PROCEDURA
ORGANIZACJA I ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI W PGE GiEK S.A.

PROC 10072/B

Sygn.: GIEK/CENT/PZ/4.16

Data zatwierdzenia: 09/01/2018
Obowiązuje od: 09/01/2018

I CEL I ZAKRES

1.1 Mając na uwadze potrzebę skutecznej ochrony aktywów informacyjnych, prowadzenie działalności gospodarczej w zgodności z przepisami prawa oraz potrzebę zapewnienia ciągłości działania Zarząd PGE GiEK S.A. podjął decyzję (pkt 3.1) o wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnego z normą PN-ISO/IEC 27001 (pkt 3.2), jako systemu składowego Zintegrowanego Systemu Zarządzania (ZSZ).
Zakres i granice SZBI zostały zdefiniowane w regulacji wewnętrznej – Model Zintegrowanego Systemu Zarządzania w PGE GiEK S.A. (pkt 3.16).

1.2 Celem niniejszej procedury (Procedura) jest opis SZBI, w szczególności określenie struktury wewnętrznej niezbędnej do zapewnienia bezpieczeństwa informacji oraz sposobu zarządzania integralnością, dostępnością i poufnością informacji w PGE GiEK S.A. (Spółka).

1.3 Procedura określa zasady postępowania z ryzykiem związanym z przetwarzaniem informacji w Spółce oraz wynikające z tych zasad działania składające się na zarządzanie bezpieczeństwem informacji, oparte o uznane normy i dobre praktyki, z uwzględnieniem celów biznesowych i wymagań prawnych, w tym związanych z:

a. ochroną danych osobowych,
b. tajemnicami Spółki,
c. obrotem na giełdach towarowych (w tym handel energią),
d. notowaniem akcji PGE Polska Grupa Energetyczna S.A. na Giełdzie Papierów Wartościowych w Warszawie.

1.4 Zakres organizacyjny Procedury obejmuje wszystkie komórki organizacyjne Spółki.

II ODPOWIEDZIALNOŚĆ

2.1 Pełnomocnik ds. ZSZ odpowiedzialny jest za zapewnienie formalnych podstaw SZBI oraz nadzór nad jego funkcjonowaniem.

2.2 Zastępca Pełnomocnika ds. ZSZ (Administrator Funkcjonalny ZSZ) odpowiedzialny jest za opracowanie i aktualizację koncepcji SZBI, monitorowanie jego funkcjonowania i podejmowanie działań odpowiednich do uzyskanych informacji, w tym koordynację współpracy Administratorów Merytorycznych SZBI w Spółce oraz inicjowanie / uzgadnianie zmian w regulacjach wewnętrznych dotyczących SZBI dla Spółki, ze szczególnym uwzględnieniem spójności ZSZ.

2.3 Administratorzy Merytoryczni SZBI w Spółce w odniesieniu do bezpieczeństwa informacji odpowiedzialni są za:

a. zapewnienie opracowania regulacji wewnętrznych i standardów dla Spółki dotyczących SZBI, w przypisanym zakresie merytorycznym, przystępności ich treści, poprawności merytorycznej oraz zgodności z wymaganiami: prawa, normy PN ISO/IEC 27001 i regulacji wewnętrznych dla spółek GK PGE dotyczących bezpieczeństwa informacji,
b. uzgadnianie i uzyskanie akceptacji Administratora Funkcjonalnego ZSZ dla zmian w opracowywanych regulacjach wewnętrznych dla Spółki oraz Administratorów Merytorycznych SZBI w Spółce i innych osób pełniących role w ZSZ, których zmiany dotyczą,
c. nadzorowanie stosowania regulacji wewnętrznych i standardów w zakresie bezpieczeństwa informacji w Centrali Spółki oraz zapewnienie spójności (interpretacji) ich stosowania w Oddziałach Spółki,
d. wnioskowanie o zwołanie / inicjowanie posiedzenia Forum BI w związku z incydentami lub innymi kwestiami dotyczącymi bezpieczeństwa informacji o szczególnym znaczeniu dla Spółki,
e. szacowanie ryzyka w bezpieczeństwie informacji w przypisanym im zakresie,
f. udzielanie wsparcia merytorycznego pracownikom Centrali Spółki w realizacji ich zadań związanych z bezpieczeństwem informacji w przypisanym zakresie merytorycznym.

2.4 Administratorzy Merytoryczni SZBI w Oddziale Spółki, w odniesieniu do bezpieczeństwa informacji, odpowiedzialni są za:

a. zapewnienie opracowania: regulacji wewnętrznych dla Oddziału dotyczących SZBI, w przypisanym zakresie merytorycznym, przystępności ich treści, poprawności merytorycznej oraz zgodności z wymaganiami: prawa, normy PN ISO/IEC 27001 i regulacji opracowanych dla GK PGE, dotyczących bezpieczeństwa informacji,

b. uzgadnianie i uzyskanie akceptacji Koordynatora SZBI (pkt 2.5) oraz Koordynatora ZSZ dla zmian w opracowywanych regulacjach wewnętrznych dla Oddziału (ze szczególnym uwzględnieniem spójności ZSZ) i innych osób pełniących role w ZSZ, których zmiany dotyczą,
c. nadzorowanie stosowania regulacji wewnętrznych dotyczących SZBI w Oddziale (w przypisanym zakresie merytorycznym),
d. wnioskowanie o zwołanie / inicjowanie posiedzenia Lokalnego Forum BI w związku z incydentami lub innymi kwestiami dotyczącymi bezpieczeństwa informacji o szczególnym znaczeniu dla Oddziału,
e. szacowanie ryzyka w bezpieczeństwie informacji w przypisanym im zakresie,
f. udzielanie wsparcia merytorycznego pracownikom Oddziału w realizacji ich zadań związanych z bezpieczeństwem informacji w przypisanym zakresie merytorycznym.

2.5 Koordynator SZBI jest odpowiedzialny za koordynację współpracy Administratorów Merytorycznych SZBI w Oddziale Spółki oraz za inicjowanie / uzgadnianie i akceptowanie zmian w regulacjach wewnętrznych dla Oddziału, ze szczególnym uwzględnieniem spójności SZBI.
Rolę Koordynatora SZBI pełni Administrator Merytoryczny SZBI w Oddziale Spółki w zakresie bezpieczeństwa fizycznego i środowiskowego lokalizacji, ochrony danych osobowych i tajemnic Spółki.

2.6 Koordynator ZSZ jest odpowiedzialny za inicjowanie / uzgadnianie i akceptowanie zmian w regulacjach wewnętrznych dotyczących SZBI dla Oddziału Spółki, ze szczególnym uwzględnieniem spójności ZSZ.

2.7 Forum Bezpieczeństwa Informacji oraz Lokalne Fora Bezpieczeństwa Informacji odpowiedzialne są za rozpatrywanie szczególnie istotnych lub spornych kwestii dotyczących bezpieczeństwa informacji zgłaszanych przez Administratorów Merytorycznych SZBI, odpowiednio w Centrali Spółki / Spółce oraz w Oddziałach Spółki.

2.8 Pracownicy Spółki zobowiązani są do stosowania i przestrzegania wymagań Procedury w ramach realizowanych obowiązków służbowych i zadań dodatkowych. Konsekwencje nieprzestrzegania zasad i standardów ochrony informacji zostały określone w Regulaminie pracy Centrali / Oddziału Spółki.

2.9 Na czas nieobecności osoby pełniącej rolę w ZSZ obowiązki i uprawnienia przejmuje jej zastępca, zgodnie z „Wykazem podstawowych ról ZSZ", dostępnym na witrynie „Zarządzanie Procesami i Systemami" (https://giek.gkpge.pl/ZPiS), w bibliotece „Model ZSZ i wykaz ról".

2.10 Szczegółowe obowiązki i uprawnienia osób pełniących role / podmiotów, o których mowa w pkt 2.1-2.9, oraz pozostałych uczestników procesu określono w dalszej części Procedury i formularzach związanych z procesem.

III DOKUMENTY POWIĄZANE*

3.1 *Uchwała Nr 485/VI/2014 Zarządu PGE GiEK S.A. z dnia 29.05.2014 r.*

3.2 *Norma PN-ISO/IEC 27001 – Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.*

3.3 *Zarządzenie nr 17/2012 z dnia 30.04.2012 r., Regulamin ochrony tajemnic Spółki w Centrali PGE GiEK S.A.*

3.4 *Zarządzenie nr 34/2014 z dnia 13.05.2014 r., Instrukcja bezpieczeństwa fizycznego i środowiskowego w PGE GiEK S.A.*

3.5 *REGL 10000/A – Regulamin organizacyjny PGE Górnictwo i Energetyka Konwencjonalna S.A.*

3.6 *PROC 10007/B Procedura – Opracowywanie Planów zapewnienia ciągłości działania w PGE GiEK S.A.*

3.7 *PROC 10029/A Procedura – Zarządzanie kapitałem ludzkim w Centrali PGE GiEK S.A. w kontekście wymagań Zintegrowanego Systemu Zarządzania.*

3.8 *PROC 10032/C Procedura – Zakupy w PGE GiEK S.A.*

3.9 *PROC 10038/A Procedura – Administrowanie zasobami teleinformatycznymi (ICT) w PGE GiEK S.A.*

3.10 *PROC 10039/A Procedura – Korzystanie z zasobów teleinformatycznych (ICT) w PGE GiEK S.A.*

3.11 *PROC 10041/A Procedura – Zarządzanie zasobami automatyki przemysłowej (OT) w PGE GiEK S.A.*

3.12 *PROC 10049/A Procedura – Wypełnianie obowiązków wynikających z rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1227/2011 z dnia 25.10.2011 r. w sprawie integralności i przejrzystości hurtowego rynku energii.*

3.13 *PROC 10057/A Procedura – Realizacja wsparcia prawnego w PGE GiEK S.A.*

3.14 *PROC 10058/A Procedura – Identyfikacja i spełnianie wymagań prawnych i innych w PGE GiEK S.A.*

3.15 *PROC 10064/A Procedura – Ochrona danych osobowych w PGE GiEK S.A.*

3.16 *PROC 10068/B Procedura – Model Zintegrowanego Systemu Zarządzania w PGE GiEK S.A.*

3.17 *PROC 10069/A Procedura – Przegląd procesów i systemów zarządzania w PGE GiEK S.A.*

3.18 *PROC 10070/A Procedura – Poprawa funkcjonowania procesów i systemów zarządzania w PGE GiEK S.A.*

3.19 *PROC 10075/A Procedura – Szacowanie i postępowanie z ryzykiem w bezpieczeństwie informacji w PGE GiEK S.A.*

3.20 *INST 10020/A Instrukcja – Zasady ochrony przepływu informacji poufnych związanych z transakcjami giełdowymi w Centrali PGE GIEK S.A.*

3.21 *INST 10021/A Instrukcja – Zarządzanie systemami informatycznymi służącymi do przetwarzania danych osobowych w PGE GiEK S.A.*

3.22 *INST 10024/A Instrukcja – Zasady ruchu osobowego i pojazdów na terenie siedziby PGE GiEK S.A.*
W przypadku Oddziałów Spółki lokalne wewnętrzne regulacje dotyczące ruchu osobowego i pojazdów.

3.23 *Pismo okólne nr 3/2017 Prezesa Zarządu PGE GiEK S.A. z dnia 21.03.2017 r. w sprawie realizacji w PGE GiEK S.A. obowiązków wynikających z Procedury Ogólnej dotyczącej realizacji giełdowych obowiązków informacyjnych PGE Polska Grupa Energetyczna S.A.*

3.24 *Zarządzenie nr 10/2013 z dnia 14.05.2013 r., Instrukcja dostępu do pomieszczeń oraz postępowania z kluczami w budynku siedziby PGE GiEK S.A.*
W przypadku Oddziałów Spółki lokalne wewnętrzne regulacje dotyczące gospodarki kluczami.

3.25 *Zarządzenie nr 28/2014 z dnia 25.04.2014 r., Regulamin Pracy Centrali PGE Górnictwo i Energetyka Konwencjonalna Spółka Akcyjna (z późniejszymi zmianami).*
W przypadku Oddziałów Spółki lokalne Regulaminy Pracy.

3.26 *Zarządzenie nr 48/2014 z dnia 10.07.2014 r., Instrukcja zgłaszania incydentów do Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL w PGE GiEK S.A.*

** Stan dokumentów powiązanych jest aktualny na dzień publikacji Procedury. Przed użyciem dokumentu powiązanego należy sprawdzić aktualność stosowanego dokumentu.*

IV ZAŁĄCZNIKI

4.1 Zał.1 Klasyfikacja informacji oraz zasady ich przetwarzania w PGE GiEK S.A.

4.2 Zał.2 Zasady zgłaszania i obsługi zdarzeń związanych z bezpieczeństwem informacji oraz podatności zasobów i zabezpieczeń w PGE GiEK S.A.

4.3 Zał.3 Plan ciągłości działania zasobu – wzór.

4.4 Zał.4 Rodzaje testów Planów ciągłości działania zasobów w PGE GiEK S.A.

4.5 Zał.5 Deklaracja stosowania zabezpieczeń w PGE GiEK S.A. – wzór.

4.6 Zał.6 Zasady opracowywania Deklaracji stosowania zabezpieczeń i oceny ich skuteczności w PGE GiEK S.A.

V SKRÓTY I DEFINICJE

AM; Centrala; Deklaracja; Forum BI; JO; KO; Lokalne Forum BI; Oddział; PCDZ; Plan; Procedura; PZCD; Spółka; SZBI; ZPiS; ZSZ;

Skróty użyte na potrzeby niniejszego dokumentu:

AM	–	Administrator Merytoryczny / Administratorzy Merytoryczni,
Centrala	–	PGE GiEK S.A., z wyłączeniem Oddziałów,
Deklaracja	–	Deklaracja stosowania zabezpieczeń w PGE GiEK S.A.,
Forum BI	–	Forum Bezpieczeństwa Informacji,
JO	–	jednostka organizacyjna (Centrala / Oddział),
KO	–	komórka organizacyjna,
Lokalne Forum BI	–	Lokalne Forum Bezpieczeństwa Informacji,
Oddział	–	wyodrębniona jednostka organizacyjna PGE GiEK S.A.,
PCDZ, Plan	–	Plan ciągłości działania zasobu,
Procedura	–	PROC 10072/B Procedura – Organizacja i zarządzanie bezpieczeństwem informacji w PGE GiEK S.A.,
PZCD	–	Plan zapewnienia ciągłości działania,
Spółka	–	PGE GiEK S.A., obejmująca Centralę wraz z Oddziałami,
SZBI	–	System Zarządzania Bezpieczeństwem Informacji,
ZPiS	–	Zarządzanie Procesami i Systemami,
ZSZ	–	Zintegrowany System Zarządzania.

Definicje pojęć użyte na potrzeby niniejszego dokumentu:

5.1 Podstawowe definicje dotyczące procesów i systemów zarządzania, znajdują się w „Słowniku Zintegrowanego Systemu Zarządzania" dostępnym w portalu Spółki, na witrynie „Zarządzanie Procesami i Systemami" (https://giek.gkpge.pl/ZPiS), w bibliotece „Słownik ZSZ".

VI REALIZACJA

6.1 WPROWADZENIE

6.1.1 Informacje, ze względu na posiadaną wartość, powinny być odpowiednio chronione przed utratą dostępności, poufności i integralności na każdym etapie ich przetwarzania. Dostępność precyzyjnych i kompletnych informacji w wymaganym czasie jest niezbędna dla zachowania efektywności biznesowej. Skuteczna ochrona aktywów informacyjnych Spółki jest istotna dla osiągania wyznaczonych celów, zachowania zgodności z prawem oraz wizerunku. Bezpieczeństwo informacji wiąże się z nadzorowaniem głównych aktywów informacyjnych – informacji oraz zasobów wspierających ich przetwarzanie.

6.1.2 Informacje mogą występować w formie:

a. cyfrowej – np. pliki danych przechowywane na nośnikach elektronicznych lub optycznych,
b. materialnej – np. na papierze,
c. niematerialnej – w postaci wiedzy posiadanej przez pracowników.

6.1.3 Informacje mogą być przesyłane: za pomocą poczty lub kuriera, elektronicznie, bądź przekazywane w komunikacji werbalnej bezpośrednio lub telefonicznie, zawsze jednak potrzebują właściwej ochrony. Informacje są szczególnie silnie powiązane z technologią teleinformatyczną, która umożliwia tworzenie, przetwarzanie, przechowywanie, przesyłanie, ochronę i niszczenie informacji.

6.1.4 Organizacje wszystkich typów i wielkości zbierają, przetwarzają, przechowują i przesyłają bardzo duże ilości informacji. Informacje i procesy związane, systemy, sprzęt, sieci oraz personel są ważnymi zasobami służącymi osiągnięciu celów organizacji. Informacje posiadane i przetwarzane przez organizacje podlegają różnorodnym zagrożeniom np.: atakom komputerowym, kradzieży lub zagrożeniom z przyczyn naturalnych (powódź, ogień itp.) oraz podatnościom nieodłącznie związanym z ich wykorzystywaniem.

6.2 KONTEKST ORGANIZACJI

6.2.1 Nasze wartości: partnerstwo, rozwój i odpowiedzialność koncentrują się na zasadach związanych z postawą wobec Spółki, pracowników, prowadzonymi działaniami biznesowymi oraz utrzymywanymi relacjami zewnętrznymi. Wspieramy je przestrzegając zasad etycznych we wszystkich obszarach działalności Spółki.

6.2.2 Na środowisko wewnętrzne Spółki składają się: struktura organizacyjna, role, odpowiedzialność, obowiązki i uprawnienia oraz wzajemne relacje pracowników związane z pracą. Wymienione elementy środowiska pracy zostały opisane w Regulaminie organizacyjnym Spółki, Regulaminach funkcjonowania Oddziałów, Regulaminach pracy Oddziałów, Modelu ZSZ w Spółce oraz innych regulacjach wewnętrznych, wymienionych w rozdziale III.

6.2.3 PGE GiEK S.A. mając na uwadze skuteczność funkcjonowania SZBI, określiła istotne dla systemu strony zainteresowane oraz ich oczekiwania, potrzeby oraz wymagania w kontekście bezpieczeństwa informacji:

a. klienci – w zakresie: ochrony dokumentacji powierzonej przez klienta, danych osobowych i specyficznych wymagań klienta, zgodności pod względem prawnym, terminowości (ciągłości) dostaw wyrobów i usług oraz szybkiej reakcji na nieprawidłowości,
b. dostawcy – w zakresie: ochrony praw własności intelektualnej, danych osobowych i specyficznych wymagań umownych, równego traktowania, uczciwej konkurencji i przejrzystości działań,
c. organy władzy, ministerstwa, urzędy i instytucje: Państwowa Inspekcja Pracy, Rządowe Centrum Bezpieczeństwa, Agencja Bezpieczeństwa Wewnętrznego, Generalny Inspektor Ochrony Danych Osobowych, Urząd Marszałkowski, Urząd Skarbowy, Zakład Ubezpieczeń Społecznych, Giełda Papierów Wartościowych, Urząd Górniczy, Urząd Regulacji Energetyki, Urząd Komunikacji Elektronicznej, Główny Urząd Statystyczny – w zakresie: przestrzegania przepisów prawnych, szybkiej reakcji na działania nadzoru i zapytania,
d. Zarząd Spółki – w zakresie: ograniczania ryzyka związanego z przetwarzaniem informacji w PGE GiEK S.A., skutecznej ochrony aktywów informacyjnych i potrzeby zapewnienia ciągłości biznesowej, szybkiej reakcji na incydenty, odpowiedzialności społecznej, integralności oraz dostępności i poufności informacji, poprawy wizerunku Spółki,
e. pracownicy Spółki – w zakresie: skutecznej realizacji zadań mających wpływ na bezpieczeństwo informacji, wiarygodności i dostępności niezbędnych danych, zwiększania świadomości zagrożeń i podatności, którym podlegają informacje, podnoszenia swoich kompetencji,
f. media – w zakresie: szybkiej odpowiedzi na zapytania, łatwego dostępu do informacji.

6.2.4 Podstawowym celem Spółki w zakresie bezpieczeństwa informacji jest wdrożenie i realizowanie spójnych, skutecznych działań składających się na zarządzanie bezpieczeństwem informacji, opartych na uznanych w tym zakresie standardach i dobrych praktykach, z uwzględnieniem celów biznesowych i wymagań prawnych.

6.2.5 Potwierdzeniem zaangażowania w budowę oraz utrzymanie bezpieczeństwa informacji jest „Deklaracja Zarządu Spółki w sprawie polityki bezpieczeństwa informacji".

6.2.6 Ryzyka związane z bezpieczeństwem informacji oraz skuteczność zabezpieczeń zależą od zmieniających się warunków, w związku z tym Spółka na bieżąco:

a. identyfikuje pojawiające się zagrożenia i związane z nimi ryzyka,
b. dobiera, wdraża i doskonali zabezpieczenia odpowiednie do oszacowanego ryzyka,
c. monitoruje i ocenia skuteczność wdrożonych zabezpieczeń.

6.2.7 Wdrażanie odpowiednich zabezpieczeń i postępowanie z nieakceptowalnym ryzykiem zapewniają skuteczną ochronę aktywów informacyjnych.

6.3 ORGANIZACJA I KOORDYNACJA DZIAŁAŃ W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI

6.3.1 Dla potrzeb rozwiązywania szczególnie istotnych lub spornych spraw w zakresie bezpieczeństwa informacji w Spółce powołano Forum Bezpieczeństwa Informacji, które:

a. rekomenduje Zarządowi Spółki do zatwierdzenia kryteria akceptowalności ryzyka w bezpieczeństwie informacji oraz plany postępowania z ryzykiem w zakresie dotyczącym Spółki – ustalone w wyniku szacowania okresowego (pkt 3.19),
b. zatwierdza wykaz krytycznych zasobów informacyjnych Centrali,
c. ocenia zasoby krytyczne zidentyfikowane w Oddziałach,
d. dokonuje przeglądów incydentów związanych z bezpieczeństwem informacji o szczególnym znaczeniu dla Spółki (np. wymagających podjęcia kroków prawnych), w celu zredukowania prawdopodobieństwa ich wystąpienia lub skutków przyszłych zdarzeń.

6.3.2 W skład Forum Bezpieczeństwa Informacji wchodzą:

a. Przewodniczący Forum BI – Prezes Zarządu Spółki,
b. Zastępcy Przewodniczącego Forum BI:
   - Dyrektor Departamentu Bezpieczeństwa – Administrator Merytoryczny SZBI w Spółce w zakresie bezpieczeństwa fizycznego i środowiskowego lokalizacji, ochrony danych osobowych i tajemnic Spółki,
   - Dyrektor Departamentu Zarządzania i Organizacji – Pełnomocnik ds. ZSZ,
c. Członkowie:
   - Dyrektor Departamentu Zarządzania Systemami ICT,
   - Dyrektor Departamentu Zarządzania Majątkiem,
   - Kierownik Biura Zarządzania Systemowego i Organizacji w Departamencie Zarządzania i Organizacji – Administrator Merytoryczny SZBI w Spółce w zakresie szacowania i postępowania z ryzykiem oraz standardów opracowywania dokumentów systemu,
   - Kierownik Biura Utrzymania Infrastruktury ICT w Departamencie Zarządzania Systemami ICT – Administrator Merytoryczny SZBI w Spółce w zakresie teleinformatyki (ICT),
   - Kierownik Biura Strategii Zarządzania Majątkiem w Departamencie Zarządzania Majątkiem – Administrator Merytoryczny SZBI w Spółce w zakresie systemów OT,
   - Kierownik Biura Zarządzania Systemami Wsparcia Produkcji w Departamencie Zarządzania Systemami ICT,
   - Kierownik Biura Zarządzania Wytwarzaniem – Administrator Merytoryczny SZCB w Spółce w zakresie ciągłości działania elektrowni i elektrociepłowni,
   - Kierownik Biura Analiz i Monitorowania Wydobycia – Administrator Merytoryczny SZCB w Spółce w zakresie ciągłości działania kopalń,
   - Główny Specjalista ds. Strategii Zarządzania Majątkiem, Biuro Strategii Zarządzania Majątkiem,
   - Główny Specjalista – Koordynator ds. Zarządzania Procesami i Systemami, Biuro Zarządzania Systemowego i Organizacji w Departamencie Zarządzania i Organizacji,
   - Główny Specjalista ds. Zarządzania Ryzykiem, Biuro Zarządzania Systemowego i Organizacji w Departamencie Zarządzania i Organizacji,
   - Specjalista ds. Zarządzania Procesami i Systemami, Biuro Zarządzania Systemowego i Organizacji w Departamencie Zarządzania i Organizacji.

6.3.3 Posiedzenia Forum BI zwołuje Przewodniczący lub jego Zastępca na wniosek Administratora / Administratorów Merytorycznych SZBI w Spółce, sporządzany odpowiednio do potrzeb (pkt 6.3.1), z zastrzeżeniem pkt 6.3.9. Pozostali członkowie Forum BI mogą zgłaszać potrzebę zwołania posiedzenia do właściwego Administratora Merytorycznego SZBI w Spółce, informując o sprawie do rozstrzygnięcia.

6.3.4 W zależności od potrzeb (rodzaju i charakteru sprawy), na posiedzenia Forum BI mogą być zapraszani Członkowie Zarządu Spółki oraz pracownicy Spółki niebędący członkami Forum BI.

6.3.5 Dla potrzeb rozwiązywania szczególnie istotnych lub spornych spraw w zakresie bezpieczeństwa informacji powołano w Oddziałach Lokalne Forum Bezpieczeństwa Informacji. Lokalne Forum BI na wniosek Administratora / Administratorów Merytorycznych SZBI w Oddziale Spółki:

a. rekomenduje Dyrektorowi Oddziału do akceptacji plany postępowania z ryzykiem w Oddziale – ustalone w wyniku szacowania okresowego (pkt 3.19),
b. zatwierdza wykaz krytycznych zasobów informacyjnych Oddziału,
c. dokonuje przeglądów incydentów związanych z bezpieczeństwem informacji o szczególnym znaczeniu dla Oddziału (np. wymagających podjęcia kroków prawnych), w celu zredukowania prawdopodobieństwa ich wystąpienia lub skutków przyszłych zdarzeń.

6.3.6 W skład Lokalnego Forum BI wchodzą:

a. Przewodniczący Lokalnego Forum BI – Zastępca Dyrektora Oddziału,
b. Zastępca Przewodniczącego Lokalnego Forum BI – kierujący komórką właściwą ds. bezpieczeństwa lub pracownik na samodzielnym stanowisku właściwym ds. bezpieczeństwa w Oddziale – Administrator Merytoryczny SZBI w Oddziale Spółki w zakresie bezpieczeństwa fizycznego i środowiskowego lokalizacji, ochrony danych osobowych i tajemnic Spółki, pełniący jednocześnie rolę Koordynatora SZBI,
c. Członkowie:
   - Koordynator ZSZ,
   - Koordynator ICT – Administrator Merytoryczny SZBI w Oddziale w zakresie teleinformatyki (ICT)[1],
   - Koordynator OT – Administrator Merytoryczny SZBI w Oddziale w zakresie systemów OT[1],
   - Koordynator ds. Zarządzania Ryzykiem w Oddziale,
   - Główny Inżynier ds. Wytwarzania Energii – Administrator Merytoryczny SZCB w zakresie ciągłości działania (dotyczy elektrowni i elektrociepłowni),
   - Kierownik Centrum Kierowania Ruchem – Administrator Merytoryczny SZCB w Oddziale Spółki w zakresie ciągłości działania (dotyczy kopalni),
   - Główny Inżynier ds. Zarządzania Majątkiem (dotyczy elektrowni i elektrociepłowni),
   - Naczelny Inżynier Energomechaniczny (dotyczy kopalni),
   - Główny Inżynier ds. Automatyki i Elektryki,
   - kierujący komórką właściwą ds. nadzoru nad automatyką przemysłową w Oddziale,
   - kierujący komórką właściwą ds. nadzoru elektrycznego w Oddziale.

6.3.7 Posiedzenia Lokalnego Forum BI zwołuje Przewodniczący lub jego Zastępca na wniosek Administratora / Administratorów Merytorycznych SZBI w Oddziale Spółki, z zastrzeżeniem pkt 6.3.9. Pozostali Członkowie Lokalnego Forum BI mogą zgłaszać potrzebę zwołania posiedzenia do właściwego Administratora Merytorycznego SZBI w Oddziale, informując o sprawie do rozstrzygnięcia.

6.3.8 W zależności od potrzeb (rodzaju i charakteru sprawy), na posiedzenia Lokalnego Forum BI mogą być zapraszani pracownicy Oddziału, niebędący jego członkami, wskazani przez zwołującego.

6.3.9 Dla potrzeb realizacji procesu szacowania ryzyka posiedzenie:

a. Forum BI zwołuje z własnej inicjatywy Administrator Merytoryczny SZBI w Spółce w zakresie szacowania i postępowania z ryzykiem,
b. Lokalnego Forum BI zwołuje z własnej inicjatywy Koordynator SZBI.

6.4 KLASYFIKACJA INFORMACJI

6.4.1 W celu zapewnienia odpowiedniego poziomu ochrony informacji przetwarzanych w Spółce, zgodnego z ich wagą i wartością biznesową dla Spółki, a w konsekwencji zapobieżenia wystąpieniu lub zredukowania niepożądanych zdarzeń, konieczne jest sklasyfikowanie (uporządkowanie) tych informacji i określenie sposobów postępowania z nimi w zależności od przypisanego im poziomu ochrony.

6.4.2 Przeprowadzono inwentaryzację grup informacji (aktywów głównych) przetwarzanych w Spółce, wyznaczono poziomy ochrony informacji oraz ustalono zasady ich przetwarzania. Istotne kwestie związane z tymi zagadnieniami oraz wytyczne dotyczące klasyfikacji informacji określono w *Zał.1*.

[1] Z wyłączeniem sytuacji, gdy na podstawie pisemnej decyzji Dyrektora Oddziału rolę AM SZBI w Oddziale Spółki w zakresie teleinformatyki (ICT) lub w zakresie systemów OT pełni AM SZBI w Oddziale Spółki w zakresie bezpieczeństwa fizycznego i środowiskowego lokalizacji, ochrony danych osobowych i tajemnic Spółki (Koordynator SZBI).

6.5 ZARZĄDZANIE ZASOBAMI WSPIERAJĄCYMI

6.5.1 W celu zapewnienia skutecznej ochrony zasobów wspierających przetwarzanie informacji w Spółce, wszystkie zasoby należy zidentyfikować (zinwentaryzować), z uwzględnieniem ich znaczenia dla Spółki (wartości biznesowej), i utrzymywać ich spis.

6.5.2 Wszystkie zinwentaryzowane wspierające zasoby informacyjne posiadają określonych:

a. Właścicieli Zasobów, którzy odpowiedzialni są m.in. za właściwe użytkowanie i ochronę przypisanych zasobów, zgodnie z określonymi standardami, oraz za przyznawanie / odbieranie uprawnień dostępu do tych zasobów – role przypisane do osób na stanowiskach kierowniczych,

b. Administratorów Merytorycznych SZBI, którzy odpowiadają za weryfikację poprawności identyfikacji zasobów wspierających, w tym zasobów krytycznych (pkt 3.19).

6.5.3 Wykazy zasobów wspierających, zinwentaryzowanych w Centrali i Oddziałach, dostępne są w przeznaczonych dla JO folderach, w portalu Spółki na witrynie ZPiS, w bibliotece SZBI.

6.5.4 Sposób i tryb postępowania obowiązujący podczas inwentaryzacji zasobów oraz zasady identyfikacji zasobów krytycznych określono w odrębnej regulacji wewnętrznej dotyczącej szacowania i postępowania z ryzykiem w bezpieczeństwie informacji w Spółce (pkt 3.19).

6.5.5 Główne zasady w zakresie administrowania i korzystania przez pracowników z zasobów teleinformatycznych oraz zarządzania systemami OT w Spółce zostały określone w odrębnych regulacjach wewnętrznych dotyczących:

a. administrowania zasobami teleinformatycznymi (ICT) (pkt 3.09),

b. korzystania z zasobów teleinformatycznych (ICT) (pkt 3.10),

c. zarządzania zasobami automatyki przemysłowej (OT) (pkt 3.11).

Ww. regulacje określają m.in. zasady w zakresie: zarządzania hasłami, logowania się i wylogowywania z sesji, nadzorowania nośników danych, korzystania z sieci Internet, poczty elektronicznej i telefonów oraz tworzenia kopii zapasowych.

6.5.6 W przypadku wystąpienia zdarzeń lub stwierdzenia istotnych podatności związanych z bezpieczeństwem zasobów wspierających, w tym związanych z usługami dotyczącymi obszarów ICT i OT, należy postępować zgodnie z zasadami ustalonymi w *Zał.2*.

6.6 PLANY CIĄGŁOŚCI DZIAŁANIA ZASOBÓW (PCDZ)

6.6.1 OPRACOWYWANIE PLANÓW CIĄGŁOŚCI DZIAŁANIA ZASOBÓW

6.6.1.1 Dla wspierających zasobów informacyjnych, uznanych za krytyczne, opracowywane są i aktualizowane Plany ciągłości działania zasobów (PCDZ, Plan), zgodnie z regulacją wewnętrzną dotyczącą szacowania i postępowania z ryzykiem w bezpieczeństwie informacji w PGE GiEK S.A. (pkt 3.19). W przypadku, gdy zasób krytyczny jest udostępniany przez podmiot zewnętrzny (np. CUW ICT) należy wówczas uwzględnić konieczność opracowywania dla niego PCDZ i testowania tego Planu w ramach umowy SLA.

6.6.1.2 Wzór PCDZ został określony w *Zał.3*.

6.6.1.3 Za opracowanie i aktualizację Planów dla zidentyfikowanych zasobów krytycznych w Spółce odpowiadają Właściciele Zasobów we współpracy z kierującymi komórkami organizacyjnymi uczestniczącymi w realizacji Planów (uczestnikami Planu).

6.6.1.4 Aktualizacji PCDZ należy dokonywać każdorazowo w przypadku zaistnienia / ustalenia zmiany wpływającej na Plan, np. w związku z uruchomieniem Planu lub przeprowadzeniem jego testu.

6.6.1.5 Opracowując PCDZ należy koniecznie uwzględnić w nim środki (organizacyjne, sprzętowe i materiałowe) niezbędne do jego realizacji oraz harmonogram dotyczący testowania Planu i szkoleń dla pracowników uczestniczących w działaniach określonych w Planie (w szczególności pod względem pełnionych przez nich ról i przypisanej odpowiedzialności).

6.6.1.6 Budując „Harmonogram testowania Planu ciągłości działania zasobu" należy:

a. przyjąć założenie zmiany lub progresywnego zwiększania zakresu ćwiczeń,

b. określić cele,

c. opracować realistyczne scenariusze materializacji zagrożeń,

d. ustalić jednoznaczne kryteria oceny.

6.6.1.7 PCDZ, po uzyskaniu akceptacji osób określonych we wzorze Planu (*Zał.3*), zatwierdza Członek Zarządu Spółki / Dyrektor w Oddziale właściwy ze względu na podległość służbową Właściciela Zasobu. Oryginał zatwierdzonego Planu przechowuje Właściciel Zasobu, dla którego Plan został opracowany.

6.6.1.8 Właściciel Zasobu odpowiedzialny jest za oszacowanie i zabezpieczenie w budżecie Centrali / Oddziału środków finansowych niezbędnych dla potrzeb utrzymania zasobu i testowania PCDZ.

6.6.1.9 Właściciel Zasobu zobowiązany jest udostępnić PCDZ właściwemu Administratorowi Merytorycznemu SZBI w Spółce / Oddziale Spółki (Właściciel Ryzyka dot. Zasobu) oraz wszystkim kierującym komórkami organizacyjnymi Spółki biorącymi udział w zadaniach określonych w Planie.

6.6.1.10 Zatwierdzone Plany, Administratorzy Merytoryczni SZBI (każdy w swoim zakresie działania) umieszczają w odpowiednim dla danej JO folderze, w portalu Spółki na witrynie ZPiS, w bibliotece SZBI. Wszystkie wersje PCDZ należy nadzorować i archiwizować zgodnie z regulacjami wewnętrznymi obowiązującymi w tym zakresie, a dostęp do nich powinni posiadać tylko uprawnieni pracownicy.

6.6.1.11 Kierujący komórkami organizacyjnymi Spółki uczestniczącymi w realizacji PCDZ, zobowiązani są przeszkolić podległych pracowników celem zapoznania ich z rolami i odpowiedzialnością w zakresie przypisanych im zadań (pkt 6.6.1.5).

6.6.2 TESTOWANIE PLANÓW CIĄGŁOŚCI DZIAŁANIA ZASOBU

6.6.2.1 Właściciel Zasobu we współpracy z AM SZBI właściwym dla zasobu (Właściciel Ryzyka dotyczącego Zasobu) i, w zależności od potrzeb, z innymi realizatorami działań określonych w Planie, zobowiązani są (zgodnie z pkt 6.6.2.4) testować i modyfikować PCDZ tak, aby zapewnić jego aktualność i skuteczność.

6.6.2.2 Testy PCDZ przeprowadza się w celu sprawdzenia:

a. zdolności Centrali / Oddziału do kontynuacji i odtworzenia sprawności działania krytycznego zasobu,
b. poprawności i skuteczności przyjętych rozwiązań,
c. czy Plan zadziała w rzeczywistej sytuacji oraz przebieg ustalonych działań jest zgodny z założeniami i wymogami czasowymi,
d. świadomości pracowników w zakresie ich ról i odpowiedzialności w ramach Planu.

6.6.2.3 Przeprowadzając testy należy się kierować zasadą maksymalnego ograniczania ryzyka utraty zasobów w trakcie testów, przy jednoczesnym zapewnieniu wysokiego poziomu zdolności odtworzenia działania zasobu.

6.6.2.4 Testy PCDZ należy przeprowadzać:

a. na bieżąco – każdorazowo po istotnej zmianie Planu (testowanie wybranych aspektów Planu) oraz
b. okresowo – tak, aby w cyklu 3-letnim przetestować cały Plan (licząc od daty pierwszego wydania).

Rodzaje testów dla potrzeb oceny skuteczności PCDZ oraz zakres i sposób ich realizacji określono w *Zał.4*.

6.6.2.5 Przeprowadzone testy muszą być udokumentowane raportem podsumowującym wyniki oraz rekomendującym określone działania doskonalące Plan. Raport z testu zatwierdzany jest analogicznie jak PCDZ (pkt 6.6.1.7).

6.7 SZACOWANIE RYZYKA I POSTĘPOWANIE Z RYZYKIEM

6.7.1 Szacowanie ryzyka w bezpieczeństwie informacji oraz postępowanie z ryzykiem w Spółce należy przeprowadzać zgodnie z metodyką określoną w odrębnej regulacji wewnętrznej dotyczącej szacowania i postępowania z ryzykiem w bezpieczeństwie informacji w Spółce (pkt 3.19).

6.7.2 Zasady określone w regulacji, o której mowa powyżej, systematycznie stosowane prowadzą do stanu, w którym ryzyko nie przekracza wielkości przyjętych za dopuszczalne w kontekście bezpieczeństwa informacji, a Zarząd Spółki otrzymuje cyklicznie informacje o występujących rodzajach ryzyka i ich wielkościach.

6.7.3 Za identyfikację ryzyka związanego z zasobami, jego analizę i ocenę oraz opracowanie i wdrożenie „Planów postępowania z ryzykiem w bezpieczeństwie informacji" odpowiadają Właściciele Zasobów i Administratorzy Merytoryczni SZBI w Spółce / Oddziale Spółki, każdy w swoim zakresie działania, we współpracy z użytkownikami zasobów (kierującymi komórkami organizacyjnymi, których dane ryzyko dotyczy).

6.7.4 Zasady dotyczące szacowania ryzyka oraz postępowania z ryzykiem w zakresie zdolności Spółki do kontynuowania działalności biznesowej określono w odrębnej regulacji wewnętrznej dotyczącej opracowywania Planów zapewnienia ciągłości działania (pkt 3.6).

6.8 ZABEZPIECZENIA I CELE ICH STOSOWANIA

6.8.1 Wykazy niezbędnych zabezpieczeń stosowanych w Spółce dla wszystkich obszarów bezpieczeństwa informacji (wg Załącznika A do normy PN-ISO IEC 27001) przedstawiono w odrębnych dla Centrali oraz Oddziałów „Deklaracjach stosowania zabezpieczeń w PGE GiEK S.A.", których wzór stanowi *Zał.5*.

6.8.2 Aktualne Deklaracje dostępne są dla uprawnionych pracowników w intranecie Spółki na witrynie ZPiS (https://giek.gkpge.pl/ZPiS), w bibliotece „System Zarządzania Bezpieczeństwem Informacji".

6.8.3 W celu weryfikacji zgodności zabezpieczeń z wymaganiami bezpieczeństwa (celami stosowania zabezpieczeń) kierujący komórkami organizacyjnymi odpowiedzialni za ocenę danego zbioru / podzbioru zabezpieczeń (*Zał.5*) zobowiązani są wykonywać okresowo pomiary skuteczności tych zabezpieczeń, a ich wyniki dokumentować w formularzu Deklaracji, w części dot. oceny skuteczności zabezpieczeń. Za nadzór merytoryczny nad Deklaracją odpowiedzialni są Administratorzy Merytoryczni SZBI w Spółce / Oddziale Spółki – każdy w swoim zakresie działania.

6.8.4 Nadzór funkcjonalny (w zakresie spójności i kompletności opracowania) nad Deklaracją sprawuje:

a. w Centrali – Administrator Funkcjonalny ZSZ (Zastępca Pełnomocnika ds. ZSZ),
b. w Oddziale – Koordynator SZBI (Administrator Merytoryczny SZBI w zakresie bezpieczeństwa fizycznego i środowiskowego lokalizacji, ochrony danych osobowych i tajemnic Spółki).

6.8.5 Deklarację dla Centrali Spółki zatwierdza Prezes Zarządu Spółki, a dla Oddziału – Dyrektor Oddziału.

6.8.6 Szczegółowe wytyczne dotyczące opracowywania, aktualizacji i zatwierdzania „Deklaracji stosowania zabezpieczeń w PGE GiEK S.A." przedstawiono w *Zał.6*.

6.9 POZOSTAŁE OBSZARY OBJĘTE SZBI

6.9.1 Zagadnienia dotyczące: utrzymania pełnej i nieniekształconej informacji oraz jej dostępności wyłącznie dla uprawnionych m.in. w związku z realizacją scenariuszy awaryjnych lub planów doraźnych w ramach Systemu Zarządzania Ciągłością Biznesową objęte są również SZBI.

6.9.2 Zasady i tryb postępowania dotyczące stosowanych w Spółce technologii, lokalizacji i organizacji zasobów ICT oraz OT zostały określone w odrębnych wewnętrznych regulacjach dotyczących odpowiednio zasad korzystania i administrowania zasobami teleinformatycznymi (ICT) (pkt 3.9 i 3.10) oraz zasad zarządzania systemami OT (pkt 3.11).

6.9.3 Zasady i tryb postępowania dotyczące bezpieczeństwa fizycznego i środowiskowego zostały określone w odrębnych dla Centrali i Oddziałów uregulowaniach dotyczących odpowiednio: bezpieczeństwa fizycznego i środowiskowego, dostępu do pomieszczeń i postępowania z kluczami oraz ruchu osobowego i pojazdów na terenie Spółki.

6.10 UWARUNKOWANIA PRAWNE I NORMATYWNE

6.10.1 Zbiór wymagań prawnych obowiązujących w Rzeczypospolitej Polskiej stanowi ważny czynnik wpływający na określenie wymagań bezpieczeństwa informacji w Spółce. Poza zbiorem przepisów prawa, istotnymi źródłami wytycznych i zaleceń w obszarze zarządzania bezpieczeństwem informacji są normy oraz dobre praktyki uznane w tym zakresie.

6.10.2 Kierujący komórkami organizacyjnymi w Spółce, uczestniczący w realizacji wyznaczonych celów w obszarze bezpieczeństwa informacji, odpowiedzialni są za przegląd wymagań prawnych i wymagań wynikających z podpisanych zobowiązań oraz dostosowywanie swoich działań do tych wymagań. Szczegółowe zasady postępowania w tym zakresie zostały określone w odrębnych regulacjach wewnętrznych dotyczących identyfikacji i spełnienia wymagań prawnych i innych w PGE GiEK S.A. (pkt 3.14) oraz realizacji wsparcia prawnego w PGE GiEK S.A. (pkt 3.13).

6.10.3 Lista podstawowych uwarunkowań prawnych i normatywnych:

a. ustawa Prawo geologiczne i górnicze,
b. ustawa Prawo energetyczne,
c. ustawa Prawo telekomunikacyjne,
d. ustawa Kodeks spółek handlowych,
e. ustawa Kodeks pracy,
f. ustawa Kodeks karny,
g. ustawa o dostępie do informacji publicznej,
h. ustawa o ochronie osób i mienia,
i. ustawa o ochronie danych osobowych,
j. ustawa o ochronie informacji niejawnych,
k. ustawa o prawie autorskim i prawach pokrewnych,
l. ustawa o zwalczaniu nieuczciwej konkurencji,
m. ustawa o rachunkowości,
n. ustawa o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych,
o. ustawa o nadzorze nad rynkiem kapitałowym,
p. ustawa o obrocie instrumentami finansowymi,
q. ustawa o Krajowym Rejestrze Sądowym,

r. norma PN-ISO/IEC 27001,
s. norma PN-EN ISO 9001,
t. norma PN-EN ISO 14001,
u. norma PN-N 18001.

6.11 POSTANOWIENIA KOŃCOWE

6.11.1 Oświadczenia o zachowaniu poufności, złożone przez pracowników Spółki w oparciu o poprzednią wersję Procedury (PROC 10072/A), należy, bez zbędnej zwłoki, wymienić na oświadczenia zgodne z aktualnym wzorem (*Zał.3.1* do „Klasyfikacji informacji oraz zasad ich przetwarzania w PGE GiEK S.A.”). Dotychczasowe oświadczenie złożone przez pracownika obowiązuje do dnia jego wymiany.

6.11.2 Nie istnieje konieczność wymiany oświadczeń o zachowaniu poufności, złożonych przez osoby niebędące pracownikami Spółki w oparciu o poprzednią wersję Procedury (PROC 10072/A).

6.11.3 Wymienić należy również dotychczasowe „Wykazy punktów kontaktowych” na zgodne z aktualnym, uniwersalnym wzorem (Zał.2 do „Zasad zgłaszania i obsługi zdarzeń związanych z bezpieczeństwem informacji oraz podatności zasobów i zabezpieczeń w PGE GiEK S.A.”), po usunięciu zapisów niedotyczących JO.

6.11.4 Jeżeli inne funkcjonujące w Spółce regulacje wewnętrzne dotyczące bezpieczeństwa informacji zawierają zasady lub wymagania ustalające w pewnych obszarach wyższy poziom ochrony, niż określony w *Zał.1*, to wymagania te powinny być stosowane.

6.11.5 Do aktualizacji *Zał.1÷6* upoważniony jest Dyrektor Departamentu Zarządzania i Organizacji bez konieczności ich wprowadzenia dokumentem systemu zarządzania. Biuro Zarządzania Systemowego i Organizacji informuje pocztą elektroniczną o zaktualizowanych załącznikach, które będą dostępne również na witrynie „Zarządzanie Procesami i Systemami” (https://giek.gkpge.pl/ZPiS), w bibliotece „Formularze”.

KLASYFIKACJA INFORMACJI ORAZ ZASADY ICH PRZETWARZANIA W PGE GiEK S.A.

1. WPROWADZENIE

1.1. Celem klasyfikacji informacji jest zapewnienie informacjom przetwarzanym w PGE GiEK S.A. odpowiedniego poziomu ochrony, zgodnego z ich wagą dla Spółki, oraz zapobieżenie wystąpieniu niepożądanych zdarzeń związanych z bezpieczeństwem informacji poprzez określenie zasad ich oznaczania i przetwarzania.

1.2. Wszystkie informacje (główne aktywa informacyjne) przetwarzane w Spółce zostały sklasyfikowane (uporządkowane i pogrupowane), zgodnie z wytycznymi określonymi w „Zasadach klasyfikacji informacji w PGE GiEK S.A." stanowiącymi *Zał.1* do „Klasyfikacji informacji oraz zasad ich przetwarzania w PGE GiEK S.A.".

1.3. Zgodnie z wytycznymi określonymi w „Zasadach klasyfikacji informacji w PGE GiEK S.A.", w Spółce ustala się:
   a. cztery grupy informacji (G1÷G4) – Tabela 1,
   b. cztery poziomy ochrony informacji – Tabela 2,
   c. zasady przetwarzania informacji dla każdego z poziomów ochrony – Tabele 3÷6,
   d. ogólne zasady czystego biurka i ekranu – „Zasady czystego biurka i ekranu w PGE GiEK S.A." stanowiące *Zał.2* do „Klasyfikacji informacji oraz zasad ich przetwarzania w PGE GiEK S.A.".

1.4. Zasady określone w Tabelach 3÷6 oraz w *Zał.2* stanowią minimalne wymagania bezpieczeństwa dla przetwarzania informacji i obowiązują wszystkich pracowników Spółki oraz strony zewnętrzne (np. wykonawców, kooperantów, dostawców usług, klientów, konsultantów, praktykantów), którzy uzyskali dostęp i korzystają z zasobów informacyjnych Spółki w oparciu o stosowne umowy.

1.5. Stosowanie zasad, o których mowa w Tabelach 3÷6 oraz w *Zał.2*, nie zwalnia żadnego pracownika z obowiązku przestrzegania wymagań wynikających z innych przepisów prawa, zawartych umów lub regulacji wewnętrznych (np. regulaminów, procedur, instrukcji czy poleceń).

2. KLASYFIKACJA INFORMACJI

Tabela 1. Klasyfikacja informacji przetwarzanych w PGE GiEK S.A.

Oznaczenie / Poziom ochrony	Grupa informacji	Rodzaje informacji
G1 I	**Informacje ogólnie dostępne wewnątrz i na zewnątrz Spółki**	1) Informacje / dane publikowane w prasie, Internecie, radiu, telewizji, KRS itp. oraz dane dotyczące Spółki, w tym: - materiały marketingowe i reklamowe, - korporacyjne informatory / publikacje, - cenniki ogólnie dostępne. 2) Inne informacje / dane ogólnie dostępne wewnątrz i na zewnątrz Spółki – zgodnie z wewnętrznymi regulacjami.
G2 II	**Informacje ogólnie dostępne wewnątrz Spółki**	Informacje / dane publikowane w intranecie, radiowęźle, w tym regulacje wewnętrzne i ich projekty – zgodnie z wewnętrznymi regulacjami.
G3 III	**Informacje o ograniczonym dostępie**	Pozostałe informacje / dane, nie ujęte w grupach G1, G2 i G4 – zgodnie z wewnętrznymi regulacjami.
G4 IV	**Informacje szczególnie chronione**	1) Tajemnice Spółki – zgodnie z regulacjami wewnętrznymi dotyczącymi tajemnic Spółki obowiązującymi w Centrali i Oddziałach oraz wykazami informacji, które mogą stanowić tajemnice Spółki, stanowiącymi załączniki do ww. regulacji. 2) Dane osobowe – zgodnie z regulacjami wewnętrznymi dot. bezpieczeństwa / ochrony danych osobowych obowiązującymi w Centrali i Oddziałach. 3) Dane wynikające z giełdowych obowiązków informacyjnych oraz dane dotyczące obrotu na giełdach towarowych, w tym informacje poufne związane z obrotem instrumentami finansowymi (w rozumieniu art. 154 ustawy o obrocie instrumentami finansowymi) oraz stanowiące tajemnicę zawodową (w rozumieniu art. 147 ww. ustawy) – do czasu ich upublicznienia – zgodnie z regulacjami wewnętrznymi dot.: • realizacji giełdowych obowiązków informacyjnych PGE GiEK S.A., • ochrony przepływu informacji poufnych związanych z transakcjami giełdowymi.

3. POZIOMY OCHRONY INFORMACJI

Tabela 2. Opis poziomów ochrony informacji przetwarzanych w PGE GiEK S.A.

Poziom ochrony	Nazwa poziomu ochrony
I	**Ogólnodostępne wewnątrz i na zewnątrz Spółki** Oznacza to, że informacje są ogólnodostępne wewnątrz i na zewnątrz Spółki; wymagają nadzoru w zakresie integralności i dostępności ze względu na wizerunek Spółki.
II	**Ogólnodostępne wewnątrz Spółki** Oznacza to, że informacje: są dostępne ogólnie wewnątrz Spółki dla wszystkich komórek org. i pracowników Spółki oraz dla uprawnionych pracowników stron zewnętrznych / praktykantów* związanych umowami (na czas i w zakresie niezbędnym do realizacji umowy) i instytucji / organów uprawnionych nadrzędnymi przepisami prawa. Informacje wymagają nadzoru; utrata atrybutów bezpieczeństwa (poufność, integralność, dostępność) może mieć lub ma nieznaczny wpływ na biznesowe działanie Spółki.
III	**Chronione, nadzorowane i kontrolowane w Spółce** Oznacza to, że informacje: są dostępne dla wybranych komórek org. i uprawnionych pracowników Spółki* oraz dla uprawnionych pracowników stron zewnętrznych / praktykantów* związanych umowami (na czas i w zakresie niezbędnym do realizacji umowy) i instytucji / organów uprawnionych nadrzędnymi przepisami prawa. Informacje wymagają stałego nadzoru; utrata atrybutów bezpieczeństwa (poufność, integralność, dostępność) może mieć lub ma poważny wpływ na biznesowe działanie Spółki.
IV	**Szczególnie chronione, nadzorowane i kontrolowane w Spółce** Oznacza to, że informacje dostępne są dla: - uprawnionych komórek org. / pracowników Spółki*, którzy dodatkowo posiadają odpowiednie upoważnienia do przetwarzania informacji wynikające z regulacji wewnętrznych dot.: bezpieczeństwa danych osobowych, ochrony tajemnic Spółki, realizacji giełdowych obowiązków informacyjnych, - instytucji / organów uprawnionych nadrzędnymi przepisami prawa i uprawnionych pracowników stron zewnętrznych / praktykantów* związanych umowami (na czas i w zakresie niezbędnym do realizacji umowy), którzy dodatkowo uzyskali odpowiednie upoważnienia do przetwarzania informacji wynikające z regulacji wewnętrznych dot.: bezpieczeństwa danych osobowych, ochrony tajemnic Spółki lub realizacji giełdowych obowiązków informacyjnych. Informacje wymagają szczególnego nadzoru; utrata atrybutów bezpieczeństwa (poufność, integralność, dostępność) może mieć lub ma kluczowy wpływ na biznesowe i strategiczne działanie Spółki.

* Uprawniony pracownik Spółki / pracownik strony zewnętrznej / praktykant – osoba, która złożyła „Oświadczenie o zachowaniu poufności" (pkt 4).

3.1. W przypadku stwierdzenia potrzeby dokonania zmian w istniejących grupach informacji lub zbiorach danych, kierujący komórką organizacyjną, który zidentyfikował taką potrzebę, zobowiązany jest przesłać wniosek (e-mail) z konkretnymi propozycjami zmian w klasyfikacji informacji do Administratora Funkcjonalnego ZSZ (Zastępcy Pełnomocnika ds. ZSZ).

4. OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI INFORMACJI

4.1. W celu zapobieżenia naruszeniu zasad bezpieczeństwa informacji obowiązujących w PGE GiEK S.A. oraz spełnienia wymagań, o których mowa w pkt 3, kierujący komórkami organizacyjnymi w Spółce, w przypadku, gdy podlegli pracownicy przetwarzają informacje objęte III i IV poziomem ochrony (grupy G3 i G4), zobowiązani są do odebrania od nich „Oświadczenia o zachowaniu poufności pracownika PGE Górnictwo i Energetyka Konwencjonalna Spółka Akcyjna", którego wzór stanowi *Zał.3.1* do „Klasyfikacji informacji i zasad ich przetwarzania" i jest dostępny na witrynie „Zarządzanie Procesami i Systemami" (ZPiS) (https://giek.gkpge.pl/ZPiS) w bibliotece „Formularze".

4.2. W sytuacji, gdy dostęp do aktywów informacyjnych Spółki objętych II i wyższym poziomem ochrony (grupy G2÷G4) uzyskują pracownicy strony zewnętrznej lub praktykanci, to kierujący komórką odpowiedzialną za nadzór nad realizacją umowy (Realizator Umowy) zobowiązany jest do odebrania od tych pracowników / praktykantów „Oświadczenia o zachowaniu poufności osoby niebędącej pracownikiem PGE Górnictwo i Energetyka Konwencjonalna Spółka Akcyjna", którego wzór stanowi *Zał.3.2* do „Klasyfikacji informacji i zasad ich przetwarzania w PGE GiEK S.A." i jest dostępny na witrynie ZPiS w bibliotece „Formularze".

4.3. Oświadczenia, o których mowa w pkt 4.1 i 4.2, należy przekazać stronom zainteresowanym, zgodnie z rozdzielnikami.

5. ZASADY PRZETWARZANIA INFORMACJI

5.1. W ramach każdego z poziomów ochrony zdefiniowano zasady postępowania z przypisanymi do nich informacjami (zbiorami danych) w odniesieniu do ich oznaczania, przechowywania, kopiowania, niszczenia oraz udostępniania wewnątrz i na zewnątrz Spółki. Zasady te przedstawiono w tabelach nr 3÷6, a ich stosowanie nie zwalnia z obowiązku spełnienia wymagań określonych w pkt 4.

5.2. Ogólne zasady związane z bezpieczeństwem informacji w zakresie: nieautoryzowanego dostępu, utraty, kradzieży lub uszkodzenia informacji w czasie i poza godzinami pracy określono w „Zasadach czystego biurka i ekranu w PGE GiEK S.A.", stanowiących *Zał.2* do „Klasyfikacji informacji i zasad ich przetwarzania w PGE GiEK S.A.".

Tabela 3. Zasady przetwarzania informacji przyporządkowanych do I poziomu ochrony

<table>
<tr><th>I
poziom ochrony</th><th colspan="2">Ogólnodostępne wewnątrz i na zewnątrz Spółki</th></tr>
<tr><th>Postać informacji</th><th>Papierowa</th><th>Elektroniczna</th></tr>
<tr><td>Oznaczanie</td><td rowspan="4">Brak szczególnych wymagań.</td><td rowspan="4">Brak szczególnych wymagań.</td></tr>
<tr><td>Przechowywanie</td></tr>
<tr><td>Kopiowanie</td></tr>
<tr><td>Niszczenie</td></tr>
<tr><td>Przekazywanie / udostępnianie wewnątrz Spółki</td><td rowspan="2">Wg opisu I poziomu ochrony informacji przetwarzanych w Spółce (pkt 3) oraz zgodnie z obowiązującymi regulacjami wewnętrznymi dotyczącymi komunikacji wewnętrznej i zewnętrznej.</td><td rowspan="2">Wg opisu I poziomu ochrony informacji przetwarzanych w Spółce (pkt 3) oraz zgodnie z obowiązującymi regulacjami wewnętrznymi dotyczącymi komunikacji wewnętrznej i zewnętrznej.</td></tr>
<tr><td>Przekazywanie / udostępnianie na zewnątrz Spółki</td></tr>
<tr><td>Wynoszenie informacji na zewnątrz Spółki</td><td>Brak szczególnych wymagań.</td><td>Brak szczególnych wymagań.</td></tr>
</table>

Uwaga. W przypadku, gdy ww. dokumenty nie regulują pewnych zagadnień, to za upoważnieniem / zgodą przełożonego lub Właściciela Zasobu.

Tabela 4. Zasady przetwarzania informacji przyporządkowanych do II poziomu ochrony

<table>
<tr><th>II
poziom ochrony</th><th colspan="2">Ogólnodostępne wewnątrz Spółki</th></tr>
<tr><th>Postać informacji</th><th>Papierowa</th><th>Elektroniczna</th></tr>
<tr><td>Oznaczanie</td><td>Zgodnie z instrukcją kancelaryjną
i standardem DSZ.</td><td>Zgodnie z instrukcją kancelaryjną
i standardem DSZ.</td></tr>
<tr><td>Przechowywanie</td><td>Zgodnie z instrukcją kancelaryjną i standardem DSZ oraz zasadami czystego biurka i ekranu.</td><td>Zgodnie z instrukcją kancelaryjną, standardem DSZ, zasadami czystego biurka i ekranu oraz regulacjami wewnętrznymi dotyczącymi korzystania / administrowania zasobami teleinformatycznymi (ICT).</td></tr>
<tr><td>Kopiowanie</td><td>Zgodnie z zasadami czystego biurka i ekranu.</td><td rowspan="2">Zgodnie z zasadami czystego biurka i ekranu oraz regulacjami wewnętrznymi dotyczącymi korzystania / administrowania zasobami teleinformatycznymi (ICT).</td></tr>
<tr><td>Niszczenie</td><td>W niszczarkach do dokumentów o poziomie bezpieczeństwa co najmniej „2” (wg normy DIN 32757 paski o szerokości mniejszej niż 6 mm lub całkowita powierzchnia ścinka mniejsza niż 800 mm^2)</td></tr>
<tr><td>Przekazywanie / udostępnianie wewnątrz Spółki</td><td rowspan="2">Zgodnie z regułami ustalonymi dla II poziomu ochrony informacji przetwarzanych w Spółce (pkt 3) oraz z zapewnieniem spełnienia wymagań bezpieczeństwa informacji obowiązujących w Spółce, w szczególności zasad określonych w regulacjach dotyczących:
- instrukcji kancelaryjnej i standardu DSZ,
- regulaminu organizacyjnego Spółki / funkcjonowania Oddziału,
- komunikacji wewnętrznej i zewnętrznej.</td><td rowspan="2">Zgodnie z regułami ustalonymi dla II poziomu ochrony informacji przetwarzanych w Spółce (pkt 3), z tym, że informacje w postaci elektronicznej można przekazywać jedynie na służbowych nośnikach informacji lub za pośrednictwem korporacyjnej poczty elektronicznej oraz z zapewnieniem spełnienia wymagań bezpieczeństwa informacji obowiązujących w Spółce, w szczególności zasad określonych w regulacjach dotyczących:
- instrukcji kancelaryjnej i standardu DSZ,
- regulaminu organizacyjnego Spółki / funkcjonowania Oddziału,
- korzystania / administrowania zasobami teleinformatycznymi (ICT),
- komunikacji wewnętrznej i zewnętrznej.</td></tr>
<tr><td>Przekazywanie / udostępnianie na zewnątrz Spółki</td></tr>
<tr><td>Wynoszenie informacji na zewnątrz Spółki</td><td>Informacje można wynosić na zewnątrz za zgodą / upoważnieniem przełożonego lub Właściciela Zasobu oraz zgodnie z regulacjami wewnętrznymi dotyczącymi:
- komunikacji wewnętrznej i zewnętrznej,
- bezpieczeństwa fizycznego i środowiskowego,
- zasad przebywania i poruszania się po terenie siedziby Spółki / Oddziału,
- wydawania przepustek.</td><td>Informacje można wynosić na zewnątrz za zgodą / upoważnieniem przełożonego lub Właściciela Zasobu, z tym, że wynoszenie informacji w postaci elektronicznej może się odbywać jedynie na służbowych nośnikach informacji i z zapewnieniem spełnienia wymagań bezpieczeństwa informacji obowiązujących w Spółce, w szczególności zasad określonych w regulacjach dotyczących:
- komunikacji wewnętrznej i zewnętrznej,
- bezpieczeństwa fizycznego i środowiskowego,
- zasad gospodarowania rzeczowymi składnikami majątku trwałego oraz wartościami niematerialnymi,
- zasad przebywania i poruszania się po terenie siedziby Spółki / Oddziału,
- wydawania przepustek.</td></tr>
</table>

Uwaga. W przypadku, gdy ww. dokumenty nie regulują pewnych zagadnień, to za upoważnieniem / zgodą przełożonego lub Właściciela Zasobu.

Tabela 5. Zasady przetwarzania informacji przyporządkowanych do III poziomu ochrony

III Poziom ochrony	Chronione, nadzorowane i kontrolowane w Spółce	
Postać informacji	**Papierowa**	**Elektroniczna**
Oznaczanie	Zgodnie z instrukcją kancelaryjną, standardem DSZ oraz innymi odrębnymi regulacjami dot. nadzoru nad dokumentami, np. nadzoru nad dokumentacją techniczną. W przypadku dokumentów nie objętych ww. regulacjami należy oznaczać je w sposób umożliwiający jednoznaczną identyfikację.	Zgodnie z instrukcją kancelaryjną, standardem DSZ oraz innymi odrębnymi regulacjami dot. nadzoru nad dokumentami, np. nadzoru nad dokumentacją techniczną. W przypadku dokumentów nie objętych ww. regulacjami należy oznaczać je w sposób umożliwiający jednoznaczną identyfikację.
Przechowywanie	W zamkniętych pomieszczeniach lub w meblach biurowych zamykanych na klucz, ewentualnie o wyższym stopniu zabezpieczenia. Po zakończeniu sprawy przekazanie do archiwum zakładowego lub przechowywanie w komórce organizacyjnej zgodnie z regulacją wewnętrzną dotyczącą instrukcji kancelaryjnej.	Zgodnie z zasadami czystego biurka i ekranu oraz regulacjami wewnętrznymi dot.: - korzystania / administrowania zasobami teleinformatycznymi (ICT), - zarządzania zasobami automatyki przemysłowej (OT). W przypadku, gdy ww. regulacje nie obejmują swoim zakresem pewnych zagadnień należy: • nośniki, na których zapisane zostały dane/ kopie zapasowe przechowywać w miejscu zabezpieczonym przed dostępem osób trzecich oraz w sposób uniemożliwiający jednoczesne zniszczenie kopii roboczych i zapasowych, • pozostałe nośniki należy przechowywać w zamkniętych pomieszczeniach lub w zamykanych meblach biurowych, bądź o wyższym stopniu zabezpieczenia.
Kopiowanie	Zgodnie z zasadami czystego biurka i ekranu oraz regulacjami wewnętrznymi dot.: - prowadzenia postępowań zakupowych i zawierania umów, - zamawiania, weryfikacji, oceny i zatwierdzania dokumentacji projektowej, - gospodarowania składnikami majątku trwałego oraz wartości niematerialnych i prawnych, a także rodzaju i obiegu dokumentów związanych z ich ewidencją.	Zgodnie z zasadami czystego biurka i ekranu oraz regulacjami wewnętrznymi dot.: - korzystania / administrowania zasobami teleinformatycznymi (ICT), - zarządzania zasobami automatyki przemysłowej (OT).
Niszczenie	Za upoważnieniem / zgodą przełożonego lub Właściciela Zasobu: - w niszczarkach do dokumentów o poziomie bezpieczeństwa co najmniej „2” (wg normy DIN 32757 paski o szerokości mniejszej niż 6 mm lub całkowita powierzchnia ścinka mniejsza niż 800 mm^2), bądź - poprzez firmę utylizacyjną i wrzucenie dokumentów do pojemników z dedykowanymi koszami wrzutowymi.	Za upoważnieniem / zgodą przełożonego lub Właściciela Zasobu, z zastrzeżeniem, że w przypadku nośników jednokrotnego zapisu należy je niszczyć w sposób uniemożliwiający odtworzenie zapisanych danych.

Przekazywanie / udostępnianie wewnątrz Spółki	Zgodnie z regułami ustalonymi dla III poziomu ochrony informacji przetwarzanych w Spółce (pkt 3) oraz z zapewnieniem spełnienia wymagań bezpieczeństwa informacji obowiązujących w Spółce, w szczególności zasad określonych w regulacjach dotyczących: - regulaminu organizacyjnego Spółki / funkcjonowania Oddziału, - prowadzenia postępowań zakupowych i zawierania umów, - nadzoru nad dokumentacją finansową i techniczną, - udostępniania zasobów informacyjnych na potrzeby realizacji prac dyplomowych i opracowań naukowych, - trybu zgłaszania i ewidencjonowania powstałych na terenie Spółki awarii i innych nadzwyczajnych zdarzeń, - trybu zgłaszania i obsługi zdarzeń i podatności związanych z bezpieczeństwem informacji, - zarządzania ciągłością biznesową (PZCD), - zarządzania komunikacją kryzysową, - ustalania okoliczności i przyczyn wypadków przy pracy, - komunikacji wewnętrznej i zewnętrznej.	Zgodnie z regułami ustalonymi dla III poziomu ochrony informacji przetwarzanych w Spółce (pkt 3), z tym, że informacje w postaci elektronicznej można przekazywać jedynie na służbowych nośnikach informacji lub za pośrednictwem korporacyjnej poczty elektronicznej oraz z zapewnieniem spełnienia wymagań bezpieczeństwa informacji obowiązujących w Spółce, w szczególności zasad określonych w regulacjach dotyczących: - prowadzenia postępowań zakupowych i zawierania umów oraz elektronicznego obiegu dokumentów zakupowych, - korzystania / administrowania zasobami teleinformatycznymi (ICT), - zarządzania zasobami automatyki przemysłowej (OT), - nadzoru nad dokumentacją finansową i techniczną, - udostępniania zasobów informacyjnych na potrzeby realizacji prac dyplomowych i opracowań naukowych, - trybu zgłaszania i obsługi zdarzeń i podatności związanych z bezpieczeństwem informacji, - zarządzania ciągłością biznesową (PZCD), - zarządzania komunikacją kryzysową, - gospodarowania składnikami majątku trwałego oraz wartości niematerialnych i prawnych, a także rodzaju i obiegu dokumentów związanych z ich ewidencją, - komunikacji wewnętrznej i zewnętrznej.
Przekazywanie / udostępnianie na zewnątrz Spółki		
Wynoszenie informacji na zewnątrz Spółki	Za zgodą / upoważnieniem przełożonego lub Właściciela Zasobu oraz z zapewnieniem spełnienia wymagań bezpieczeństwa informacji obowiązujących w Spółce, w szczególności zasad określonych w regulacjach dotyczących: - bezpieczeństwa fizycznego i środowiskowego, - przebywania i poruszania się po terenie siedziby Spółki / Oddziału, - komunikacji wewnętrznej i zewnętrznej, - wynoszenia mienia na zewnątrz.	Informacje w postaci elektronicznej można wynosić jedynie na służbowych nośnikach informacji, za zgodą / upoważnieniem przełożonego lub Właściciela Zasobu oraz z zapewnieniem spełnienia wymagań bezpieczeństwa informacji obowiązujących w Spółce, w szczególności zasad określonych w regulacjach dotyczących: - bezpieczeństwa fizycznego i środowiskowego, - zasad gospodarowania rzeczowymi składnikami majątku trwałego oraz wartościami niematerialnymi, - przebywania i poruszania się po terenie siedziby Spółki / Oddziału, - komunikacji wewnętrznej i zewnętrznej, - wynoszenia mienia na zewnątrz.

Uwaga. W przypadku, gdy ww. dokumenty nie regulują pewnych zagadnień, to za upoważnieniem / zgodą przełożonego lub Właściciela Zasobu.

Tabela 6. Zasady przetwarzania informacji przyporządkowanych do IV poziomu ochrony

IV poziom ochrony	Szczególnie chronione, nadzorowane i kontrolowane w Spółce	
Postać informacji	**Papierowa**	**Elektroniczna**
Oznaczanie	Zgodnie z instrukcją kancelaryjną oraz dodatkowo: • informacje stanowiące tajemnicę Spółki oznaczamy klauzulą „Tajemnica Spółki", wg regulacji dot. ochrony tajemnic Spółki; • informacje poufne i stanowiące tajemnicę zawodową, w rozumieniu ustawy o obrocie instrumentami finansowymi, które spełniają warunki określone odpowiednio w art. 154 i 147 ww. ustawy, należy – do czasu ich publikacji – oznaczać zgodnie z regulacjami wewnętrznymi dot. realizacji giełdowych obowiązków informacyjnych i transakcji giełdowych. Ww. informacje / dane oznaczane są klauzulą od momentu ich utworzenia.	Zgodnie z instrukcją kancelaryjną oraz dodatkowo: • informacje stanowiące tajemnicę Spółki oznaczamy klauzulą „Tajemnica Spółki", a foldery / pliki w których się znajdują oznaczamy klauzulą „TS", wg regulacji dotyczących ochrony tajemnic Spółki; • informacje poufne i stanowiące tajemnicę zawodową, w rozumieniu ustawy o obrocie instrumentami finansowymi, które spełniają warunki określone odpowiednio w art. 154 i 147 ww. ustawy, należy – do czasu ich publikacji – oznaczać zgodnie z regulacjami wewnętrznymi dot. realizacji giełdowych obowiązków informacyjnych i transakcji giełdowych. Ww. informacje / dane oznaczane są klauzulą od momentu ich utworzenia.
Przechowywanie	Zgodnie z zasadami czystego biurka i ekranu oraz instrukcją kancelaryjną i regulacjami wewnętrznymi dotyczącymi: - ochrony tajemnic Spółki, - bezpieczeństwa danych osobowych, - realizacji giełdowych obowiązków informacyjnych i transakcji giełdowych, oraz wg Rozporządzenia Ministra Pracy i Polityki Socjalnej ws. zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika. Ponadto zgodnie z zasadami: • w godzinach pracy (w trakcie przetwarzania) poza wskazanymi miejscami przechowywania, ww. dokumenty nie mogą być pozostawione bez nadzoru; • po zamknięciu sprawy przekazanie do archiwum lub przechowywanie w komórce org. zgodnie z instrukcją kancelaryjną oraz regulacją wewnętrzną dotyczącą ustalania okoliczności i przyczyn wypadków przy pracy. W przypadku, gdy ww. regulacje nie obejmują swoim zakresem pewnych zagadnień, dokumentację należy przechowywać w szafach biurowych lub metalowych zamykanych na klucz, ewentualnie w sejfach.	Zgodnie z zasadami czystego biurka i ekranu oraz instrukcją kancelaryjną i regulacjami wewnętrznymi dotyczącymi: - ochrony tajemnic Spółki, - bezpieczeństwa danych osobowych, - realizacji giełdowych obowiązków informacyjnych i transakcji giełdowych, - korzystania / administrowania z zasobów teleinformatycznych (ICT), - zarządzania zasobami automatyki przemysłowej (OT), oraz wg Rozporządzenia Ministra Pracy i Polityki Socjalnej ws. zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika. W przypadku, gdy ww. regulacje nie obejmują swoim zakresem pewnych zagadnień należy: • nośniki, na których zapisane zostały dane / kopie zapasowe przechowywać w miejscu zabezpieczonym przed dostępem osób trzecich oraz w sposób uniemożliwiający jednoczesne zniszczenie kopii roboczych i zapasowych; • pozostałe nośniki należy przechowywać w zamkniętych pomieszczeniach lub w zamykanych meblach biurowych, bądź o wyższym stopniu zabezpieczenia; • dane na nośnikach należy przechowywać w sposób zaszyfrowany lub chroniony hasłem.

Kopiowanie	Zgodnie z zasadami czystego biurka i ekranu oraz regulacjami wewnętrznymi dot.: - ochrony tajemnic Spółki, - bezpieczeństwa danych osobowych, - realizacji giełdowych obowiązków informacyjnych i transakcji giełdowych.	Zgodnie z zasadami czystego biurka i ekranu oraz regulacjami wewnętrznymi dot.: - ochrony tajemnic Spółki, - bezpieczeństwa danych osobowych, - realizacji giełdowych obowiązków informacyjnych i transakcji giełdowych.
Niszczenie	Dokumenty po utracie wartości niszczymy zgodnie z regulacjami wewnętrznymi dot.: - ochrony tajemnic Spółki, - bezpieczeństwa danych osobowych, - realizacji giełdowych obowiązków informacyjnych. W przypadku, gdy ww. regulacje nie obejmują swoim zakresem pewnych zagadnień, to wg poniższych zasad: - w niszczarkach do dokumentów o poziomie bezpieczeństwa co najmniej „3” (wg normy DIN 32757 paski o szerokości mniejszej niż 2 mm lub ścinki o powierzchni mniejszej niż 320 mm^2, szerokości mniejszej niż 4 mm, długości mniejszej niż 80 mm) lub - w dedykowanych pojemnikach z koszami wrzutowymi lub niszczenie poprzez firmę utylizacyjną, po uprzednim uzyskaniu zgody Właściciela Zasobu.	Dokumenty po utracie wartości niszczymy zgodnie z regulacjami wewnętrznymi dot.: - ochrony tajemnic Spółki, - bezpieczeństwa danych osobowych, - realizacji giełdowych obowiązków informacyjnych. W przypadku, gdy ww. regulacje nie obejmują swoim zakresem pewnych zagadnień, to informacje należy zniszczyć w sposób uniemożliwiający odtworzenie zapisanych danych, np.: - przy wykorzystaniu specjalistycznego oprogramowania zapewniającego pięciokrotne nadpisanie danych lub - w sposób komisyjny zapewniający bezpieczne usunięcie danych, np. przy pomocy impulsu elektromagnetycznego, po uprzednim uzyskaniu zgody Właściciela Zasobu.
Przekazywanie / udostępnianie wewnątrz Spółki	Zgodnie z regułami ustalonymi dla IV poziomu ochrony informacji przetwarzanych w Spółce (pkt 3) oraz z zapewnieniem spełnienia wymagań bezpieczeństwa informacji obowiązujących w Spółce, w szczególności zasad określonych w regulacjach dotyczących: - ochrony tajemnic Spółki, - bezpieczeństwa danych osobowych, - realizacji giełdowych obowiązków informacyjnych i transakcji giełdowych.	Zgodnie z regułami ustalonymi dla IV poziomu ochrony informacji przetwarzanych w Spółce (pkt 3), z tym, że informacje w postaci elektronicznej można przekazywać jedynie na służbowych nośnikach informacji lub za pośrednictwem korporacyjnej poczty elektronicznej, w zaszyfrowanej formie lub chronione hasłem, oraz z zapewnieniem spełnienia wymagań bezpieczeństwa informacji obowiązujących w Spółce, w szczególności zasad określonych w regulacjach dotyczących: - instrukcji kancelaryjnej, - ochrony tajemnic Spółki, - bezpieczeństwa danych osobowych, - realizacji giełdowych obowiązków informacyjnych i transakcji giełdowych, - korzystania / administrowania zasobami teleinformatycznymi (ICT), - zarządzania zasobami automatyki przemysłowej (OT), oraz wg ustawy Prawo telekomunikacyjne (dot. Oddziałów będących operatorami publicznej sieci telekomunikacyjnej).
Przekazywanie / udostępnianie na zewnątrz Spółki		

Wynoszenie informacji na zewnątrz Spółki	Zgodnie z obowiązującymi regulacjami wewnętrznymi dotyczącymi: - ochrony tajemnic Spółki, - bezpieczeństwa danych osobowych, - realizacji giełdowych obowiązków informacyjnych i transakcji giełdowych, - bezpieczeństwa fizycznego i środowiskowego, - przebywania i poruszania się po terenie siedziby Spółki / Oddziału, - wydawania przepustek.	Informacje w postaci elektronicznej można wynosić jedynie na służbowych nośnikach informacji, w zaszyfrowanej formie lub chronione hasłem, zgodnie z regulacjami wewnętrznymi dotyczącymi: - ochrony tajemnic Spółki, - bezpieczeństwa danych osobowych, - realizacji giełdowych obowiązków informacyjnych i transakcji giełdowych, - bezpieczeństwa fizycznego i środowiskowego, - przebywania i poruszania się po terenie Oddziału Spółki / siedziby Spółki, - wydawania przepustek, oraz zgodnie z ustawą Prawo telekomunikacyjne (dot. Oddziałów będących operatorami publicznej sieci telekomunikacyjnej).

Uwaga. W przypadku, gdy ww. dokumenty nie regulują pewnych zagadnień, to za upoważnieniem / zgodą przełożonego lub Właściciela Zasobu.

ZAŁĄCZNIKI

Zał.1 Zasady klasyfikacji informacji w PGE GiEK S.A.
Zał.2 Zasady czystego biurka i ekranu w PGE GiEK S.A.
Zał.3.1 Oświadczenie o zachowaniu poufności pracownika PGE GiEK S.A.
Zał.3.2 Oświadczenie o zachowaniu poufności osoby niebędącej pracownikiem PGE GiEK S.A.

ZASADY KLASYFIKACJI INFORMACJI W PGE GiEK S.A.

1. WPROWADZENIE

1.1. Do przeprowadzenia klasyfikacji informacji (uporządkowania i pogrupowania informacji) koniecznym jest:
   a. zinwentaryzowanie przetwarzanych w Spółce informacji,
   b. połączenie informacji w grupy informacji,
   c. określenie wrażliwości grup informacji poprzez przydzielenie im stosownych wartości współczynników poufności, integralności i dostępności (pkt 2),
   d. wyznaczenie poziomów ochrony informacji, definiujących sposoby postępowania z nimi w odniesieniu do: oznaczania, przechowywania, kopiowania, niszczenia, przekazywania / udostępniania informacji wewnątrz i na zewnątrz Spółki oraz ich wynoszenia,
   e. przypisanie ustalonych grup informacji do odpowiednich poziomów ochrony informacji.

2. WRAŻLIWOŚĆ GRUP INFORMACJI

2.1. W PGE GiEK S.A. ustalono cztery grupy informacji (Tabela 1 w „Klasyfikacji informacji oraz zasadach ich przetwarzania w PGE GiEK S.A.” – *Zał.1* do Procedury).

2.2. Każda z grup informacji posiada pewną wartość dla Spółki zwaną wrażliwością grupy. Określa się ją poprzez przyporządkowanie grupie odpowiednich wartości współczynników poufności, integralności i dostępności, zgodnie ze wzorem **WG = P + D + I**, gdzie:
WG – wrażliwość grupy informacji,
P – współczynnik poufności danej grupy informacji,
D – współczynnik dostępności danej grupy informacji,
I – współczynnik integralności danej grupy informacji.

2.3. Wartości poszczególnych współczynników, o których mowa powyżej, ustala się na podstawie skal określonych w tabelach 1÷3:

Tabela 1. Wartości współczynnika poufności

Skala	Poziom poufności (P)
0	Informacje ogólnodostępne wewnątrz i na zewnątrz Spółki.
1	Informacje ogólnodostępne wewnątrz Spółki oraz dla uprawnionych pracowników* stron zewnętrznych związanych umowami lub uprawnionych nadrzędnymi przepisami prawa.
2	Informacje dostępne dla wybranych komórek / uprawnionych pracowników* w Spółce oraz uprawnionych pracowników* stron zewnętrznych związanych umowami lub uprawnionych nadrzędnymi przepisami prawa.
3	Informacje dostępne dla: - uprawnionych komórek org. / pracowników Spółki*, którzy dodatkowo posiadają uprawnienia / upoważnienia do przetwarzania informacji w zakresie danych osobowych / tajemnic Spółki / realizacji giełdowych obowiązków informacyjnych i transakcji giełdowych, - uprawnionych pracowników* stron zewnętrznych związanych umowami, którzy dodatkowo otrzymali uprawnienia / upoważnienia do przetwarzania informacji w zakresie danych osobowych / tajemnic Spółki / realizacji giełdowych obowiązków informacyjnych i transakcji giełdowych, - instytucji państwowych / organów administracji uprawnionych nadrzędnymi przepisami prawa.

* Uprawniony pracownik Spółki / strony zewnętrznej – pracownik, który złożył „Oświadczenie o zachowaniu poufności”.

Tabela 2. Wartości współczynnika dostępności

Skala	Poziom dostępności (D)
1	Informacje mogą być niedostępne powyżej 48 godzin.
2	Informacje mogą być niedostępne maksymalnie do 48 godzin.
3	Informacje mogą być niedostępne maksymalnie do 4 godzin w czasie dnia roboczego.

Tabela 3. Wartości współczynnika integralności

Skala	Poziom integralności (I)
0	Zmiana informacji zapewnia dokładność i kompletność informacji.
1	Zmiana informacji nie zapewnia dokładności i kompletności informacji.

3. WYLICZENIE WRAŻLIWOŚCI GRUP INFORMACJI I PRZYPISANIE POZIOMU OCHRONY DO KAŻDEJ Z GRUP

3.1. Na podstawie uzyskanych wartości wrażliwości grupy (WG) (Tabela 4), poszczególne grupy informacji przyporządkowuje się do ustalonych w Spółce poziomów ochrony informacji.

3.2. W Spółce ustalono cztery poziomy ochrony informacji (Tabela 2 w „Klasyfikacji informacji oraz zasadach ich przetwarzania w PGE GiEK S.A.” – *Zał.1* do Procedury).

3.3. Dla każdego z poziomów ochrony informacji określone zostały zasady przetwarzania informacji. Do zasad tych zalicza się sposoby oznaczania, przechowywania, kopiowania, niszczenia, archiwizowania, udostępniania informacji wewnątrz i na zewnątrz Spółki (Tabele 3÷6 w „Klasyfikacji informacji oraz zasadach ich przetwarzania w PGE GiEK S.A.”) oraz ogólne zasady czystego biurka i ekranu (*Zał.2* do „Klasyfikacji informacji oraz zasad ich przetwarzania w PGE GiEK S.A.”).

Tabela 4. Wyliczenie wrażliwości grup informacji i przypisanie poziomu ochrony do każdej z grup

Oznacze-nie grupy	Grupa informacji	P	D	I	WG	Poziom ochrony
G1	Informacje ogólnie dostępne wewnątrz i na zewnątrz Spółki	0	1	1	**2**	**I**
G2	Informacje ogólnie dostępne wewnątrz Spółki	1	2	1	**4**	**II**
G3	Informacje o ograniczonym dostępie	2	3	1	**6**	**III**
G4	Informacje szczególnie chronione	3	3	1	**7**	**IV**

ZASADY CZYSTEGO BIURKA I EKRANU W PGE GiEK S.A.

Ogólne zasady czystego biurka i ekranu określają zalecenia, których stosowanie pozwala ograniczyć ryzyko związane z bezpieczeństwem informacji takie jak: nieautoryzowany dostęp, utrata, kradzież lub uszkodzenie informacji w czasie i poza godzinami pracy.

Zasady czystego biurka i ekranu dotyczą:

- informacji zapisanych zarówno na papierze jak i na nośnikach elektronicznych (pendrive, płyta CD/DVD, dysk zewnętrzny, karta pamięci itp.) oraz
- serwerów, stacji roboczych (komputerów), sprzętu peryferyjnego oraz sprzętu przenośnego (laptopów, telefonów mobilnych, smartfonów itp.).

1.	**„Zasady czystego biurka”**
a.	Na stanowisku pracy można przechowywać tylko te dokumenty papierowe i nośniki elektroniczne, z których aktualnie korzystamy. Nieużywane dokumenty należy bezwzględnie zabezpieczyć, choćby w zamykanych szafach, a niepotrzebne niszczyć w sposób uniemożliwiający ich odczyt.
b.	Zabrania się pozostawiania na wierzchu (w widocznym miejscu) jakichkolwiek dokumentów objętych IV poziomem ochrony, kiedy na pewien okres czasu tracimy nad nimi kontrolę, np. na chwilę wychodzimy z pokoju.
c.	Przy każdorazowym opuszczeniu pokoju należy zamykać drzwi na klucz i nie pozostawiać go w zamku (nie dotyczy drzwi z elektrozamkami)
d.	Niedopuszczalne jest pozostawienie w pomieszczeniu osób trzecich bez żadnego nadzoru.
e.	Dokumenty, zarówno w wersji papierowej, jak i elektronicznej (w szczególności objęte III i IV poziomem ochrony), nie mogą pozostać niezabezpieczone po zakończeniu pracy (z wyłączeniem sytuacji, gdy praca jest kontynuowana na następnej zmianie) – dokumenty należy schować do zamykanej szafy, a klucz przechowywać w miejscu wiadomym osobom uprawnionym.
f.	Drukarki, kopiarki i faksy, ulokowane w miejscach ogólnie dostępnych (korytarz, pokój wydruków) oraz te usytuowane w obszarach bezpiecznych, należy chronić, a dokumenty odbierać natychmiast po wykonaniu przez urządzenie zleconego wydruku / kopii.
g.	Korzystanie z urządzeń, o których mowa pod lit. f, może być możliwe dopiero po autoryzacji dostępu.
2.	**„Zasady czystego ekranu”**
a.	Komputer / telefon mobilny powinien posiadać włączony „Wygaszacz ekranu” aktywowany hasłem / PIN-em. Zaleca się, aby czas aktywacji zabezpieczenia był wystarczająco krótki (zalecany czas to 1÷7 minut – należy go dopasować do klasyfikacji przetwarzanych informacji i ryzyka ich utraty). Uwaga: Nie dotyczy komputerów wykorzystywanych do monitorowania prawidłowości pracy urządzeń technicznych.
b.	Każdorazowe odejście od stanowiska pracy należy poprzedzić zablokowaniem komputera (np. w systemie Windows: naciskając jednocześnie klawisze: [Windows] i [L] albo wcisnąć kombinację klawiszy [Ctrl] [Alt] [Del] i użyć funkcji „Zablokuj komputer”.
c.	Na zakończenie pracy należy zamknąć aktywne sesje oraz wylogować się ze stacji roboczej. Uwaga! Dopuszcza się wyjątki od tej zasady w przypadku, kiedy zamknięcie danej sesji może spowodować istotne szkody w przetwarzaniu informacji, np. pracownik nadzoruje stan pracy urządzeń technicznych lub administrator przeprowadza w tym czasie testy sprzętu.
d.	Zabrania się zapisywania i przechowywania danych logowania (nazwa użytkownika i hasło) na dyskach twardych komputerów w postaci niezaszyfrowanej lub takiego z nimi postępowania, które umożliwia w prosty sposób dostęp do haseł osobom trzecim, np. zapisanie hasła na karteczce i przyklejenie jej do monitora.
e.	Ekrany monitorów komputerowych należy ustawić w sposób uniemożliwiający bezpośredni odczyt informacji przez osoby postronne, np. skierowane tyłem lub bokiem do drzwi wejściowych, ewentualnie być wyposażone w folie ograniczające pole widzenia.
f.	Zabrania się zapisywania dokumentów objętych IV poziomem ochrony bezpośrednio na pulpicie systemu operacyjnego.
g.	Zabrania się przetwarzania informacji objętych IV poziomem ochrony na urządzeniach przenośnych (w tym telefonach), o ile nie umożliwiają one szyfrowania danych.

AKTUALIZACJA 11.01.2018 r.

Oświadczenie o zachowaniu poufności pracownika PGE Górnictwo i Energetyka Konwencjonalna Spółka Akcyjna[1]

Ja niżej podpisana(-y) oświadczam, że znane mi są zasady dotyczące bezpieczeństwa informacji określone w procedurze „Organizacja i zarządzanie bezpieczeństwem informacji w PGE GiEK S.A." (PROC 10072) i zobowiązuję się do ich stosowania, a w szczególności do:

1) zachowania w poufności informacji, do których uzyskałam(-em) dostęp w związku z wykonywaniem obowiązków służbowych, niezależnie od formy przekazania tych informacji i ich źródła;
2) wykorzystywania / udostępniania uzyskanych informacji jedynie w celach związanych z wykonywaną pracą, wymaganiami umownymi oraz obowiązującymi uregulowaniami prawnymi;
3) odpowiedniego zabezpieczenia uzyskanych informacji, które uniemożliwi dostęp do nich podmiotom i osobom nieuprawnionym;
4) nieujawniania uzyskanych informacji i ich źródła osobom lub podmiotom nieuprawnionym*;
5) wykorzystywania przydzielonych lub udostępnionych mi zasobów do przetwarzania informacji jedynie do celów wynikających z zakresu wykonywanej pracy;
6) zwrotu, niezwłocznie po zakończeniu zatrudnienia, wszystkich przydzielonych / udostępnionych mi dokumentów i nośników, na których zostały utrwalone uzyskane informacje, nie zatrzymując żadnych ich kopii ani innych reprodukcji.

Jestem świadomy(-a) odpowiedzialności za naruszenie obowiązujących zasad, wynikających w szczególności z:

a) rozdziału XXXIII, Ustawy z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz.U. z 2016 r., poz. 1137 z późn. zm.),
b) Ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz.U. z 2003 r. Nr 153, poz. 1503 z późn. zm.),
c) Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r., poz. 922),
d) Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz.U. z 2016 r. poz. 1666 z późn. zm.),
e) regulaminu pracy obowiązującego w PGE GiEK S.A. – Centrala / Oddział.....[2]

Zobowiązuje się do zachowania poufności uzyskanych informacji również po zakończeniu zatrudnienia przez okres 3 lat**, chyba że odrębne pisemne ustalenia stanowią inaczej.

Stwierdzam, iż poinformowany(-a) zostałem(-am), że:

- *Zebrane dane osobowe będą przetwarzane, zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r. poz. 1182 ze zm.), przez PGE Górnictwo i Energetyka Konwencjonalna Spółka Akcyjna z siedzibą w Bełchatowie, ul. Węglowa 5, 97-400 Bełchatów, w celach związanych z zapewnieniem bezpieczeństwa informacji, których dotyczy niniejsze oświadczenie. Nie przewiduje się żadnych odbiorców danych w rozumieniu art. 7 ust. 6 ustawy o ochronie danych osobowych.*
- *Osoba, której dane dotyczą ma prawo wglądu do swoich danych oraz ich poprawiania.*
- *W chwili podpisania niniejszego oświadczenia pracodawca jest administratorem danych osobowych pracownika na podstawie art. 22[1] § 1 i 2 Kodeksu pracy.*

Imię i nazwisko pracownika składającego oświadczenie	Nr kadrowy pracownika	Podpis
.....	.....	.....

[1] Przez pojęcie „pracownik PGE Górnictwo i Energetyka Konwencjonalna Spółka Akcyjna" należy rozumieć pracownika Centrali lub Oddziału.
[2] Niepotrzebne usunąć.

* *W przypadku wątpliwości dotyczących uprawnień pracowników PGE GiEK S.A. lub osób i podmiotów zewnętrznych do uzyskania określonych informacji, należy zwrócić się do przełożonego celem uzyskania jednoznacznego stanowiska.*

** *Obowiązek zachowania poufności informacji wygasa jedynie w odniesieniu do tych informacji, które zostaną upowszechnione w wyniku okoliczności niestanowiących naruszenia zobowiązania do zachowania poufności oraz jeżeli wymagają tego bezwzględnie obowiązujące przepisy prawa, w zakresie wynikającym z tych przepisów.*

..... dnia .....

(Miejscowość)

.....
Podpis i pieczęć
osoby przyjmującej oświadczenie

Otrzymują:

1 x osoba składająca oświadczenie (kopia)

1 x komórka właściwa ds. HR w JO przyjmującej oświadczenie – akta osobowe pracownika (oryginał)

1 x komórka org. przyjmująca oświadczenie (kopia)

Oświadczenie o zachowaniu poufności osoby niebędącej pracownikiem PGE Górnictwo i Energetyka Konwencjonalna Spółka Akcyjna

W związku z wykonywaniem prac na rzecz PGE GiEK S.A. / realizacją dostaw dla PGE GiEK S.A. / odbywaniem praktyki w PGE GiEK S.A.[1], zgodnie z umową:

.....

.....

(nr i nazwa umowy)

w zakresie: .....

.....

.....

Ja niżej podpisana(-y) oświadczam, że:

1) zobowiązuję się zachować w poufności wszelkie informacje techniczne, technologiczne, ekonomiczne, finansowe, prawne, handlowe, organizacyjne i inne, które nie zostały podane do publicznej wiadomości, w szczególności stanowiące tajemnicę Spółki, uzyskane w związku z realizacją umowy, niezależnie od formy przekazania tych informacji i ich źródła;
2) zobowiązuję się uzyskane informacje wykorzystywać jedynie w celach określonych ustaleniami umowy oraz wynikającymi z obowiązujących uregulowań prawnych;
3) zobowiązuję się nie kopiować, nie ujawniać ani w jakikolwiek inny sposób nie rozpowszechniać informacji podmiotom oraz osobom nieuprawnionym z wyjątkiem uzasadnionej potrzeby wynikającej z realizacji umowy, po uprzednim poinformowaniu PGE GiEK S.A.;
4) zobowiązuję się nie wykraczać poza nadane mi uprawnienia oraz wykorzystywać przydzielone lub udostępnione mi zasoby do przetwarzania informacji, tylko do celów realizacji prac wynikających z zakresu umowy;
5) ponoszę pełną odpowiedzialność za szkodę wywołaną ujawnieniem informacji, o których mowa w pkt 1), w szczególności wynikłą z przekazania lub udostępnienia danych innym podmiotom i osobom nieuprawnionym oraz za brak odpowiedniego zabezpieczenia uzyskanych informacji, który może umożliwić dostęp do nich innym podmiotom i osobom nieuprawnionym;
6) zobowiązuję się do podjęcia wszelkich niezbędnych kroków dla zapewnienia, że uzyskanych informacji i ich źródła nie ujawnię podmiotom oraz osobom nieuprawnionym bez uzyskania uprzednio wyraźnego upoważnienia na piśmie od PGE GiEK S.A.;
7) jestem świadomy(-a) odpowiedzialności za naruszenie obowiązujących zasad, wynikających w szczególności z:
   a) rozdziału XXXIII Ustawy z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz.U. z 2016 r., poz. 1137 z późń zm.),
   b) Ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz.U. z 2003 r. Nr 153, poz. 1503 z późn. zm.),
   c) Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r., poz. 922),
   d) Ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2016 r., poz. 380),
8) zobowiązuję się najpóźniej w ciągu 10 dni po zakończeniu umowy, chyba że umowa stanowi inaczej, zwrócić wszystkie przydzielone / udostępnione przez PGE GiEK S.A. dokumenty i nośniki,
   na których zostały utrwalone uzyskane informacje, lub usunąć je w sposób uniemożliwiający ich odtworzenie nie zatrzymując żadnych ich kopii ani innych reprodukcji oraz zobowiązuję się w tym samym terminie do złożenia pisemnego oświadczenia o należytym wykonaniu tego obowiązku.

[1] Niepotrzebne usunąć.

Obowiązek zachowania poufności informacji obowiązuje przez okres 5 lat, licząc od dnia zakończenia umowy, chyba że odrębne pisemne ustalenia stanowią inaczej. Przy czym obowiązek zachowania poufności informacji wygasa jedynie w odniesieniu do tych informacji, które zostaną upowszechnione w wyniku okoliczności niestanowiących naruszenia zobowiązania do zachowania poufności oraz jeżeli wymagają tego bezwzględnie obowiązujące przepisy prawa w zakresie wynikającym z tych przepisów. W drugim przypadku składający oświadczenie o zachowaniu poufności informacji zobowiązuje się niezwłocznie powiadomić PGE GiEK S.A. o obowiązku ujawnienia informacji oraz podjąć wszelkie prawnie dopuszczalne kroki zmierzające do zminimalizowania zakresu ujawnianych informacji.

Wyrażam zgodę na przetwarzanie moich danych osobowych przez PGE Górnictwo i Energetyka Konwencjonalna Spółka Akcyjna z siedzibą w Bełchatowie, ul. Węglowa 5, 97-400 Bełchatów. Zgoda obejmuje również przetwarzanie danych w przyszłości, przez następców prawnych PGE GiEK S.A.
Stwierdzam, iż poinformowany(-a) zostałem(-am), że:

- *Zebrane dane osobowe będą przetwarzane, zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2014 r. poz. 1182 ze zm.), przez PGE Górnictwo i Energetyka Konwencjonalna Spółka Akcyjna z siedzibą w Bełchatowie, ul. Węglowa 5, 97-400 Bełchatów, w celach związanych z zapewnieniem bezpieczeństwa informacji, których dotyczy niniejsze oświadczenie. Nie przewiduje się żadnych odbiorców danych w rozumieniu art. 7 ust. 6 ustawy o ochronie danych osobowych.*
- *Osoba, której dane dotyczą ma prawo wglądu do swoich danych oraz ich poprawiania.*
- *Podanie danych osobowych jest dobrowolne i następuje w związku z realizacją umowy wskazanej na początku oświadczenia.*

Imię i nazwisko osoby składającej oświadczenie	Seria i nr dowodu osobistego	Nazwa firmy / instytucji	Podpis

..... dnia .....

(Miejscowość)

.....
Podpis i pieczęć
osoby przyjmującej oświadczenie

Otrzymują:

1 x osoba składająca oświadczenie (kopia)

1 x komórka właściwa ds. bezpieczeństwa w JO przyjmującej oświadczenie (oryginał)

1 x komórka org. przyjmująca oświadczenie (kopia)

ZASADY ZGŁASZANIA I OBSŁUGI ZDARZEŃ ZWIĄZANYCH Z BEZPIECZEŃSTWEM INFORMACJI ORAZ PODATNOŚCI ZASOBÓW I ZABEZPIECZEŃ W PGE GiEK S.A.

1. WPROWADZENIE

1.1. Przedmiotem regulacji „Zasady zgłaszania i obsługi zdarzeń związanych z bezpieczeństwem informacji oraz podatności zasobów i zabezpieczeń", zwanej dalej Zasadami, jest określenie sposobu postępowania w przypadku zaobserwowania zdarzenia związanego z bezpieczeństwem informacji lub podatności dotyczącej zasobu / zabezpieczenia, w zakresie:
   a. wykrycia i zgłoszenia zdarzenia związanego z bezpieczeństwem informacji lub podatności zasobu / zabezpieczenia,
   b. oceny zdarzenia pod względem poziomu istotności dla Spółki (identyfikacja incydentu) oraz analizy przyczyn jego wystąpienia,
   c. powstrzymania dalszego przebiegu incydentu oraz ograniczenia zasięgu i szkodliwości jego skutków,
   d. komunikacji z osobami związanymi ze zdarzeniem / incydentem oraz zaangażowanymi w jego rozwiązanie,
   e. planowania i wdrażania działań korygujących zmierzających do uniknięcia powtórzenia się incydentu w przyszłości,
   f. gromadzenia i zabezpieczenia dowodów oraz ich dokumentowania,
   g. raportowania działań do właściwych osób.

1.2. Zdarzenie związane z bezpieczeństwem informacji, to stwierdzone wystąpienie stanu systemu, usługi lub sieci, który wskazuje na możliwe naruszenie bezpieczeństwa informacji lub błąd zabezpieczenia, lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacji.

1.3. Incydent związany z bezpieczeństwem informacji, to pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.

1.4. Podatność, to słabość zasobu lub zabezpieczenia, która może być wykorzystana przez co najmniej jedno zagrożenie.

1.5. Działania opisane w Zasadach należy traktować priorytetowo i realizować bez zbędnej zwłoki.

2. ZGŁASZANIE ZDARZEŃ ZWIĄZANYCH Z BEZPIECZEŃSTWEM INFORMACJI ORAZ PODATNOŚCI ZASOBÓW I ZABEZPIECZEŃ

2.1. Tryb i zasady postępowania dotyczące zgłaszania zdarzeń związanych z bezpieczeństwem informacji oraz podatności zasobów i zabezpieczeń przedstawiono w tabeli poniżej:

Działanie	Osoba odpowiedzialna	Opis postępowania
Wykrycie i zgłoszenie zdarzenia lub podatności („Lista przykładowych zdarzeń / incydentów" stanowi *Zał.1* do Zasad)	1) Pracownik Spółki 2) Pracownik strony zewnętrznej który zauważył lub otrzymał informację o zdarzeniu bądź podatności zasobu / zabezpieczenia	Ad.1) Powiadomienie właściwego punktu kontaktowego (telefonicznie lub przy pomocy poczty elektronicznej) oraz przełożonego i odpowiednie służby / osoby (w razie potrzeby lub jeśli wynika to z wewnętrznych regulacji) o: - zdarzeniu związanym z bezpieczeństwem informacji, - podatności zasobu / zabezpieczenia, która może skutkować naruszeniem bezpieczeństwa informacji. „Wykazy punktów kontaktowych" w Spółce dostępne są w intranecie Spółki, na witrynie „Zarządzanie Procesami i Systemami" (https://giek.gkpge.pl/ZPiS) (pkt 2.2). W przypadku, gdy zdarzenie / stwierdzenie podatności ma miejsce poza godzinami pracy lub poza Spółką (np. kradzież laptopa, zagubienie dokumentów) zgłoszenia należy dokonać do właściwego punktu kontaktowego oraz jak najszybciej powiadomić swojego przełożonego. Ad.2) Powiadomienie pracownika Spółki, odpowiedzialnego za realizację umowy (Realizatora Umowy), który ma obowiązek powiadomić właściwy punkt kontaktowy i przełożonego.

2.2. Za opracowanie i bieżącą aktualizację „Wykazu punktów kontaktowych" oraz jego umieszczenie na witrynie „Zarządzanie Procesami i Systemami" (https://giek.gkpge.pl/ZPiS) odpowiedzialni są:
- w Oddziale – Koordynator SZBI,
- w Centrali – Zastępca Pełnomocnika ds. ZSZ.

Wykaz zatwierdza odpowiednio Dyrektor Oddziału lub Prezes Zarządu Spółki. Wzór „Wykazu punktów kontaktowych" przedstawia *Zał.2* do Zasad.

2.3. Zaleca się, aby kierujący komórkami organizacyjnymi umieścili „Wykaz punktów kontaktowych" w miejscach ogólnie dostępnych dla podwładnych (pracowników), np. na tablicach informacyjnych, w pokojach wydruku.

3. OBSŁUGA ZDARZEŃ / INCYDENTÓW ZWIĄZANYCH Z BEZPIECZEŃSTWEM INFORMACJI ORAZ PODATNOŚCI ZASOBÓW I ZABEZPIECZEŃ

3.1. Tryb i zasady postępowania dotyczące obsługi zdarzeń / incydentów związanych z bezpieczeństwem informacji przedstawiono w tabeli poniżej:

Lp.	Działanie	Osoba odpowiedzialna	Opis postępowania
1.	**Przyjęcie zgłoszenia o zdarzeniu / podatności**	Pracownik punktu kontaktowego	1) Przyjęcie zgłoszenia o: - zdarzeniu związanym z bezpieczeństwem informacji, - podatności zasobu / zabezpieczenia, która może skutkować naruszeniem bezpieczeństwa informacji. 2) Odnotowanie zgłoszenia w lokalnie prowadzonym rejestrze (dziennik zdarzeń, książka raportowa itp.). 3) Powiadomienie Administratora Merytorycznego SZBI właściwego ze względu na zakres działania[1], których wykaz dostępny jest w intranecie Spółki, na witrynie ZPiS (https://giek.gkpge.pl/ZPiS), w bibliotece „Model ZSZ i wykaz ról", plik „Wykaz_PodstawoweRoleZSZ".
2.	**Podjęcie bieżących działań naprawczych**	Pracownik punktu kontaktowego	1) Podjęcie bieżących działań naprawczych mających na celu minimalizację skutków wystąpienia zdarzenia i przywrócenie zasobów do sprawności. 2) Zabezpieczenie materiałów / informacji związanych ze zdarzeniem tak, aby zachowały wartość dowodową na potrzeby ewentualnego postępowania dyscyplinarnego lub procesowego. 3) W przypadku niemożności podjęcia samodzielnych działań, uruchomienie postępowania wg pkt 2.1.
2.1.	**Postępowanie naprawcze**	Odpowiednie komórki organizacyjne Centrali lub Oddziału / podmiot zewnętrzny	1) Zaplanowanie i wdrożenie działań mających na celu: - minimalizację skutków wystąpienia zdarzenia, - przywrócenie zasobów do normalnego stanu działania. 2) Zabezpieczenie materiałów / informacji związanych ze zdarzeniem tak, aby zachowały wartość dowodową na potrzeby ewentualnego postępowania dyscyplinarnego lub procesowego.
3.	**Poinformowanie o zakończeniu działań naprawczych**	Pracownik punktu kontaktowego	Poinformowanie o zakończeniu działań naprawczych kierujących komórkami organizacyjnymi objętymi zdarzeniem i Administratora Merytorycznego SZBI właściwego ze względu na zakres działania.

[1] Nie dotyczy zdarzeń i podatności z obszaru ICT, które zgłoszono do Service Desk (pkt 4, ppkt 2).

4.	**Analiza zgłoszeń**	• Administratorzy Merytoryczni SZBI w Spółce • Administratorzy Merytoryczni SZBI w Oddziałach Spółki – każdy w swoim zakresie	1) Bieżące przeglądanie i analizowanie zgłoszeń pod względem: okoliczności (przyczyn) wystąpienia zdarzenia, zakresu i poziomu jego istotności (wpływu na procesy biznesowe), skali przewidywanych / możliwych skutków (finansowych, prawnych, wizerunkowych) oraz ustalenie, czy mamy do czynienia z incydentem związanym z bezpieczeństwem informacji, z zastrzeżeniem ppkt 2. 2) Zdarzenia i podatności zgłoszone do Service Desk rejestruje i obsługuje CUW ICT (PGE Systemy S.A.) – rola Administratora Merytorycznego SZBI w zakresie teleinformatyki ogranicza się do bieżącego przeglądania i analizowania raportów przesyłanych przez CUW ICT oraz, w zależności od potrzeb, do podejmowania odpowiednich działań korygujących (pkt 6). 3) Jeżeli zdarzenie: a) zakwalifikowano jako incydent związany z bezpieczeństwem informacji lub podatność – rejestracja zgłoszenia zgodnie z pkt 5, b) nie zostało zakwalifikowane jako incydent lub podatność – zakończenie postępowania (pkt 7).
5.	**Rejestracja incydentu / podatności**	• Administratorzy Merytoryczni SZBI w Spółce • Administratorzy Merytoryczni SZBI w Oddziale Spółki – każdy w swoim zakresie	Rejestracja incydentu / podatności w „Rejestrze incydentów i podatności” oraz zanotowanie odpowiednich danych i szczegółów o incydencie / podatności potrzebnych do jego / jej obsługi (z wyłączeniem incydentów i podatności z obszaru ICT, które zgłoszono do Service Desk – pkt 4, ppkt 2). Rejestr prowadzony jest w formie elektronicznej i udostępniony w portalu Spółki na witrynie ZPiS (https://giek.gkpge.pl/ZPiS).
6.	**Przeciwdziałanie incydentom / podatnościom w przyszłości**		1) Uruchomienie działań doskonalących poprzez wystawienie „Protokołu poprawy funkcjonowania” (PPF) zgodnie z regulacją dot. poprawy funkcjonowania procesów i systemów zarządzania. 2) Uzupełnienie danych w „Rejestrze incydentów i podatności” w zakresie wystawionego PPF.
7.	**Zakończenie postępowania**	• Kierujący komórką org. odpowiedzialną za realizację działań doskonalących / naprawczych • Administratorzy Merytoryczni SZBI w Spółce / Oddziale Spółki – każdy w swoim zakresie	O ile zgłoszenie zostało zarejestrowane zgodnie z pkt 5, poinformowanie właściwego AM SZBI o ukończeniu działań doskonalących i uzupełnienie danych w „Rejestrze incydentów i podatności”. W pozostałych przypadkach – zakończenie działań.
8.	**Okresowe raportowanie**	• Administratorzy Merytoryczni SZBI w Spółce • Administratorzy Merytoryczni SZBI w Oddziale Spółki – każdy w swoim zakresie	Sporządzenie okresowej oceny procesu zarządzania incydentami związanymi z bezpieczeństwem informacji wraz z wnioskami, w terminach właściwych dla przeglądu procesów i systemów zarządzania.

Uwaga. W przypadku wystąpienia zdarzenia / incydentu związanego z cyberbezpieczeństwem należy powiadomić odpowiednie instytucje rządowe wg odrębnej regulacji (pkt 3.26 Procedury).

3.2. Dla ułatwienia realizacji procesu zarządzania incydentami opracowano algorytm postępowania na wypadek wystąpienia zdarzenia związanego z bezpieczeństwem informacji oraz podatności zasobów i zabezpieczeń, który przedstawiono w „Schemacie zgłaszania i obsługi zdarzeń związanych z bezpieczeństwem informacji oraz podatności zasobów i zabezpieczeń" – *Zał.3* do Zasad.

ZAŁĄCZNIKI

Zał.1 Lista przykładowych zdarzeń / incydentów.

Zał.2 Wykaz punktów kontaktowych (osób / służb odpowiedzialnych za przyjmowanie zgłoszeń o zdarzeniach związanych z bezpieczeństwem informacji oraz o podatnościach zasobów i zabezpieczeń).

Zał.3 Schemat zgłaszania i obsługi zdarzeń związanych z bezpieczeństwem informacji oraz podatności zasobów i zabezpieczeń.

LISTA PRZYKŁADOWYCH ZDARZEŃ / INCYDENTÓW

(poniższa lista nie wyczerpuje wszystkich możliwych przypadków wystąpienia zdarzenia / incydentu związanego z bezpieczeństwem informacji)

Lp.	Obszar	Zdarzenie / incydent
1.	Teleinformatyka / systemy przemysłowe	Zidentyfikowanie lub komunikat o wykryciu złośliwego oprogramowania, np. wirus, spyware.
2.		Niestabilna praca systemów.
3.		Niewłaściwe funkcjonowanie / awaria urządzenia (np. serwer, komputer, UPS, urządzenie sieciowe).
4.		Niewłaściwe funkcjonowanie aplikacji.
5.		Niedostępność systemu / aplikacji.
6.		Awaria / utrata zasilania urządzeń przetwarzających informacje (np. stacja robocza, system, serwer).
7.		Utrudniona praca w systemie np. zbyt duże obciążenie procesora, przekroczenie dostępnych zasobów systemowych.
8.		Nadmierne uprawnienia w systemach w stosunku do wykonywanej pracy.
9.		Nieuprawniona zmiana danych lub ich uszkodzenie.
10.		Utrata danych.
11.		Fizyczne zniszczenie lub uszkodzenie sprzętu oraz nośników przetwarzających informacje.
12.		Błędy w obsłudze i konserwacji sprzętu komputerowego służącego do przetwarzania informacji.
13.		Błędy w przechowywaniu, eksploatacji oraz konserwacji oprogramowania.
14.		Włamanie do sieci i systemów teleinformatycznych (np. atak crackera / hackera).
15.		Niewykonanie kopii bezpieczeństwa.
16.		Niezweryfikowanie możliwości odtworzenia danych z kopii zapasowych.
17.		Wykorzystanie nielegalnego oprogramowania oraz narzędzi służących do obchodzenia zabezpieczeń w systemach informatycznych.
18.		Próba instalacji niezatwierdzonego oprogramowania.
19.		Wykorzystanie ogólnodostępnych serwisów pocztowych (np. wp.pl, onet.pl, o2.pl) w celach służbowych.
20.		Niewłaściwe wykorzystywanie lub nadużywanie zasobów informacyjnych, np. wykorzystanie służbowych środków przetwarzania informacji do celów prywatnych.
21.		Niezgłaszanie informacji o nieprawidłowym działaniu systemów bezpieczeństwa (firewall, program AV).
22.		Rozpoznanie, penetracja i próby omijania systemów zabezpieczeń.
23.		Zmiana konfiguracji sprzętowej oraz programowej systemów oraz stacji roboczych przez niepowołane osoby.
24.		Wykonywanie pracy zdalnej przy pomocy komputera innego niż służbowy.
25.		Zablokowane konto w systemach informatycznych.
26.		Podjęcie pracy w stanie zagrożenia bezpieczeństwa informacji.
27.		Niestosowanie się do wymagań dotyczących złożoności haseł.
28.		Niezablokowana stacja robocza / niewylogowanie się z konta.
29.		Przesłanie wiadomości e-mail do niewłaściwego adresata.
30.		Przechowywanie haseł w niewłaściwy sposób.
31.		Przekazywanie haseł innym osobom.
32.		Pojawienie się nieautoryzowanej informacji na stronie internetowej.
33.		Niewłaściwe niszczenie nośników z danymi pozwalającymi na ich odczyt.
34.		Nieprzestrzeganie zasad czystego biurka i ekranu.
35.		Brak staranności przy zbywaniu sprzętu komputerowego / nośników lub przekazywaniu do ponownego użycia.

Lp.	Obszar	Zdarzenie / incydent
36.	Teleinformatyka / systemy przemysłowe cd.	Nieautoryzowany dostęp fizyczny do urządzeń.
37.		Naruszenie / fałszowanie praw.
38.		Wyciek informacji.
39.		Trudności z przywróceniem systemu.
40.		Manipulowanie urządzeniem.
41.		Manipulacja danymi.
42.		Nieprawidłowe użytkowanie systemu.
43.		Awaria systemu klimatyzacji.
44.		Awaria systemu ppoż.
45.	Strony zewnętrzne	Ujawnienie informacji / danych osobom nieuprawnionym.
46.		Brak stosownych zapisów dot. bezpieczeństwa informacji (zabezpieczeń) w umowach ze stronami zewnętrznymi.
47.		Praca pracowników firm zewnętrznych bez nadzoru (np. serwisantów).
48.		Wyłudzenia (lub próby wyłudzeń) ważnych informacji (np. tajemnice Spółki).
49.		Brak monitorowania i przeglądu dostarczanych usług zewnętrznych.
50.	Bezpieczeństwo osobowe	Brak oświadczenia pracownika o zachowaniu poufności.
51.		Nie podjęto działań związanych z odebraniem / zmianą uprawnień pracownika w związku z rozwiązaniem / zmianą umowy o pracę.
52.		Pracownik nie rozliczył się z powierzonych środków przetwarzania informacji.
53.		Naruszenie / łamanie zasad regulacji wewnętrznych, praw autorskich, przepisów prawnych.
54.		Brak szkoleń/ uświadamiania pracowników w zakresie bezpieczeństwa informacji.
55.		Nieświadome udostępnienie danych.
56.	Bezpieczeństwo fizyczne i środowiskowe	Nieuprawniony dostęp do pomieszczeń.
57.		Umieszczenie środków przetwarzania informacji niezabezpieczonych przed dostępem osób nieuprawnionych w strefie ogólnodostępnej.
58.		Pozostawienie osoby trzeciej w biurze / pomieszczeniu bez nadzoru.
59.		Wejście na obszar chroniony z pominięciem kontroli dostępu.
60.		Pozostawienie otwartych okien / drzwi po zakończeniu pracy.
61.		Pożar, zalanie, wilgoć, zapylenie.
62.		Pozostawienie środków przetwarzania informacji bez nadzoru.
63.		Nieprzestrzeganie / niewłaściwe stosowanie zasad czystego biurka i ekranu.
64.		Pozostawienie dokumentów w koszu na śmieci.
65.		Pozostawienie wydruków na ogólnodostępnej drukarce.
66.		Nieautoryzowane wykonanie kopii klucza do pomieszczeń biurowych.
67.		Wyniesienie klucza poza Spółkę lub pozostawienie klucza w drzwiach.
68.		Brak zapasowego klucza / niewłaściwe zarządzanie kluczami.
69.		Wynoszenie sprzętu poza Spółkę bez zezwolenia.
70.		Brak / zagubienie identyfikatora osobistego.
71.		Kradzież lub zniszczenie urządzeń przetwarzających lub przechowujących informacje oraz nośników danych.
72.		Kradzież dokumentów lub zniszczenia informacji, niezależnie od ich nośnika.
73.		Zgubienie nośników danych / dokumentów
74.		Brak / niewystarczająca fizyczna ochrona budynków, drzwi, okien.
75.		Pozostawienie niezabezpieczonych urządzeń / pomieszczeń technicznych wspierających przetwarzanie informacji.
76.	Zarządzanie aktywami / zasobami	Zidentyfikowano sprzęt / nośnik przetwarzający informacje nieznanego pochodzenia.
77.		Stwierdzono niewystarczającą pojemność zasobów.
78.		Wykorzystano nośnik informacji nienależący do Spółki.
79.	Zgodność	Nielegalne przetwarzanie danych.
80.		Brak / niekompletna dokumentacja wymagana prawem.

PGE GiEK S.A. – Centrala / Oddział...[1]

WZÓR

WYKAZ PUNKTÓW KONTAKTOWYCH

(osób / służb odpowiedzialnych za przyjmowanie zgłoszeń o zdarzeniach związanych z bezpieczeństwem informacji oraz o podatnościach zasobów i zabezpieczeń)

<table>
<tr><th>Lp.</th><th colspan="2">Rodzaj zgłoszenia</th><th colspan="2">Powiadamiana osoba / służba</th></tr>
<tr><td rowspan="2">1.</td><td colspan="2" rowspan="2">Zgłaszanie pożaru, klęski żywiołowej oraz innych miejscowych zagrożeń</td><td colspan="2">w Oddziale Spółki na I, II i III zmianie oraz w dni wolne od pracy</td></tr>
<tr><td colspan="2">Właściwe służby ratownicze + przełożony, który powiadamia Dyżurnego / Zmianowego Inżyniera Ruchu[1], tel. ....., e-mail: .....
(który z kolei powiadamia AM SZBI[2] w Oddziale Spółki w zakresie bezpieczeństwa fizycznego i środowiskowego lokalizacji, ochrony danych osobowych i tajemnic Spółki, tel. ....., e-mail: .....)
w Centrali Spółki na I zmianie
Właściwe służby ratownicze + przełożony, który powiadamia Dyrektora Departamentu HR, tel. ....., e-mail: .....
(który z kolei powiadamia AM SZBI[2] w Spółce w zakresie bezpieczeństwa fizycznego i środowiskowego lokalizacji, ochrony danych osobowych i tajemnic Spółki, tel. ....., e-mail: .....)</td></tr>
<tr><td>2.</td><td colspan="2">Zgłaszanie zdarzeń oraz podatności dotyczących telefonii</td><td colspan="2">w Oddziale Spółki na I, II i III zmianie oraz w dni wolne od pracy
Służba właściwa ds. łączności, tel. .....,
a w przypadku jej braku wg pkt 3.a
(która powiadamia AM SZBI[2] w Oddziale Spółki w zakresie systemów OT, tel. ..... e-mail: .....)
+ przełożony (w razie potrzeby)</td></tr>
<tr><td rowspan="2">3.</td><td rowspan="2">Zgłaszanie zdarzeń oraz podatności dot. zasobów i zabezpieczeń:</td><td>a) teleinformatycznych (ICT), w tym telefonii[3]</td><td colspan="2">na I, II i III zmianie oraz w dni wolne od pracy
Service Desk:
tel. 5555 (z tel. mob.: 22 344 5555), e-mail: sd@gkpge.pl
(który okresowo raportuje do AM SZBI[2] w Spółce w zakresie teleinformatyki – ICT)
+ przełożony (w razie potrzeby)</td></tr>
<tr><td>b) OT</td><td colspan="2">na I, II i III zmianie oraz w dni wolne od pracy
Służba właściwa ds. systemów OT, tel. ....., e-mail: .....
(która powiadamia AM SZBI[2] w Spółce / Oddziale Spółki[1] w zakresie systemów OT, tel. ....., e-mail: .....,
+ przełożony</td></tr>
<tr><td>4.</td><td colspan="2">Zgłaszanie zdarzeń oraz podatności związanych z bezpieczeństwem fizycznym, w tym z zagrożeniem terrorystycznym i sabotażem
(kradzież, zniszczenie lub zagubienie mienia, w tym elektronicznych kart dostępu, włamanie, uszkodzone drzwi, otwarte okno, nieznana osoba bez identyfikatora na terenie Spółki itp.)</td><td>na I zmianie
AM SZBI[2] w Spółce / Oddziale Spółki[1] w zakresie bezpieczeństwa fizycznego i środowiskowego lokalizacji, ochrony danych osobowych i tajemnic Spółki,
tel. ....., e-mail: .....)
+ przełożony</td><td>na II i III zmianie oraz w dni wolne od pracy
Służba ochrony, tel. .....
(która powiadamia AM SZBI[2] Spółce / Oddziale Spółki[1] w zakresie bezpieczeństwa fizycznego i środowiskowego lokalizacji, ochrony danych osobowych i tajemnic Spółki, tel. ....., e-mail: .....)
+ przełożony</td></tr>
</table>

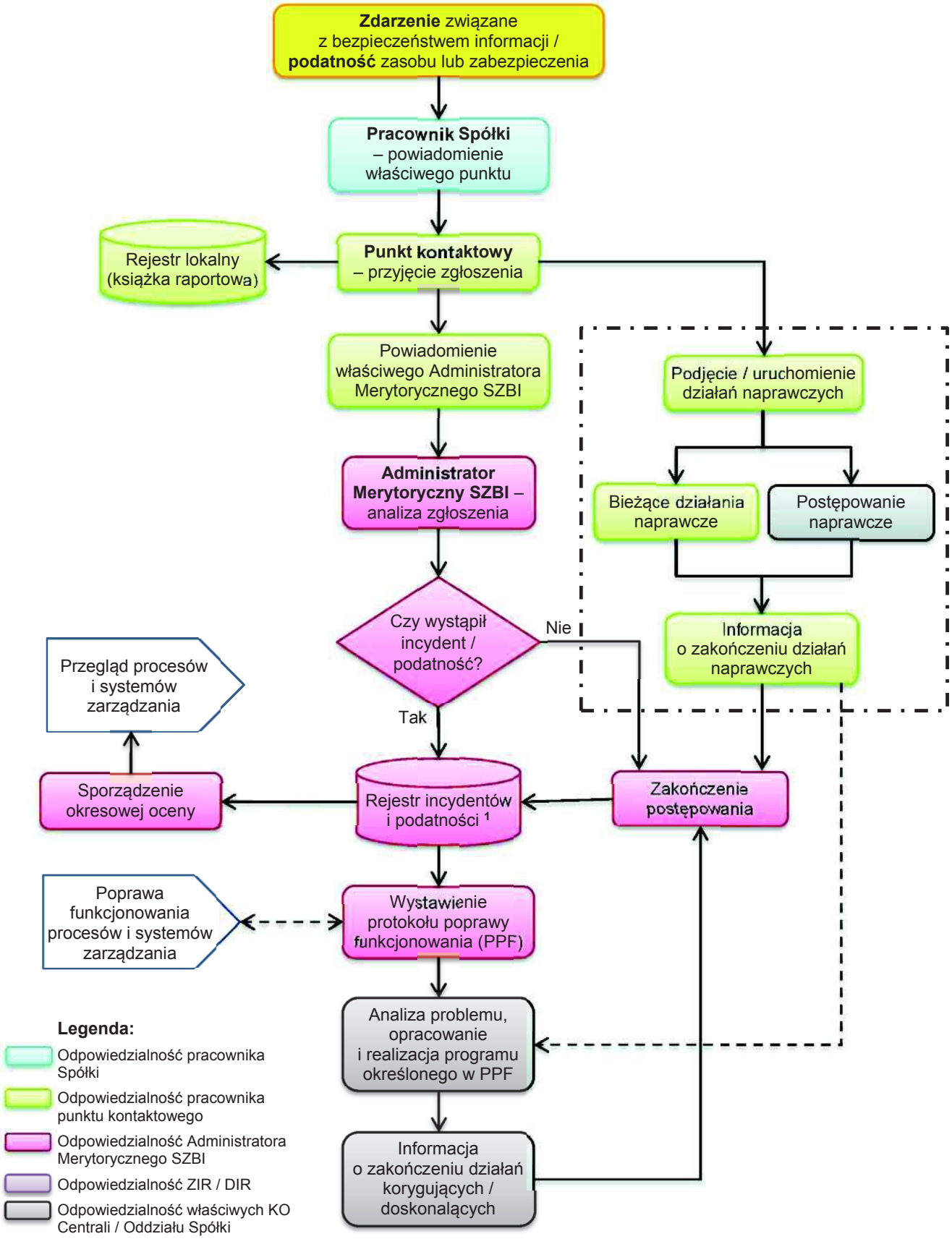
[1] Niepotrzebne usunąć.
[2] AM SZBI – Administrator Merytoryczny Systemu Zarządzania Bezpieczeństwem Informacji.
[3] Dotyczy JO, w których nie występują służby właściwe ds. łączności (pkt 2).

<table>
<tr><td rowspan="4">5.</td><td rowspan="4">Zgłaszanie zdarzeń i podatności dot. informacji szczególnie chronionych:</td><td>a) tajemnice Spółki, dane wynikające z giełdowych obowiązków informacyjnych oraz dot. obrotu na giełdach towarowych</td><td>na I zmianie</td></tr>
<tr><td></td><td>Kierujący komórką organizacyjną, który powiadamia bezpośredniego przełożonego oraz
AM SZBI[2] Spółce / Oddziale Spółki[1] w zakresie bezpieczeństwa fizycznego i środowiskowego lokalizacji, ochrony danych osobowych i tajemnic Spółki, tel. ....., e-mail: .....</td></tr>
<tr><td rowspan="2">b) dane osobowe</td><td>na I zmianie</td></tr>
<tr><td><u>w Oddziale Spółki:</u>
Koordynator ds. Ochrony Danych Osobowych, tel. ....., e-mail: .....
(który powiadamia AM SZBI[2] w Oddziale Spółki w zakresie bezpieczeństwa fizycznego i środowiskowego lokalizacji, ochrony danych osobowych i tajemnic Spółki, tel. ....., e-mail: .....)
+ przełożony
<u>w Centrali Spółki:</u>
Pełnomocnik ds. Ochrony Danych Osobowych, tel. ....., e-mail: .....
(AM SZBI[2] w Spółce w zakresie bezpieczeństwa fizycznego i środowiskowego w lokalizacji, ochrony danych osobowych i tajemnic Spółki)
+ przełożony</td></tr>
<tr><td>6.</td><td>Zgłaszanie podatności i awarii instalacji: elektrycznej, centralnego ogrzewania, wodociągowej, kanalizacyjnej itp.</td><td colspan="2"><table>
<tr><th>na I zmianie</th><th>na II i III zmianie oraz w dni wolne od pracy</th></tr>
<tr><td colspan="2"><u>w Oddziale Spółki:</u></td></tr>
<tr><td>Administrator budynku / obiektu, tel. ....., e-mail: .....
(który powiadamia AM SZBI[2] w Oddziale Spółki w zakresie bezpieczeństwa fizycznego i środowiskowego lokalizacji, tel. ..... e-mail: .....)</td><td>Dyżurny / Zmianowy Inżynier Ruchu, tel. .....
(który powiadamia AM SZBI[2] w Oddziale Spółki w zakresie bezpieczeństwa fizycznego i środowiskowego lokalizacji, tel. ....., e-mail: .....)</td></tr>
<tr><td colspan="2"><u>w Centrali Spółki:</u></td></tr>
<tr><td>Biuro Administracji, tel. ....., e-mail: .....
(które powiadamia AM SZBI[2] w Oddziale Spółki w zakresie bezpieczeństwa fizycznego i środowiskowego lokalizacji, ochrony danych osobowych i tajemnic Spółki, tel. ....., e-mail: .....)</td><td>Kierownik Biura Administracji, tel. ....., e-mail: .....
(który powiadamia AM SZBI[2] w Oddziale Spółki w zakresie bezpieczeństwa fizycznego i środowiskowego lokalizacji, ochrony danych osobowych i tajemnic Spółki, tel. ....., e-mail: .....)</td></tr>
</table></td></tr>
</table>

Uwagi:
1) Zgłoszenia o zdarzeniu dokonuje bezpośrednio pracownik lub jego przełożony.
2) Pracownicy punktów kontaktowych wyróżnieni pogrubioną czcionką – pracownicy odpowiedzialni za podjęcie / uruchomienie bieżących działań naprawczych zgodnie z *Zał.2* do Procedury.
3) W przypadku wystąpienia zdarzenia / incydentu związanego z cyberbezpieczeństwem należy powiadomić odpowiednie instytucje rządowe wg odrębnej regulacji (pkt 3.26 Procedury).

	Sporządził:	Zatwierdził
Miejscowość i data	Z-ca Pełnomocnika ds. ZSZ / Koordynator SZBI (podpis i pieczęć)	Prezes Zarządu / Dyrektor Oddziału (podpis i pieczęć)

SCHEMAT ZGŁASZANIA I OBSŁUGI ZDARZEŃ ZWIĄZANYCH Z BEZPIECZEŃSTWEM INFORMACJI ORAZ PODATNOŚCI ZASOBÓW I ZABEZPIECZEŃ W PGE GiEK S.A.



[1] Nie dotyczy zdarzeń i podatności z obszaru ICT, które zgłoszono do Service Desk.

Uwaga. W przypadku wystąpienia zdarzenia / incydentu związanego z cyberbezpieczeństwem należy powiadomić odpowiednie instytucje rządowe wg odrębnej regulacji (pkt 3.26 Procedury).

W Z Ó R

PGE GiEK S.A. – Centrala / Oddział ...[1]

(Nazwa jednostki organizacyjnej)

PLAN CIĄGŁOŚCI DZIAŁANIA ZASOBU

(Nazwa zasobu wspierającego)

Opracował:	Akceptował:		Zatwierdził:
Właściciel Zasobu	Administrator Merytoryczny SZBI w Spółce / Oddziale Spółki[1] – właściwy dla zasobu	Pełnomocnik ds. ZSZ / Koordynator SZBI[1]	Członek Zarządu / Dyrektor w Oddziale[1] – właściwy dla Właściciela Zasobu

(Miejscowość i data)

[1] Niepotrzebne usunąć – w tym ten przypis.

Spis treści

Rozdział 1
Cel Planu ciągłości działania zasobu (PCDZ)

Jednoznaczny cel powstania Planu: Zapewnienie natychmiastowej i skutecznej reakcji w przypadku wystąpienia sytuacji awaryjnej w celu zapewnienia ciągłości działania zasobu, tj. utrzymania zdolności Centrali / Oddziału do dalszej realizacji procesu / procesów, minimalizacji strat oraz szybkiego odtworzenia normalnego poziomu działania zasobu.[1]

...

Rozdział 2
Informacja o zasobie

Zwięzły opis zasobu, dla którego tworzony jest Plan ciągłości działania zasobu (jego charakterystyka, opis normalnego stanu funkcjonowania zasobu, m.in. godziny dostępności zasobu, uprawnienia do zasobu itp.). [1]

...

Rozdział 3
Środowisko funkcjonowania zasobu

W sposób opisowy lub graficzny przedstawić środowisko, w którym funkcjonuje zasób objęty Planem, np. infrastruktura, na której pracuje zasób (macierze, serwery itd.), w tym inne zasoby mające wpływ na jego funkcjonowanie.[1]

...

Rozdział 4
Osoby odpowiedzialne za zasób i środowisko jego funkcjonowania

Dla zasobu krytycznego objętego Planem oraz każdego zasobu mającego wpływ na jego funkcjonowanie (rozdz. 3) należy wymienić osoby odpowiedzialne za utrzymanie w sprawności tych zasobów podając imię, nazwisko, stanowisko, komórkę organizacyjną oraz dane kontaktowe (adres e-mail, nr tel. stacjonarnego i mobilnego), a w przypadku, gdy dostawcą usługi jest podmiot zewnętrzny również nazwę i dane teleadresowe tego podmiotu. [1]

...

Rozdział 5
Określenie akceptowalnego poziomu utraty informacji i niedostępności zasobu

Należy podać dopuszczalny czas niedostępności zasobu objętego planem (w tym czasy przerw technicznych) oraz akceptowalny poziom utraty informacji i usług.[1]

...

Rozdział 6
Zagrożenia dla zasobu i środowiska jego funkcjonowania oraz sposoby postępowania w przypadku wystąpienia zagrożeń

Należy wskazać istotne zagrożenia dla zasobu objętego planem i środowiska jego funkcjonowania (np. zidentyfikowane podczas analizy ryzyka) oraz określić sposoby postępowania odpowiednie dla skutków wystąpienia poszczególnych zagrożeń.[1]

...

Rozdział 7
Działania podejmowane w przypadku przekroczenia akceptowanego czasu niedostępności zasobu

Opis działań zastępczych, które należy podjąć, aby zapewnić ciągłość realizacji procesu / procesów w przypadku, gdy czas niedostępności zasobu jest dłuższy niż dopuszczalny wraz z określeniem odpowiedzialności za te działania (zasady i tryb postępowania, w tym schematy komunikacji, na czas awarii uniemożliwiającej korzystanie z zasobu / świadczenie usługi).[1]

...

Rozdział 8
Sposób postępowania po zakończeniu działań naprawczych lub odtworzeniowych

Określenie sposobu i odpowiedzialności w zakresie oceny poprawności i skuteczności zakończonych działań naprawczych lub odtworzeniowych oraz przekazania zasobu do użytkowania (testy, próby, badania, pomiary i odbiory techniczne).[1]

...

Rozdział 9
Zasady oraz harmonogram testowania planu ciągłości działania

Opracowanie, wg wytycznych określonych w pkt 6.6.1.6 Procedury, „Harmonogramu testowania PCDZ" uwzględniającego: sam zasób oraz środowisko, w którym on działa, rodzaje testów (Zał.4 do Procedury) oraz terminy i odpowiedzialność za ich przeprowadzenie. W harmonogramie należy również określić odpowiedzialność za przygotowanie, z odpowiednim wyprzedzeniem, szczegółowych planów testów oraz sporządzenie raportów z testów.

...

Rozdział 10
Działania prewencyjne podejmowane w celu utrzymania zasobu w wymaganej sprawności

Opis działań koniecznych do utrzymania zasobu objętego planem w sprawności (umowy serwisowe, przeglądy techniczne i konserwacje, niezbędne części zamienne, kopie bezpieczeństwa i inne) oraz przypisanie osób odpowiedzialnych za poszczególne działania.[1]

...

Rozdział 11
Działania uświadamiające i szkolenia dotyczące planu ciągłości działania

Opis działań uświadamiających i szkoleń dla uczestników PCDZ, jakie należy dokonywać, aby zapewnić skuteczność planu ciągłości działania wraz z przedstawieniem harmonogramu szkoleń oraz osób odpowiedzialnych za ich przeprowadzanie i dokumentowanie (listy obecności, tematyka szkolenia).[1]

...

RODZAJE TESTÓW PLANÓW CIĄGŁOŚCI DZIAŁANIA ZASOBÓW W PGE GiEK S.A.

1. WPROWADZENIE

1.1. W celu zapewnienia adekwatności i skuteczności Planów ciągłości działania zasobów (PCDZ) należy je testować i w zależności od potrzeb modyfikować. Rodzaje testów przedstawiono w tabeli w pkt 2.

1.2. Testowanie PCDZ pokazuje praktyczną zdolność Oddziału / Spółki do kontynuacji i odtworzenia krytycznych zasobów informacyjnych oraz pozwala na weryfikację poprawności i skuteczności przyjętych rozwiązań. Testy angażują wielu uczestników, przyczyniając się do poszerzania wiedzy o PCDZ.

1.3. Testy należy przeprowadzać w zaplanowanych odstępach czasu, zgodnie z „Harmonogramem testowania PCDZ" stanowiącym element Planu (Rozdział 9). Aby ocenić, czy PCDZ zadziała w rzeczywistej sytuacji, zaleca się przeprowadzanie testów operacyjnych. Należy przy tym kierować się zasadą maksymalnego ograniczania ryzyka utraty zasobów w trakcie testów, przy jednoczesnym zapewnieniu wysokiego poziomu zdolności do odtworzenia działalności.

1.4. W sytuacji, gdy zweryfikowanie działań ustalonych w PCDZ za pomocą testu operacyjnego może stanowić poważny problem dla Oddziału / Centrali, np. ze względów finansowych, logistycznych lub ze względu na możliwość przerwania procesów biznesowych, zaleca się przeprowadzenie testu „Symulacja", ewentualnie „Seminarium".

2. RODZAJE TESTÓW

Lp.	Rodzaj testu	Opis	Uczestnicy testu
1	**Seminarium**	Uczestnicy testu nie przemieszczają się w trakcie testu poza miejsce spotkania, dzieleni są na grupy oraz trzymują pytania związane z wybranym zdarzeniem. Grupy omawiają metody działania i reakcji na zdarzenie, a następnie przedstawiają swoje propozycje pozostałym uczestnikom. W trakcie dyskusji omawiane są proponowane sposoby działania i reakcji oraz ustalane ostateczne metody postępowania Jego uczestnicy testu, winni przeprowadzić weryfikację / analizę PCDZ pod względem spójności, kompletności, niezbędnych zasobów i sposobu jego przeprowadzenia, w tym kolejności ustalonych działań.	• Uczestnicy PCDZ • Właściciel Zasobu • AM SZBI właściwy dla zasobu • Administrator Techniczny właściwy dla zasobu
2	**Symulacja**	Uczestnicy testu przemieszczają się w miejsca właściwe dla poszczególnych zadań oraz komunikują się z pozostałymi uczestnikami – przekazując informacje i polecenia (używając zasobów służących komunikacji). Osoby kierownictwa otrzymują komunikaty, na podstawie których podejmują decyzje istotne dla przebiegu akcji awaryjnej. Pozostali uczestnicy reagują na zaaranżowane zdarzenia symulując użycie zasobów. Ćwiczenie umożliwia dużą elastyczność i może być łatwo dostosowane do potrzeb Oddziału / Spółki. Symulacja zazwyczaj wymaga udziału koordynatora oraz obserwatorów oceniających działania podejmowane przez uczestników testu.	• Uczestnicy PCDZ • Koordynator testu • Właściciel Zasobu • AM SZBI właściwy dla zasobu • Administrator Techniczny właściwy dla zasobu • Obserwatorzy

3	**Test operacyjny**	Złożone ćwiczenia, które przeprowadza się w warunkach zaaranżowanego zdarzenia i mają one tym większą wartość, im bardziej te warunki odpowiadają realiom. Uczestnicy testu podejmują działania określone w PCDZ i przywołanych w nim procedurach – reagują na zdarzenie używając zasobów materialnych. Przykładem testu operacyjnego mogą być ćwiczenia z udziałem jednostek ratowniczych i porządkowych, w których zespoły przemieszczają się do lokalizacji zapasowych (gdzie weryfikują dostępne wyposażenie), a systemy ICT lub OT przełączane są do ośrodka zapasowego. Ćwiczenia wymagają udziału koordynatora oraz obserwatorów oceniających działania podejmowane przez uczestników testu.	• Uczestnicy PCDZ • Koordynator testu • Właściciel Zasobu • AM SZBI właściwy dla zasobu • Administrator Techniczny właściwy dla zasobu • Wszyscy pracownicy objęci zdarzeniem • Dostawcy • Obserwatorzy

Deklaracja stosowania zabezpieczeń
w PGE GiEK S.A. - Centrala / Oddział...[1]

z dnia ...

Zaakceptował merytorycznie:

.....	.....	.....	.....
Administrator Merytoryczny SZBI w Spółce / Oddziale Spółki[1] w zakresie bezpieczeństwa fizycznego i środowiskowego lokalizacji, ochrony danych osobowych i tajemnic Spółki	Administrator Merytoryczny SZBI w Spółce / Oddziale Spółki[1] w zakresie teleinformatyki (ICT)	Administrator Merytoryczny SZBI w Spółce / Oddziale Spółki[1] w zakresie systemów OT	Dyrektor Departamentu HR / Kierujący komórką właściwą ds. HR w Oddziale Spółki [1]

Zaakceptował:

.....	.....
Administrator Funkcjonalny ZSZ / Koordynator ZSZ [1]	Pełnomocnik ds. ZSZ (dotyczy Centrali Spółki)

Zatwierdził:

.....
Prezes Zarządu / Dyrektor Oddziału [1]

[1] Niepotrzebne usunąć - w tym ten przypis.

Deklaracja stosowania zabezpieczeń w PGE GiEK S.A. - Centrala / Oddział...

Stan na dzień: …

Załącznik A do normy PN-ISO/IEC 27001			Opis zabezpieczenia	Komórka org. odpowiedzialna za aktualizację opisu zabezpieczenia **GRUPA I** *(symbol KO)*	Komórka org. odpowiedzialna za ocenę zbioru/ podzbioru zabezpieczeń **GRUPA II** *(symbol KO)*	Komórka org. odpowiedzialna za dostarczenie danych **GRUPA III** *(symbol KO)*	Częstość przeprowa-dzania oceny skuteczności zabezpieczeń *(wg listy wyboru)*	Miernik *(opis miernika lub wzór i opis miernika)*	Ocena skuteczności						Nr wystawionego PPF *(dotyczy poziomu nieakcepto-walnego)*
									Data oceny *(rrrr.mm.dd)*	Wartości liczbowe składników miernika *(podstawione do wzoru)*	Wartość miernika *(liczba)*	Kryterium skuteczności *(zakładany cel - wartość miernika)*	Poziom skuteczności: akceptowalny / nieakceptowalny	Kierunek zmian (porównanie bieżącej wartości miernika do ostatniej) *(wg listy wyboru)*	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
A.x (Nr Rozdziału)	**Nazwa Rozdziału**														
A.x.x (Nr Rozdziału)	Nazwa Rozdziału	Cel: …			Symbol [redacted]	Symbol [redacted]	1 x [redacted]	Miernik ustalony dla Spółki	Data ostatniej oceny	x_1	**6,00**	0,0 - 5,0	nieakceptowalny	→ bez zmian	…/…/…
									Data bieżącej oceny	…	**2,00**		akceptowalny	↗ pozytywny	
A.x.x.x	Nazwa Rozdziału	Zabezpieczenie: …	Opis 1 Opis 2 Opis 3 …	[redacted]											
A.x.x.x	Nazwa Rozdziału	Zabezpieczenie: …	Opis 1 Opis 2 Opis 3 …	[redacted]											
A.x.x (Nr Rozdziału)	Nazwa Rozdziału	Cel: …			Symbol kom. org.	Symbol kom. org.	[redacted]	[redacted]	Data poprze-dniej oceny	x_2 / y_2	**0,75**	0,9 - 1,0	nieakceptowalny	→ bez zmian	…/…/…
									Data ostatniej oceny	…	**0,95**		akceptowalny	↗ pozytywny	
									Data bieżącej oceny	…	**0,75**		nieakceptowalny	↘ negatywny	…/…/…
A.x.x.x	Nazwa Rozdziału	Zabezpieczenie: …	Opis 1 Opis 2 Opis 3 …	Symbol KO 1 Symbol KO 2 Symbol KO 3 …											
A.x.x.x	Nazwa Rozdziału	Zabezpieczenie: …	Opis 1 Opis 2 …	Symbol KO 1 Symbol KO 2 …											
A.x.x.x	Nazwa Rozdziału	Zabezpieczenie: …	Opis 1 Opis 2 …	[redacted] Symbol KO 2 …											
A.x.x (Nr Rozdziału)	Nazwa Rozdziału	Cel: …			Symbol kom. org. 1	Symbol kom. org.	1 x na kwartał	Miernik ustalony dla Spółki	Data poprze-dniej oceny	…	**0,90**	0,8 - 1,0	akceptowalny	→ bez zmian	
									Data poprze-dniej oceny	…	**0,75**		nieakceptowalny	↘ negatywny	
					Symbol kom. org. 2	Symbol kom. org.			Data ostatniej oceny	…	**0,70**		nieakceptowalny	↘ negatywny	…/…/…
									Data bieżącej oceny	x_3 / y_3	**0,80**		akceptowalny	↗ pozytywny	
A.x.x.x	Nazwa Rozdziału	Zabezpieczenie: …	Opis 1 Opis 2	Symbol KO 1 Symbol KO 2											
A.x.x.x	Nazwa Rozdziału	Zabezpieczenie: …	Opis 1 Opis 2 Opis 3	Symbol KO 1 Symbol KO 2 Symbol KO 3											

ZASADY OPRACOWYWANIA DEKLARACJI STOSOWANIA ZABEZPIECZEŃ I OCENY ICH SKUTECZNOŚCI W PGE GiEK S.A.

1. WPROWADZENIE

1.1. Deklarację stosowania zabezpieczeń i ocenę ich skuteczności sporządza się w oparciu o formularz „Deklaracja stosowania zabezpieczeń w PGE GiEK S.A.", którego wzór stanowi *Zał.5* do Procedury „Organizacja i zarządzanie bezpieczeństwem informacji w PGE GiEK S.A.". Wersja edytowalna formularza dostępna jest na witrynie Spółki „Zarządzanie Procesami i Systemami" (https://giek.gkpge.pl/ZPiS), w bibliotece „Formularze".

1.2. Deklaracja, zawiera wykaz obligatoryjnych zabezpieczeń i celów ich stosowania przygotowany na podstawie Załącznika A do normy PN-ISO/IEC 27001, który, w zależności od potrzeb, może być uzupełniony.

1.3. Opracowując Deklarację należy:
   a. upewnić się, że odniesiono się do wszystkich zabezpieczeń określonych w Załączniku A (pkt 1.2),
   b. dokonać opisu zabezpieczenia (niezależnie od tego czy zabezpieczenia są wdrożone czy nie) poprzez odesłanie do właściwego aktu normatywnego / dokumentu regulującego kwestie dotyczące zabezpieczenia lub bezpośrednio opisać sposób realizacji zabezpieczenia albo
   c. uzasadnić brak potrzeby zastosowania określonego zabezpieczenia z Załącznika A.

1.4. W celu weryfikacji zgodności zabezpieczeń z wymaganiami bezpieczeństwa (celami stosowania zabezpieczeń) należy wykonywać pomiary skuteczności tych zabezpieczeń.

1.5. Ocenę skuteczności zabezpieczeń należy przeprowadzać regularnie, z ustaloną w Deklaracji częstotliwością, lecz nie rzadziej niż raz do roku.

2. ODPOWIEDZIALNOŚĆ

2.1. Kierujący komórkami organizacyjnymi Spółki wskazani w Deklaracji, jako „Komórki org. odpowiedzialne za aktualizację opisów zabezpieczeń" – grupa I (kolumna 5 formularza), są uprawnieni i zobowiązani do:
   a. identyfikacji zabezpieczeń stosowanych w JO i ich rzetelnego opisu,
   b. bieżącej aktualizacji opisów zabezpieczeń, z zastrzeżeniem pkt 2.2.

2.2. W przypadku, gdy zmiany w Deklaracji dotyczą regulacji / dokumentów obejmujących swoim zakresem całą Spółkę, aktualizację opisów zabezpieczeń w pierwszej kolejności przeprowadzają kierujący KO w Centrali (odpowiedzialni za aktualizację opisu zabezpieczenia - grupa I) i udostępniają ją na witrynie ZPiS, w bibliotece System Zarządzania Bezpieczeństwem Informacji. Następnie aktualizację Deklaracji, w oparciu o dokument przygotowany przez Centralę, przeprowadzają kierujący KO (odpowiedzialni za aktualizację opisu zabezpieczenia - grupa I) w Oddziałach.

2.3. Kierujący komórkami organizacyjnymi Centrali Spółki wskazanymi w Deklaracji jako „Komórki org. odpowiedzialne za ocenę zbioru / podzbioru zabezpieczeń" – grupa II (kolumna 6 formularza), są uprawnieni i zobowiązani do:
   a. zdefiniowania i aktualizowania mierników niezbędnych do oceny skuteczności zabezpieczeń dla całej Spółki, zgodnie z wytycznymi określonymi w pkt 3.2, oraz ich kryteriów skuteczności,
   b. określenia częstotliwości przeprowadzania ocen w Spółce,
   c. ustalenia źródeł danych niezbędnych do obliczenia mierników w Centrali (grupa III),
   d. przeprowadzania okresowych ocen skuteczności zabezpieczeń w Centrali (pkt 1.5), zgodnie z wytycznymi określonymi w pkt 3, z zastrzeżeniem pkt 2.9,
   e. występowania do kierujących KO (grupa III) o przygotowanie danych niezbędnych do obliczenia mierników,
   f. monitorowania wyników oceny w Centrali i Oddziałach oraz – w przypadku, gdy osiągnięta wartość miernika jest nieakceptowalna – podejmowania / uruchamiania właściwych działań doskonalących zapewniających zwiększenie skuteczności zabezpieczeń w Centrali lub Spółce, zgodnie z pkt 4.1.

2.4. Kierujący komórkami organizacyjnymi Oddziału Spółki wskazanymi w Deklaracji jako „Komórki org. odpowiedzialne za ocenę zbioru / podzbioru zabezpieczeń" – grupa II (kolumna 6 formularza), są uprawnieni i zobowiązani do:
   a. ustalenia źródeł danych niezbędnych do obliczenia mierników w Oddziale (grupa III),
   b. przeprowadzania okresowych ocen skuteczności zabezpieczeń w Oddziale (pkt 1.5), zgodnie z wytycznymi określonymi w pkt 3, z zastrzeżeniem pkt 2.9,
   c. występowania do kierujących KO (grupa III) o przygotowanie danych niezbędnych do obliczenia mierników,
   d. monitorowania wyników oceny w Oddziale oraz – w przypadku, gdy osiągnięta wartość miernika jest nieakceptowalna – podejmowania / uruchomiania działań doskonalących zapewniających zwiększenie skuteczności zabezpieczeń w Oddziale, zgodnie z pkt 4.1.

2.5. Kierujący komórkami organizacyjnymi Spółki wskazanymi w Deklaracji jako „Komórki org. odpowiedzialne za dostarczenie danych" – grupa III (kolumna 7 formularza), są uprawnieni i zobowiązani do niezwłocznego przygotowania i przekazania danych niezbędnych do obliczenia mierników, o które wystąpili kierujący KO z „grupy II".

2.6. Kierujących KO z „grup I i II" wskazuje, zgodnie z wytycznymi określonymi w pkt 2.6, Koordynator SZBI we współpracy z właściwymi ze względu na zakres działania Administratorami Merytorycznymi SZBI, bazując na przykładzie Deklaracji przygotowanym przez Administratora Funkcjonalnego ZSZ i udostępnionym w portalu Spółki na witrynie ZPiS, w bibliotece „System Zarządzania Bezpieczeństwem Informacji i Ciągłością Biznesową".

2.7. Kierujących KO z „grupy III" wskazują kierujący KO z „grupy II", odpowiednio do źródeł danych potrzebnych do przeprowadzenia oceny skuteczności zabezpieczeń i obliczenia mierników.

2.8. Jako odpowiedzialnych za aktualizację opisów zabezpieczeń (grupa I) należy wskazywać komórki organizacyjne będące autorami regulacji / dokumentu, natomiast jako odpowiedzialnych za zbiór / podzbiór zabezpieczeń (grupa II) – właściwych Administratorów Merytorycznych SZBI lub kierujących KO właściwych merytorycznie dla zakresu danego zbioru / podzbioru zabezpieczeń lub jego kluczowych elementów.

2.9. Ocenę skuteczności zabezpieczeń w JO dla obszarów ICT i zakupów dokonują właściwe komórki merytoryczne Centrali.

2.10. Deklaracja w wersji papierowej wymaga zatwierdzenia:

a. dla Centrali – zatwierdza Prezes Zarządu Spółki po wcześniejszym uzyskaniu akceptacji merytorycznej przez kierujących KO z „grupy II" oraz akceptacji Administratora Funkcjonalnego ZSZ i Pełnomocnika ds. ZSZ,

b. dla Oddziału – zatwierdza Dyrektor Oddziału po wcześniejszym uzyskaniu akceptacji merytorycznej przez kierujących KO z „grupy II" oraz akceptacji Koordynatora SZBI.

2.11. Deklaracja przygotowana do zatwierdzenia powinna obejmować kolumny od 1 do 9 formularza.

3. METODA OCENY SKUTECZNOŚCI ZABEZPIECZEŃ

3.1. Do oceny skuteczności zabezpieczeń stosowana jest metoda ilościowo-jakościowa, polegająca na określeniu parametrów liczbowych charakteryzujących badane zabezpieczenie, a następnie klasyfikacji danych (wartości miernika) według określonych kryteriów (przypisaniu wartości miernika do danego poziomu, o którym mowa w pkt 4).

3.2. Mierniki stosowane w ocenie powinny:

a. być adekwatne do celów stosowania poszczególnych zbiorów / podzbiorów zabezpieczeń,

b. posiadać wiarygodne i dostępne źródło danych,

w związku z tym, dla każdego zbioru / podzbioru zabezpieczeń należy opracować indywidualne mierniki.

3.3. W celu przeprowadzenia oceny skuteczności należy podjąć następujące działania:

a. zweryfikować dane źródłowe otrzymane z komórek odpowiedzialnych za ich przygotowanie,

b. obliczyć wartość miernika zdefiniowanego w Deklaracji w kolumnie 12 „Wartość miernika", podając przy tym w poprzedzającej kolumnie wartości liczbowe składników miernika,

c. w zależności od otrzymanej wartości miernika, przypisać do zabezpieczenia odpowiedni poziom skuteczności (kolumna 14 „Poziom skuteczności").

3.4. W przypadku, gdy ocena skuteczności zabezpieczeń przeprowadzania jest:

a. dla potrzeb Przeglądu procesów i systemów zarządzania – należy przygotować informację o jej wynikach i kierunkach zmian (z uwzględnieniem wyników poprzednich ocen) oraz dodatkowo, jeśli wynik oceny odpowiada poziomowi „nieakceptowalnemu" (pkt 4.1), podać przyczyny takiego stanu rzeczy oraz przedłożyć stosowne wnioski, zgodnie z procedurą dotyczącą Przeglądu procesów i systemów zarządzania w PGE GiEK S.A.,

b. z częstotliwością większą niż na potrzeby Przeglądu – należy, w zależności od uzyskanego poziomu skuteczności zabezpieczeń, wdrożyć odpowiedni tryb postępowania określony w pkt 4.

4. POZIOMY SKUTECZNOŚCI ZABEZPIECZEŃ

4.1. Poziom nieakceptowalny

W przypadku, gdy otrzymana wartość miernika dla zabezpieczenia odpowiada poziomowi nieakceptowalnemu, kierujący komórką organizacyjną odpowiedzialną za zbiór / podzbiór zabezpieczeń (grupa II) zobowiązany jest niezwłocznie uruchomić działania korygujące zgodnie z odrębną regulacją dotyczącą poprawy funkcjonowania procesów i systemów zarządzania w PGE GiEK S.A.

4.2. Poziom akceptowalny

Wartość miernika odpowiadająca poziomowi akceptowalnemu nie wymaga podjęcia szczególnych działań, poza bieżącym monitorowaniem zasobów w odniesieniu, do których dane zabezpieczenie ma zastosowanie, a w razie potrzeby do uruchomienia działań doskonalących zgodnie z odrębną regulacją dotyczącą poprawy funkcjonowania procesów i systemów zarządzania w PGE GiEK S.A.