ochrony Danych Osobowych do właściwego IOD.
3.15	Komórka właściwa ds. cyberbezpieczeństwa OT w Centrali Spółki Komórka właściwa ds. cyberbezpieczeństwa OT w Oddziale Spółki	Przekazanie informacji do komórki właściwej ds. bezpieczeństwa	Przekazanie informacji o podejrzeniu Naruszenia Bezpieczeństwa Informacji do właściwej komórki ds. bezpieczeństwa.

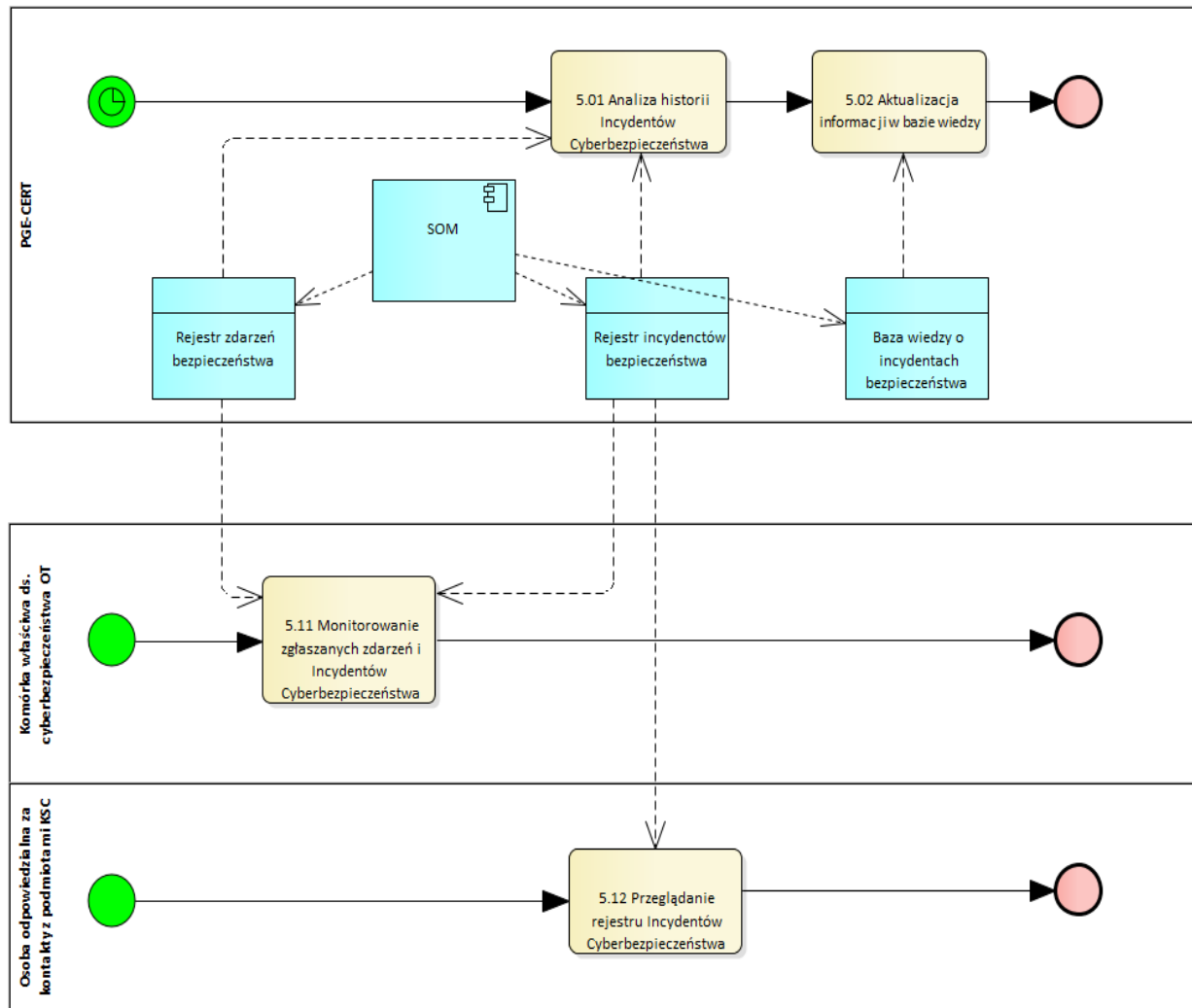
- 6.3.4.1 Jeżeli Incydent Cyberbezpieczeństwa jest powiązany z podejrzeniem Naruszenia ochrony Danych Osobowych, PGE-CERT ma obowiązek przekazywać posiadane na dany moment informacje właściwemu IOD bez zbędnej zwłoki, zgodnie z Kartą komunikacji, w tym prawdopodobna przyczyna incydentu, kategoria osób, których dotyczy incydent, liczba i zakres danych, których dotyczy incydent, skutki naruszenia w zakresie poufności, integralności, dostępności danych, podjęte i planowane działania zaradcze.
- 6.3.4.2 Informacje o których mowa w pkt. 6.3.4.1 powyżej powinny być przekazane za pomocą Karty informacyjnej ODO, stanowiącej załącznik nr 6 do Procedury.
- 6.3.4.3 IOD niezwłocznie przekazuje zwrótnie informację o kwalifikacji incydentu jako Naruszenia ochrony Danych Osobowych oraz podjętych działaniach. IOD ma prawo pozyskiwania z PGE CERT wszelkich informacji koniecznych do zakwalifikowania incydentu jako Naruszenia oraz wszelkich informacji koniecznych do przygotowania zgłoszenia Naruszenie do organu nadzorczego.
- 6.3.4.4 Jeżeli Incydent Cyberbezpieczeństwa jest powiązany z podejrzeniem naruszenia Bezpieczeństwa Informacji, PGE-CERT ma obowiązek przekazywać posiadane na dany moment informacje właściwemu kierującemu komórką ds. bezpieczeństwa w Spółce bez zbędnej zwłoki, zgodnie z Kartą komunikacji.

6.3.5 Rozwiązanie Incydentu Cyberbezpieczeństwa.

Strona 16 z 20

ID czynności	Rola	Nazwa czynności	Opis czynności
			Cyberbezpieczeństwa, gdy to zasadne we współpracy ze specjalistami, np. Administratorami Systemu. Dla działań naprawczych wymagane jest określenie priorytetu, który pozwoli na wykonanie działań pilnych w pierwszej kolejności. W ramach działań naprawczych należy uwzględnić konieczność ograniczenia skutków Incydentu Cyberbezpieczeństwa.
4.02	Ekspert Obsługi Incydentów Cyberbezpieczeństwa	Eksperskie opracowanie działań naprawczych	Opracowanie działań naprawczych wykonywane przez zewnętrznych ekspertów, na podstawie umów PGE-CERT.
4.03	Administrator Systemu	Realizacja działań naprawczych	Aktywność obejmuje testowanie rozwiązania i zastosowanie go. W sytuacji gdy PGE-CERT nie dysponuje dokumentacją pozwalającą na zidentyfikowanie odpowiedniego Administratora Systemu, zwraca się do Dyrektora ICT o potrzebie wsparcia w obsłudze Incydentu Cyberbezpieczeństwa.
4.04	PGE-CERT	Opracowanie i wysłanie wymaganych raportów	Jeżeli kwalifikacja Incydentu wymaga opracowania raportu i przekazania do współpracujących organizacji, to takie raporty są wykonywane i przekazywane. Organizacje współpracujące to np. inne zespoły CERT lub CSIRT. Raporty z Incydentów poważnych / krytycznych będą przekazywane również do Jednostek organizacyjnych, w których te Incydenty wystąpiły.
4.11	Komórka właściwa ds. cyberbezpieczeństwa OT w Centrali Spółki Komórka właściwa ds. cyberbezpieczeństwa OT w Oddziale Spółki	Opracowanie działań naprawczych OT i określenie priorytetu ich realizacji	Decyzję w zakresie zastosowania odpowiednich działań naprawczych i ograniczających ewentualne skutki Incydentu podejmuje kierujący komórką właściwą ds. cyberbezpieczeństwa OT w Oddziale Spółki przy współpracy z Właścicielem Systemu OT i Administratorem Systemu OT w uzgodnieniu z Komórką właściwą ds. cyberbezpieczeństwa OT w Centrali Spółki i odnotowuje w Karcie Incydentu Cyberbezpieczeństwa.
4.12	Komórka właściwa ds. cyberbezpieczeństwa OT w Centrali Spółki Komórka właściwa ds. cyberbezpieczeństwa OT w Oddziale Spółki	Zlecenie wsparcia PGE-CERT w opracowaniu działań naprawczych	Zlecenie wsparcia przez PGE-CERT opracowania działań naprawczych.
4.13	Komórka właściwa ds. cyberbezpieczeństwa OT w Centrali Spółki Komórka właściwa ds. cyberbezpieczeństwa OT w Oddziale Spółki	Realizacja działań naprawczych OT	Koordynacja i nadzór nad pracami podejmowanymi w celu usunięcia Podatności lub Incydentu.

6.3.6 Przegląd historii Incyidentów Cyberbezpieczeństwa.



Rysunek 7 Przegląd historii Incyidentów Cyberbezpieczeństwa

ID czynności	Rola	Nazwa czynności	Opis czynności
5.01	PGE-CERT	Analiza historii Incyidentów Cyberbezpieczeństwa	Analiza historii Zdarzeń i Incyidentów Cyberbezpieczeństwa oraz zaplanowanie działań w celu redukcji ryzyka w przyszłości. W zakresie swoich kompetencji - przekazanie rekomendacji.
5.02	PGE-CERT	Aktualizacja informacji w bazie wiedzy	Aktualizacja bazy wiedzy o Standardowych Incyidentach Cyberbezpieczeństwa.
5.11	Komórka właściwa ds. cyberbezpieczeństwa OT w Centrali Spółki Komórka właściwa ds. cyberbezpieczeństwa OT w Oddziale Spółki	Monitorowanie zgłaszanych Zdarzeń i Incyidentów Cyberbezpieczeństwa	Przegląd i monitorowanie informacji o Zdarzeniach cyberbezpieczeństwa oraz Incyidentach Cyberbezpieczeństwa. Analiza historii Incyidentów Cyberbezpieczeństwa i zaplanowanie działań w celu redukcji ryzyka w przyszłości. Jeżeli Incydent dotyczy ODO – informacja o poziomie ryzyka przekazywana jest do właściwego IOD.
5.12	Osoba odpowiedzialna za kontakty z podmiotami KSC	Przeglądanie rejestru Incyidentów Cyberbezpieczeństwa	Przeglądanie zarejestrowanych Incyidentów Cyberbezpieczeństwa.

6.3.6.1 Przegląd historii Incyidentów Cyberbezpieczeństwa musi być przeprowadzony nie rzadziej niż raz na 3 miesiące. W trakcie prowadzenia przeglądu weryfikowana jest również aktualność macierzy kontaktów w Karcie komunikacji.

6.3.6.2 W zależności od wyników przeglądu podejmowana jest decyzja o:

- a. dodaniu nowego Incydentu Cyberbezpieczeństwa do listy Standardowych Incydentów Cyberbezpieczeństwa, wraz z opisami sprawdzonych metod zbierania Materiałów Dowodowych oraz rozwiązania Incydentu Cyberbezpieczeństwa,
 - b. modyfikacji istniejących postanowień dotyczących Standardowych Incydentów Cyberbezpieczeństwa (np. zmiany którejs z metod na inną, uznaną za bardziej efektywną),
 - c. zainicjowaniu zmiany w Procedurze,
 - d. zarekomendowaniu zmian w obszarze zarządzania cyberbezpieczeństwem GK PGE lub Klientów.
- 6.3.6.3 Wyniki przeglądu zostają przedstawione w Raporcie Incydentów Cyberbezpieczeństwa. Kierownik PGE-CERT przedkłada raport CIO, Głównemu Architektowi Bezpieczeństwa ICT i OT oraz kierującemu komórką właściwą ds. cyberbezpieczeństwa w PGE Systemy S.A. w terminie do dwóch tygodni od daty przeprowadzenia przeglądu.
- 6.3.6.4 Kierownik PGE-CERT zapewnia dostępność Raportów Incydentów Cyberbezpieczeństwa osobom upoważnionym przez Spółkę.
- 6.3.6.5 Raporty Incydentów Cyberbezpieczeństwa oznaczane są klauzulą „Tajemnica Spółki” i rejestrowane są w stosownym dzienniku.

6.4 KARTA INCYDENTU CYBERBEZPIECZEŃSTWA

- 6.4.1 Informacje o Incydencie bezpieczeństwa są przechowywane w Karcie Incydentu Cyberbezpieczeństwa.
- 6.4.2 Karta Incydentu Cyberbezpieczeństwa obejmuje, co najmniej następujące informacje:
- a. numer Incydentu,
 - b. datę utworzenia karty,
 - c. typ Incydentu,
 - d. priorytet,
 - e. kategorie Incydentu,
 - f. klasyfikacja Incydentu,
 - g. symptomy Incydentu,
 - h. przyczyny Incydentu,
 - i. zastosowane rozwiązanie.
- 6.4.3 Karta Incydentu Cyberbezpieczeństwa jest przechowywana w formie elektronicznej w SOM.
- 6.4.4 Kopie Karty Incydentu Cyberbezpieczeństwa, np. w postaci eksportu danych lub wydruku są aktualne na moment wykonania tej czynności.

6.5 KATEGORIE INCYDENTÓW CYBERBEZPIECZEŃSTWA

- 6.5.1 Incydynty Cyberbezpieczeństwa podlegają kategoryzacji określonej w [Załącz. 1](#) Kryteria klasyfikacji Incydentów Cyberbezpieczeństwa.
- 6.5.2 Incydynty Cyberbezpieczeństwa, które mają określoną kategorię pochodzącą z [Załącz. 1](#) Kryteria klasyfikacji Incydentów Cyberbezpieczeństwa, mogą mieć przypisaną inną kategorię niewprowadzoną jeszcze do ww. [Załącz. 1](#).

6.6 PROCEDURY OBSŁUGI STANDARDOWYCH INCYDENTÓW CYBERBEZPIECZEŃSTWA

- 6.6.1 Standardowe Incydynty Cyberbezpieczeństwa w pierwszej kolejności są obsługiwane przy wykorzystaniu procedur obsługi Standardowych Incydentów Cyberbezpieczeństwa.
- 6.6.2 Procedury obsługi Standardowych Incydentów Cyberbezpieczeństwa są gromadzone i wykorzystywane zarówno przez PGE-CERT jak również innych specjalistów zajmujących się Obsługą incydentów.
- 6.6.3 Procedury obsługi Standardowych Incydentów Cyberbezpieczeństwa mogą być opracowywane przez specjalistów posiadających doświadczenie w opracowywaniu sposobów Obsługi incydentów.
- 6.6.4 Każda Procedura obsługi Standardowych Incydentów Cyberbezpieczeństwa musi zawierać, co najmniej:
- a. nazwę,
 - b. wersję,
 - c. kroki Obsługi incydentu z określeniem, czy krok jest wymagany bądź opcjonalny.

6.7 POWOŁANIE RÓL W PGE-CERT I KOMÓRKACH DS. CYBERBEZPIECZEŃSTWA OT

- 6.7.1 Członkowie zespołu PGE-CERT są powoływani przez kierującego komórką właściwą ds. cyberbezpieczeństwa w PGE Systemy S.A.
- 6.7.2 Członkowie Komórki właściwej ds. cyberbezpieczeństwa OT w Oddziale Spółki są powoływani zgodnie z regulacjami obowiązującymi w Spółkach.

6.8 WYZNACZANIE UPOWAŻNIONEGO PRACOWNIKA SPÓŁKI

- 6.8.1 Przez upoważnionych Pracowników Spółki rozumie się osoby wskazane do kontaktu dla Pracowników PGE- CERT oraz inne osoby, które zostały wskazane przez upoważnionych Pracowników Spółki zgodnie z Kartą komunikacji.
- 6.8.2 Upoważnionym Pracownikiem Spółki jest w szczególności Administrator Systemu.
- 6.8.3 W sytuacji, gdy PGE-CERT nie dysponuje dokumentacją pozwalającą na zidentyfikowanie odpowiedniego Administratora Systemu, zwraca się do Dyrektora ICT z potrzebą wsparcia w obsłudze Incydentu Cyberbezpieczeństwa, który wskazuje upoważnionego Pracownika Spółki.

6.9 POSTANOWIENIA KOŃCOWE

- 6.9.1 W zakresie nieobjętym niniejszą Procedurą lub innymi regulacjami zawartymi w aktach normatywnych GK PGE, należy postępować zgodnie z interesem Spółki, kierując się wiedzą, doświadczeniem oraz najlepszymi praktykami dochowując należytej staranności we wszystkich podejmowanych działaniach.
- 6.9.2 Wszelkie zmiany w załącznikach do Procedury, niezbędne dla prawidłowej realizacji Procedury (poza zmianami dotyczącymi dołączania nowych i usuwania istniejących załączników lub powodującymi zmianę przebiegu procesu), wymagają uzgodnienia ze Spółkami, jeśli ich dotyczą i nie powodują konieczności zmiany Procedury, oraz wymagają akceptacji kierującego komórką właściwą ds. strategii ICT w PGE S.A.
- 6.9.3 Z dniem wejścia w życie niniejszej Procedury, traci moc obowiązująca *PROG 00116/A Procedura Ogólna Zarządzania Incydentami Cyberbezpieczeństwa w GK PGE*.
- 6.9.4 Procedura wchodzi w życie po upływie 7 dni od dnia jej publikacji w Banku DSZ.