

PROCEDURA OGÓLNA BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

PROG 00039/B

Sygn.: PGE/CENT/DSIT/4.07

Data zatwierdzenia: 2022/02/21

Obowiązuje od: 2022/03/09

I CEL I ZAKRES

- 1.1 Celem Procedury Ogólnej bezpieczeństwa teleinformatycznego jest zapewnienie spójnych w GK PGE zasad eksploatacji Systemów Teleinformatycznych i Sieci Korporacyjnej, zapewniających bezpieczeństwo Systemów Teleinformatycznych, minimalizacja ryzyka nieautoryzowanego Dostępu lub awarii oraz wykrywanie nieautoryzowanych działań związanych z przetwarzaniem informacji.
- 1.2 Procedura obejmuje swoim zakresem zasady bezpieczeństwa teleinformatycznego dotyczące wszystkich informacji w Spółce przetwarzanych w Systemach Teleinformatycznych.
- 1.3 Procedura reguluje:
 - a. zasady zarządzania Systemami Teleinformatycznymi w GK PGE,
 - b. zasady ochrony Danych zawartych w Systemach Teleinformatycznych w GK PGE,
 - c. prawa i obowiązki Menedżera Danych i Administratora,
 - d. zasady nadawania uprawnień i Dostępów do Systemów Teleinformatycznych,
 - e. zasady zarządzania kontami i Dostępami do Systemów Teleinformatycznych,
 - f. zasady udostępniania Danych z Systemów Teleinformatycznych,
 - g. zasady zarządzania Nośnikami Informacji,
 - h. zasady monitorowania Systemów Teleinformatycznych pod kątem bezpieczeństwa,
 - i. obowiązki Użytkownika Systemów Teleinformatycznych.

II ODPOWIEDZIALNOŚĆ

- 2.1 Za stosowanie niniejszej Procedury odpowiedzialne są:
 - a. Spółki z GK PGE, których Pracownicy wykorzystują Zasoby udostępniane i zarządzane przez CUW ICT,
 - b. wszystkie osoby pełniące role opisane niniejszą Procedurą,
 - c. osoby wykorzystujące sprzęt IT będący własnością CUW ICT,
 - d. CIO w zakresie aktualizacji Procedury.
- 2.2 Spółki są zobowiązane do zapewnienia spójności z Procedurą dokumentów spółek od siebie zależnych, które nie są bezpośrednio zobowiązane do stosowania procedury.

III DOKUMENTY POWIĄZANE

- 3.1 *REGL 00082 Polityka Organizacji Teleinformatyki w Grupie Kapitałowej PGE*
- 3.2 *PROG 00035 Procedura Ogólna – Wytyczne w zakresie ochrony danych osobowych w GK PGE*
- 3.3 *PROG 00037 Procedura Ogólna – Wytyczne w zakresie Klasyfikacji i ochrony informacji w Grupie Kapitałowej PGE*
- 3.4 *PROG 00099 Procedura Ogólna – zarządzania Licencjami oprogramowania w Grupie Kapitałowej PGE*
- 3.5 *PROG 00103 Procedura Ogólna – Korzystanie z Zasobów Teleinformatycznych (ICT) w GK PGE*
- 3.6 *PROG 00105 Procedura Ogólna Zarządzania Użytkownikami Końcowymi w SAP w Grupie Kapitałowej PGE*
- 3.7 *PROG 00116 Procedura Ogólna Zarządzania Incydentami Cyberbezpieczeństwa w GK PGE*
- 3.8 *Umowy SLA zawarte pomiędzy Spółkami GK PGE a CUW ICT określające zasady obsługi ICT*
- 3.9 *DIN 66399 - Norma regulująca wymogi i obowiązki w zakresie bezpiecznego niszczenia dokumentów i nośników danych*
- 3.10 *ISO/IEC 27001 - Norma międzynarodowa standaryzująca systemy zarządzania bezpieczeństwem informacji*

IV ZAŁĄCZNIKI

- 4.1 [Załącznik 1](#) Mierniki zabezpieczeń
- 4.2 [Załącznik 2](#) Wymagania RODO do Systemu Teleinformatycznego

V SKRÓTY I DEFINICJE

[PGE, PGE S.A.:](#)

[Dokument Systemu Zarządzania / Dokumenty Systemu Zarządzania \(DSZ\) Komórka organizacyjna / komórka; Nośnik Informacji / Nośnik; Segment; Spółka GK PGE, Spółka, Spółki; Spółka GK PGE bezpośrednio zależna od PGE](#)

[Skróty użyte na potrzeby niniejszego dokumentu:](#)

CRL	- lista unieważnionych certyfikatów (ang. Certificate Revocation List)
DC	- Komórka organizacyjna w CUW IT obsługująca obszar Cyberbezpieczeństwa w GK PGE
EOG	- Europejski Obszar Gospodarczy
IAM	- System Zarządzania Tożsamością (ang. Identity and Access Management)
ICT/IT	- (ang. Information and Communication Technologies), Teleinformatyka

IPSEC	- zbiór protokołów służących implementacji bezpiecznych połączeń oraz wymiany kluczy szyfrowania pomiędzy komputerami
MAC	- kod Uwierzytelnienia wiadomości – główne zastosowanie to zapewnienie Integralności i Autentyczności w trakcie szyfrowania danych(ang. Message Authentication Code)
OCSP	- usługa weryfikacji statusu certyfikatu on-line (ang. On-line Certificate Status Protocol)
ODO	- Ochrona Danych Osobowych
PGE, PGE S.A.	- PGE Polska Grupa Energetyczna S.A.
PIM	- System zarządzania uprawnieniami uprzywilejowanymi (ang. Privileged Identity Management)
PIN	- Indywidualny kod wymagany do Uwierzytelnienia Użytkownika (ang. Personal Identity Number)
PKI	- Infrastruktura Klucza Publicznego (ang. Public Key Infrastructure)
RODO	- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
SIEM	- Rodzaj Systemów do zarządzania informacją i zdarzeniami bezpieczeństwa
SNMP	- Rodzina protokołów sieciowych wykorzystywanych do zarządzania urządzeniami
SOC	- Wyodrębniona Jednostka organizacyjna zajmująca się Cyberbezpieczeństwem
SSH	- Standard protokołów komunikacyjnych używanych w sieciach komputerowych (ang. Secure Shell)
SSL	- Protokół sieciowy używany do bezpiecznych połączeń internetowych
ZZL	- Zarządzanie Zasobami Ludzkim

Definicje pojęć użyte na potrzeby niniejszego dokumentu:

- 5.1 **Active Directory (AD)** – korporacyjna usługa katalogowa, w której określone są parametry oraz Dane o zasobach dotyczących domeny gkpge.pl.
- 5.2 **Administrator Danych Osobowych (ADO)** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania Danych Osobowych (Rozporządzenie o Ochronie Danych Osobowych RODO Art. 4 pkt 7). W przypadku Spółek wchodzących w skład Grupy Kapitałowej Administratorem Danych Osobowych jest samodzielnie każda Spółka GK PGE.
- 5.3 **Administrator Techniczny / Administrator** – Pracownik CUW ICT lub Osoba Trzecia posiadająca odpowiedni poziom uprawnień i odpowiedzialności za System Teleinformatyczny lub element infrastruktury teleinformatycznej. Osoba ta zarządza i sprawuje nadzór nad Systemem Teleinformatycznym lub innym elementem infrastruktury teleinformatycznej od strony technicznej. Za pisemną zgodą CIO – w ramach odstępstwa od Procedury – Administratorem może zostać Pracownik GK PGE niebędący Pracownikiem CUW ICT pod warunkiem realizowania przez niego wszystkich zadań wynikających z Procedury a przypisanych do roli Administratora.
- 5.4 **Anonimizacja** – metoda usunięcia w sposób nieodwracalny informacji umożliwiających identyfikację konkretnej osoby fizycznej, z zachowaniem pozostałych informacji, które na identyfikację osoby nie pozwalają, np. poprzez zacernienie w tekście dokumentu informacji pozwalających na identyfikację osoby, wykasowanie tychże informacji z bazy danych lub zastąpienie ich wielokropkiem lub ciągiem określonych znaków.
- 5.5 **Autentyczność** – właściwość potwierdzająca, że podmiot jest tym, za kogo się podaje.
- 5.6 **Baza CMDB, (CMDB)** – baza prowadzona w wersji elektronicznej, w dedykowanym narzędziu informatycznym zawierająca informacje o Usługach ICT w GK PGE, Zasobach ICT, ich elementach składowych oraz relacjach między nimi.
- 5.7 **Bezpieczeństwo Informacji** – zapewnienie Poufności, Integralności i Dostępności informacji dla przetwarzanych informacji, czyli zabezpieczanie jej przed nieautoryzowanym Dostępem, zmianą, utratą, uszkodzeniem, zniszczeniem lub zatajeniem.
- 5.8 **Bezpieczna Koperta, Koperta** – koperta zapewniająca Poufność przechowywanej informacji, pozwalająca stwierdzić czy została otwarta w sposób nieautoryzowany, posiadająca unikalny numer seryjny nadawany przez producenta.
- 5.9 **Centrum Usług Wspólnych ICT, CUW ICT** – podmiot, którego celem jest świadczenie Usług ICT na rzecz pozostałych Spółek GK PGE.
- 5.10 **Certyfikat** – zbiór danych zawierający, co najmniej: nazwę wystawcy certyfikatu, identyfikator Użytkownika, Klucz publiczny Użytkownika, okres ważności certyfikatu i numer seryjny certyfikatu, podpisany przez Urząd Certyfikacji GK PGE, który w ten sposób poświadcza tożsamość Użytkownika i że Klucz publiczny zamieszczony w Certyfikacie rzeczywiście należy do tego Użytkownika, Urządzenia lub Serwera.
- 5.11 **Chief Information Officer (CIO)** – rola pełniona przez Kierującego komórką właściwą ds. strategii ICT GK PGE. Odpowiada za operacyjne zarządzanie Funkcją ICT w GK PGE.

- 5.12 **CMDB** – System zarządzania konfiguracją Systemów Teleinformatycznych utrzymywany przez CUW ICT.
- 5.13 **Cyberbezpieczeństwo** – odporność systemów informacyjnych na działania naruszające Poufność, Integralność, Dostępność i Autentyczność przetwarzanych Danych lub związanych z nimi Usług oferowanych przez te Systemy (definicja na podstawie Ustawy o Krajowym Systemie Cyberbezpieczeństwa).
- 5.14 **Dane** – danymi (ang. data) jest wszystko to, co jest lub może być przetwarzane umysłowo lub komputerowo. W szczególności Danymi są informacje przetwarzane w Systemach Teleinformatycznych lub przechowywane na Nośnikach Informacji wraz z informacjami konfiguracyjnymi Zasobów ICT.
- 5.15 **Dane Osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której Dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
- 5.16 **Dokument Systemu Zarządzania / Dokumenty Systemu Zarządzania (DSZ)** – regulacja/-e dotyczące Grupy PGE wskazane w Art. 25 Kodeksu Grupy PGE, wiążące dla Spółki wchodzącej w skład Grupy PGE w związku z przyjęciem Kodeksu Grupy PGE; wykorzystywane przy prowadzeniu działalności Spółki, służące komunikowaniu wymagań i zasad postępowania przy realizacji procesu/-ów oraz zapewniające ich jednolitość i spójność. W szczególności dokument taki:
- a. określa i ustala zasady organizacji i postępowania w procesie, Spółce / Spółkach,
 - b. pozwala nadzorować procesy,
 - c. określa zakres obowiązków i zadań w procesach, Spółce / Spółkach,
 - d. zawiera uzgodnienia wymagań między komórkami organizacyjnymi,
 - e. zawiera informacje o zaplanowanych działaniach lub o planowanych wynikach.
- W Grupie PGE do zbioru Dokumentów Systemu Zarządzania należą: Regulaminy i Polityki (REGL), Procedury Ogólne (PROG), Procedury (PROC), Instrukcje (INST) oraz Karty Procesów i Mapy Procesów.
- 5.17 **Dostęp** – mechanizm Dostępu do Danych w Systemach Teleinformatycznych składający się z Konta Użytkownika oraz odpowiedniego poziomu uprawnień.
- 5.18 **Dostęp Podstawowy** – Dostęp do podstawowych Zasobów ICT GK PGE wymaganych do realizowania przez Użytkownika podstawowych zadań służbowych. W szczególności w ramach Dostępu Podstawowego nadawane są Dostępy do: korporacyjnej domeny imiennej skrzynki poczty elektronicznej, usług sieciowych, Internetu oraz Danych publikowanych dla Spółki. Zakres Dostępu Podstawowego może być różny dla poszczególnych Spółek i wynika z zapisów Umowy SLA zawartej pomiędzy Spółką a CUW ICT. W ramach jednej Jednostki organizacyjnej mogą być zdefiniowane różne Dostępy Podstawowe w zależności od przypadku użycia: Pracownik, członek Organów Spółki, Osoba Trzecia.
- 5.19 **Dostępność** – właściwość bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu.
- 5.20 **Dziennik Systemu Teleinformatycznego** – opis działań Administratora, które wynikają z bezpiecznej eksploatacji Systemu (co najmniej: zakładanie i blokowanie Kont, nadawanie, modyfikacja i usuwanie uprawnień, czynności konserwacyjne, wykonywanie kopii zapasowych), lub z Incydentów Cyberbezpieczeństwa.
- 5.21 **Funkcja ICT** – rozumiana jest jako całość aktywów organizacji, procesów, praktyk, budżetów, wchodzących w skład lub będących własnością Grupy Kapitałowej PGE, które składają się na planowanie, realizację i utrzymanie wszystkich usług teleinformatycznych w Grupie Kapitałowej PGE.
- 5.22 **Grupa Kapitałowa PGE (GK lub GK PGE)** – PGE oraz Spółki względem których PGE posiada status spółki dominującej w rozumieniu artykułu 4 § 1 pkt 4 Kodeksu spółek handlowych.
- 5.23 **Grupa Profili Zdalnego dostępu / Grupa Profili VPN** – zbiór Profili Zdalnego Dostępu sumujący uprawnienia na poziomie sieciowym w ramach Zdalnego Dostępu. Grupa Profili VPN definiowana jest dla jednej lub wielu Jednostek organizacyjnych w zależności od potrzeby granulacji.
- 5.24 **Hasło** – ciąg znaków, który służy do Uwierzytelniania w Systemie Teleinformatycznym.
- 5.25 **Identyfikator Subskrybenta** – informacja zamieszczona w Certyfikacie, pozwalająca na jednoznaczną identyfikację Subskrybenta w ramach zbioru Subskrybentów obsługiwanych przez Urząd Certyfikacji GK PGE.
- 5.26 **Identyfikator w Systemie Teleinformatycznym / Identyfikator** – unikalny ciąg znaków jednoznacznie identyfikujący w Systemie Teleinformatycznym Użytkownika lub inny System Teleinformatyczny.
- 5.27 **Identyfikator EK** – Identyfikator elementu konfiguracji w systemie CMDB.
- 5.28 **Incydent Cyberbezpieczeństwa** – zdarzenie, które ma lub może mieć niekorzystny wpływ na Cyberbezpieczeństwo w tym na Bezpieczeństwo Informacji.
- 5.29 **Integralność** – właściwość polegająca na zapewnieniu dokładności i kompletności informacji.

- 5.30 **Jednostka organizacyjna** – organizacja powołana do wykonywania określonych części zadań w obszarze/ Segmencie, mająca ustalone miejsce w jego/jej strukturze organizacyjnej. Jednostką organizacyjną może być Spółka lub Oddział.
- 5.31 **Kierownik Komórki organizacyjnej / Kierujący komórką** – osoba kierująca Komórką organizacyjną (dyrektor lub zastępca dyrektora).
- 5.32 **Kierujący komórką ds. DC** – osoba nadzorująca obszar Cyberbezpieczeństwa w CUW ICT.
- 5.33 **Kierujący komórką ds. ICT** – osoba nadzorująca obszar ICT w Spółce oraz odpowiedzialna za zamawianie i rozliczanie Usług ICT.
- 5.34 **Kierujący komórką ds. ZZL** – osoba nadzorująca obszar ZZL w Spółce.
- 5.35 **Kierujący ODO** – osoba umocowana w Jednostce organizacyjnej do nadzoru ochrony Danych Osobowych oraz do kontaktu w kwestiach dotyczących tego obszaru. W spółkach może być to stanowisko łączone z funkcją Inspektora ochrony danych w rozumieniu RODO lub jego odpowiednika.
- 5.36 **Klucz prywatny** – klucz kryptograficzny do wyłącznego użytku Subskrybenta, służący do składania podpisu lub odszyfrowania informacji.
- 5.37 **Klucz publiczny** – klucz kryptograficzny publicznie znany, powiązany z Kluczem prywatnym, który jest stosowany do weryfikowania podpisu lub szyfrowania informacji.
- 5.38 **Kodeks Grupy PGE** – akt wewnątrzorganizacyjny regulujący stosunki wewnętrzne w Grupie PGE, określający tworzenie, organizację i funkcjonowanie Grupy PGE.
- 5.39 **Komórka organizacyjna / Komórka** – jedno - lub wieloosobowe ciało powołane do wykonywania określonych części zadań w Jednostce organizacyjnej, mające ustalone miejsce w jej strukturze organizacyjnej. Komórką może być: departament, biuro, zespół, wydział, dział, sekcja lub inna komórka wewnętrzna w Spółce lub Oddziale Spółki.
- 5.40 **Komputer Biurowy** – komputer stacjonarny, komputer przenośny (laptop), umożliwiający Przetwarzanie Danych wraz z przynależnymi akcesoriami.
- 5.41 **Konto** – obiekt składający się z Loginu i Hasła umożliwiający Dostęp do wybranych Zasobów ICT. Wyróżnia się następujące rodzaje Kont: Konto Podstawowe, Konto Dodatkowe, Konto Techniczne.
- 5.42 **Konto Dodatkowe** – imienne Konto Użytkownika dedykowane do realizacji zadań wykraczających poza funkcje realizowane na Koncie Podstawowym (np. Konto administracyjne, deweloperskie, testowe). Konto Dodatkowe przeznaczone jest do obsługi technicznej Systemu i posiada wyższe uprawnienia w Systemie niż Konto Podstawowe.
- 5.43 **Konto Podstawowe** – imienne Konto Użytkownika przeznaczone do realizacji podstawowych, biurowych zadań służbowych poprzez zapewniające temu Użytkownikowi, Dostępu Podstawowego do Zasobów ICT GK PGE.
- 5.44 **Konto Techniczne** – Konto nieimienne w tym współdzielone, wykorzystywane do ściśle zdefiniowanych zadań technicznych i biznesowych, z którego korzysta jeden lub wielu Użytkowników, lub System.
- 5.45 **Kontraktor** – Osoba, niebędącą Osobą Trzecią, realizująca zadania na rzecz Spółki na innej podstawie niż umowa o pracę.
- 5.46 **Lista Akceptujących** – Lista przedstawicieli Spółek uprawnionych do akceptacji Wniosków z uwzględnieniem rodzaju Wniosku i poziomu akceptacji.
- 5.47 **Lista CRL** – plik zawierający informacje o zawieszeniu lub unieważnieniu Certyfikatów.
- 5.48 **Lista Oprogramowania** – Lista Oprogramowania, które zostało zabronione lub dopuszczone do stosowania w GK PGE. Listy ustala oraz publikuje CUW ICT.
- 5.49 **Login** – Identyfikator Konta w Systemie Teleinformatycznym.
- 5.50 **Menadżer Danych / Menadżer Dostępu** – osoba sprawująca nadzór nad Danymi w Systemie Teleinformatycznym, oraz Dostępem do Danych będących własnością Spółki.
- 5.51 **Menadżer Konta** – osoba merytoryczna wskazana w atrybutach Konta, odpowiadająca za to Konto. W przypadku:
 - a. Pracownika jest to bezpośredni Przełożony,
 - b. Kontraktora - wskazany Pracownik,
 - c. członka Organu Spółki – osoba pełniąca funkcję lub rolę Kierującego komórką właściwą ds. obsługi
 - d. Organów Spółki,
 - e. Osoby Trzeciej – Opiekun Osoby Trzeciej,
 - f. Konta Dodatkowego Użytkownika – odpowiednio Użytkownik jeśli jest Pracownikiem, w pozostałych przypadkach Menadżer Konta Podstawowego,
 - g. Konta Technicznego - upoważniony Pracownik Spółki.

- 5.52 **Nośnik Informacji / Nośnik** – wszelkiego rodzaju Nośniki Danych, używane w procesie przetwarzania informacji, w szczególności dyski twarde, płyty CD/DVD/BR, taśmy DLT/DDS, pamięci przenośne, dyski magneto-optyczne.
- 5.53 **Opiekun Osoby Trzeciej** – Kierownik Komórki organizacyjnej, w ramach której Osoba Trzecia realizuje swoje zadania lub wyznaczony przez niego Pracownik.
- 5.54 **Organy Spółki** – członkowie zarządu Spółki.
- 5.55 **Osoba Trzecia** – osoba udostępniona przez dostawcę, która nie może posiadać Dostępów odpowiadających Pracownikowi a realizująca określone zadania na rzecz Spółki. Osoba Trzecia to również: praktykanci, stażyści, wolontariusze i inne osoby realizujące zadania na rzecz Spółki, nie będące Kontraktorem.
- 5.56 **PGE-CERT** – (Computer Security Incident Response Team) Komórka organizacyjna w strukturach GK PGE, świadcząca usługi monitorowania Cyberbezpieczeństwa i obsługi Incydentów Cyberbezpieczeństwa.
- 5.57 **Podatność** – właściwość Systemu informacyjnego, która może być wykorzystana przez zagrożenie Cyberbezpieczeństwa.
- 5.58 **Podmiot Przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza powierzone Dane Osobowe w imieniu ADO, w sposób zapewniający wystarczające gwarancje wdrożenia odpowiednich środków ochrony Danych Osobowych, by przetwarzanie spełniało wymogi RODO i chroniło prawa jednostki.
- 5.59 **Poufność** – właściwość, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.
- 5.60 **Pracodawca** – Spółka lub Oddział Spółki zatrudniający Pracowników w ramach stosunku pracy reprezentowany przez Zarząd lub inne osoby uprawnione do dokonywania w imieniu Pracodawcy czynności w sprawach z zakresu prawa pracy, na podstawie pełnomocnictw lub innych wewnętrznych aktów prawnych obowiązujących w Spółce.
- 5.61 **Pracownik** – osoba, z którą Pracodawca nawiązał stosunek pracy w rozumieniu art. 22 Kodeksu pracy, nie obejmuje osób wykonujących pracę na innej podstawie niż stosunek pracy.
- 5.62 **Procedura** – PROG 00039 Procedura Ogólna Bezpieczeństwa Teleinformatycznego, niniejszy dokument.
- 5.63 **Profil Zdalnego dostępu / Profil VPN** – zestaw uprawnień na poziomie sieciowym umożliwiający dostęp do wybranej Usługi i/lub Systemu w Sieci Korporacyjnej GK PGE z sieci publicznej Internet po zestawieniu Zdalnego Dostępu.
- 5.64 **Profil Internetowy** – zestaw uprawnień na poziomie sieciowym umożliwiający Dostęp do wybranych witryn sieci publicznej Internet z Sieci Korporacyjnej GK PGE.
- 5.65 **Przełożony** – osoba zajmująca stanowisko, którego miejsce w strukturze organizacyjnej Spółki oraz powiązany z nim zakres obowiązków i wynikająca z niego odpowiedzialność wymaga i umożliwia wydanie poleceń służbowych oraz egzekwowanie ich wykonania od Pracowników i Kontraktorów w wyznaczonym obszarze struktury organizacyjnej Spółki.
- 5.66 **Pseudonimizacja** – metoda ukrycia informacji umożliwiających identyfikację konkretnej osoby fizycznej polegająca na zastąpieniu jednego atrybutu w zapisie innym atrybutem, np. poprzez zaszyfrowanie tychże kluczem tajnym, skrócenie ich nazwy, lub też zastąpienie imienia i nazwiska liczbą, pseudonimem lub inicjałem, przy jednoczesnym przechowywaniu ukrytych informacji osobno w sposób uniemożliwiający do nich Dostęp osobom nieposiadającym do tego uprawnień.
- 5.67 **Rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
- 5.68 **Segment** – grupa Jednostek Biznesowych wyodrębniona w ramach GK PGE do realizacji działań w obszarze wskazanej technologii lub rynku na którym działa, stanowiąca centrum kompetencyjne w tym zakresie; zastępuje pojęcie „Linii Biznesowej”, o którym mowa w Kodeksie Grupy PGE.
- 5.69 **Service Desk (SD)** – zespół osób w ramach CUW ICT przyjmujący i realizujący obsługę zgłoszeń z zakresu wszelkich zdarzeń związanych z informatyką lub telekomunikacją.
- 5.70 **Sieć Korporacyjna** – urządzenia komputerowe, oprogramowanie i okablowanie wraz z urządzeniami sieciowymi, umożliwiające gromadzenie, przetwarzanie oraz wymianę Danych w tym sieć rozległa geograficznie, obejmująca swoim zasięgiem lokalizacje Spółek i Oddziałów na terenie kraju, będąca własnością bądź wykorzystywana przez GK PGE.
- 5.71 **Spółka GK PGE, Spółka, Spółki** – podmiot / podmioty prawa handlowego wchodzące w skład Grupy Kapitałowej PGE.
- 5.72 **Spółka GK PGE bezpośrednio zależna od PGE** – Spółka w stosunku do której PGE S.A. jest spółką z większościowym bezpośrednim zaangażowaniem kapitałowym, tj. posiada 50% i więcej udziałów lub akcji w kapitale zakładowym takiej spółki.

- 5.73 **Subskrybent** – osoba fizyczna, która jest Użytkownikiem usług certyfikacyjnych dostarczanych przez urzędy certyfikacji i której imię, nazwisko lub nazwa została umieszczona w Certyfikacie.
- 5.74 **System Monitorowania Usług (SMU)** – System służący do monitorowania Dostępności Usług ICT, współpracujący z Systemem Obsługi Zgłoszeń w zakresie wyliczania poziomu realizacji parametru Dostępności Usługi.
- 5.75 **System Obsługi Zgłoszeń (SOZ)** – System informatyczny służący m.in. do wsparcia Procesów zarządzania Usługami ICT, obsługi zgłoszeń i Wniosków dostępny pod adresem sd.gkpge.pl.
- 5.76 **System Teleinformatyczny / System** – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie Danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego wraz z przetwarzanymi w nim Danymi w postaci elektronicznej.
- 5.77 **System Zarządzania tożsamością (IAM)** – System nadzorujący zarządzanie prawami dostępu do Zasobów ICT.
- 5.78 **Systemy ICT** – Systemy realizujące Funkcje ICT nie będące Systemami OT, utrzymywane i rozwijane przez CUW ICT, wspierające realizację celów biznesowych określanych przez Spółkę.
- 5.79 **Systemy OT (ang. Operational Technology)** – Systemy Teleinformatyczne, które realizują w Spółce funkcje zarządzania, sterowania, regulacji, pomiaru, monitoringu, bezpieczeństwa (lub kilku tych funkcji łącznie) dla procesów technologicznych i przemysłowych realizowanych w ramach infrastruktury przemysłowej GK PGE wraz z Systemami teletransmisji, niezbędnymi do ich działania.
- 5.80 **Teleinformatyka (ICT)** – dziedzina łącząca informatykę, telekomunikację oraz narzędzia i inne technologie związane z przetwarzaniem informacji. Nie obejmuje rozwiązań związanych z teleinformatyką przemysłową i automatyką. W sytuacji wątpliwej w zakresie granicy ICT oraz teleinformatyki przemysłowej i automatyki, bądź też konieczności wyłączenia fragmentu obszaru z definicji Usługi ICT stosowne decyzje będzie podejmował Komitet Teleinformatyki.
- 5.81 **Umowa SLA** – Umowa zawarta pomiędzy Spółką GK PGE a CUW ICT określająca zasady współpracy w zakresie obsługi ICT.
- 5.82 **Urząd Certyfikacji GK PGE** – komponent funkcjonalny Systemu PKI, obsługiwany przez zaufane role, który świadczy usługi wystawiania, dystrybucji, przechowywania, weryfikacji i unieważniania Certyfikatów cyfrowych z wykorzystaniem kryptografii Klucza publicznego. Urząd Certyfikacji GK PGE jest udostępniony i utrzymywany przez CUW ICT.
- 5.83 **Urządzenie Mobilne** – osobiste urządzenie typu telefon komórkowy, smartfon, tablet, PDA zwykle wyposażone w obsługę sieci GSM, WiFi, Bluetooth wykorzystywane w ramach realizacji zadań biurowych. Komputer przenośny (laptop) nie jest traktowany jako Urządzenie Mobilne.
- 5.84 **Usługa ICT / Usługa** – usługa świadczona z wykorzystaniem technologii teleinformatycznych, ludzi i procesów. Usługa ICT zorientowana jest na Spółkę i bezpośrednio wspiera procesy biznesowe. Docelowy poziom świadczenia usługi powinien być zdefiniowany w Umowie SLA. Usługa ICT może obejmować także modyfikacje oraz rozszerzenia rozwiązań ICT oraz prace analityczne.
- 5.85 **Uwierzytelnienie** – sprawdzenie i potwierdzenie zadeklarowanej tożsamości.
- 5.86 **Użytkownik** – osoba uprawniona do korzystania z Systemu Teleinformatycznego; Użytkownikami mogą być członkowie Organów Spółki, Pracownicy, Kontraktorzy oraz Osoby Trzecie.
- 5.87 **Właściciel Zasobu ICT** – funkcja przypisana do osoby merytorycznie odpowiedzialnej za rozwój Zasobu ICT w Spółce.
- 5.88 **Wniosek** – formalne wystąpienie o podjęcie określonych działań lub wykonanie określonej czynności w Usłudze ICT (także w zakresie nadania, modyfikacji lub odebrania uprawnień do Usługi).
- 5.89 **Zasoby Teleinformatyczne, Zasoby ICT, Zasoby** – Systemy ICT wraz ze sprzętem komputerowym oraz infrastrukturą ICT Sieci Korporacyjnej, itp., Dane i osoby je przetwarzające oraz inne elementy mające wpływ na bezpieczeństwo tych Danych.
- 5.90 **Zaufane Źródło tożsamości o Pracowniku / Źródło tożsamości** – System dedykowany do obsługi obszaru kadrowego (np. SAP ZKL, Symfonia).
- 5.91 **Zdalny Dostęp (VPN)** – (ang. Virtual Private Network), wirtualna sieć prywatna, tunel między dwoma punktami sieci (np. laptopem, a siecią wewnętrzną GK PGE), który umożliwia bezpieczną transmisję danych, np. poprzez sieć publiczną Internet. Zdalny Dostęp umożliwia uprawnionym Użytkownikom szybki, łatwy i bezpieczny dostęp do Systemów Teleinformatycznych znajdujących się w Sieci Korporacyjnej spoza ich miejsca pracy.

VI REALIZACJA

6.1 POSTANOWIENIA OGÓLNE

- 6.1.1 Procedura Ogólna bezpieczeństwa teleinformatycznego stanowi zbiór zasad niezbędnych do zapewnienia właściwej ochrony Danych przetwarzanych w Systemach Teleinformatycznych wykorzystywanych w Spółce, w szczególności są to:
- a. zasady i procedury opisujące sposób zarządzania Systemami, Siecią Korporacyjną (ochronę przed złośliwym oprogramowaniem, bezpieczeństwo sieci, Bezpieczeństwo Informacji, kopie zapasowe, monitorowanie Systemów i sieci),
 - b. zasady kontroli Dostępu do Danych przetwarzanych w Systemach (zarządzanie uprawnieniami, polityka Haseł, Zdalny Dostęp do Sieci Korporacyjnej).
- 6.1.2 Procedura określa wymagania bezpieczeństwa w stosunku do Systemów oraz Zasobów ICT.
- 6.1.3 Systemy mogą być wykorzystywane przez Użytkowników wyłącznie w celach, dla których zostały im udostępnione i w zakresie przydzielonych uprawnień oraz zgodnie z interesem Spółki, obowiązującymi przepisami prawa powszechnego i wewnętrznymi aktami normatywnymi.
- 6.1.4 Szczegółowe obowiązki Użytkowników Systemów Teleinformatycznych, obowiązujące także Użytkowników o rozszerzonych uprawnieniach i obowiązkach, reguluje *PROG 00103 Procedura Ogólna Korzystanie z Zasobów Teleinformatycznych (ICT) w GK PGE*.

6.2 ZARZĄDZANIE SYSTEMAMI TELEINFORMATYCZNYMI

- 6.2.1 Każda Spółka odpowiada za zarządzanie Systemami Teleinformatycznymi i Zasobami ICT w zakresie ról i obowiązków, jakie pełni dla danego Systemu.
- 6.2.2 Każdy z Zasobów ICT, będący własnością Spółki lub eksploatowany w Spółce, w tym również Systemy Teleinformatyczne będące środowiskami rozwojowymi lub testowymi ma powołanego Administratora. Administratorzy zapewniają obsługę techniczną dla powierzonego im Zasobu ICT, w celu zapewnienia obsługi Systemu na wymaganym poziomie..
- 6.2.3 Administrator nie może wykorzystywać nadanych uprawnień w Systemie do wykonywania zadań niezwiązanych z obowiązkami służbowymi lub w zakresie przekraczającym te obowiązki.
- 6.2.4 Administrator nie może ujawniać osobom nieuprawnionym jakichkolwiek informacji związanych z budową Systemu Teleinformatycznego i zastosowanymi w nim zabezpieczeniami lub podejmować czynności mogących prowadzić do ich ujawnienia.
- 6.2.5 Administrator Systemu zapewnia właściwą ochronę Systemu zgodnie z dokumentacją bezpieczeństwa Zasobu ICT, a w szczególności odpowiada za:
- a. utrzymanie Systemu w stanie bezpiecznej, nieprzerwanej i bezawaryjnej pracy,
 - b. opracowanie, wdrożenie i przestrzeganie procedur awaryjnych umożliwiających w razie awarii odtworzenie Systemu,
 - c. konfigurowanie technicznych środków ochrony Systemu oraz okresowe kontrole poprawności ich konfiguracji,
 - d. bieżące aktualizowanie Systemu i usuwanie Podatności,
 - e. bieżące monitorowanie Bezpieczeństwa Informacji przetwarzanych w Systemie i niezwłoczne informowanie PGE-CERT o wszelkich zdarzeniach mogących stanowić zagrożenie dla tego bezpieczeństwa lub zdarzeniach noszących znamiona Incydentu Cyberbezpieczeństwa,
 - f. aktywne wspieranie osób zaangażowanych w obsługę Incydentów Cyberbezpieczeństwa, w szczególności dostarczenie wszelkich żądanych przez te osoby informacji,
 - g. nadzorowanie Osób Trzecich wykonujących prace, z którymi wiąże się konieczność uzyskania fizycznego Dostępu do urządzeń Systemu Teleinformatycznego.
- 6.2.6 Spółka będąca właścicielem Zasobu ICT jest zobowiązana do wskazania Właściciela dla tego Zasobu ICT. Właściciel Zasobu ICT sprawuje nadzór nad Zasobem ICT poprzez:
- a. zapewnienie wymaganego poziomu technicznego i bezpieczeństwa poprzez realizację zakupów rozwojowych i odtworzeniowych zgodnie z rekomendacjami CUW ICT (np. poprzez zapewnienie Dostępu do aktualizacji),
 - b. zapewnienie wsparcia dla Administratora w procesach utrzymaniowych przez utrzymywanie umów serwisowych z dostawcami dla sprzętu komputerowego i oprogramowania na wymaganym poziomie,
 - c. wspieranie Administratora w kontaktach z dostawcami, z którymi Spółka ma podpisane umowy serwisowe,
 - d. przekazywanie Administratorowi informacji licencyjnych niezbędnych do realizacji okresowego przeglądu legalności oprogramowania.
- 6.2.7 Dla każdego z eksploatowanych Systemów Spółka zobowiązana jest powołać Menadżera Dostępu, który jest odpowiedzialny za zapewnienie adekwatnego poziomu uprawnień Użytkowników z tej Spółki do Systemu. Menadżer Dostępu w szczególności:
- a. wykonuje okresowe przeglądy uprawnień Użytkowników do nadzorowanego Systemu,

- b. zatwierdza, na swoim poziomie akceptacji, nadanie Użytkownikom adekwatnego poziomu Dostępu do Systemu,
 - c. zarządza dostępem do Danych Spółki niezależnie od formy Nośnika dla przechowywanej informacji (informacja przetwarzana w Systemach Teleinformatycznych, kopiach bezpieczeństwa, Nośnikach przenośnych, wydrukach),
 - d. identyfikuje potrzeby biznesowe Systemu dotyczące czasów dostępności, czasów niedostępności, retencji przechowywania kopii zapasowych i uzgadnia możliwość ich realizacji z Administratorem oraz Właścicielem Zasobu,
 - e. przy wykonywaniu działań o których mowa w pkt 6.2.7.a - 6.2.7.d bierze pod uwagę klasyfikację informacji przetwarzanych przez System i ich istotność dla procesów biznesowych.
- 6.2.8 Dla poczty korporacyjnej prowadzone jest niezależne archiwum wiadomości, które zawiera domyślnie całą korespondencję z ostatnich 3 lat liczone wstecz od daty bieżącej.
- 6.2.9 Spółka zapewnia aktualność Listy Akceptujących pod względem roli Menadżera Dostępu.
- 6.2.10 Zasady informowania o zmianach ról:
- a. Kierujący komórką właściwą ds. ICT w Spółce informuje Kierującego komórką DC o powołaniu/odwołaniu Kierującego komórką ds. ICT w Spółce,
 - b. Kierujący komórką ds. ICT w danej Spółce informuje CUW ICT o zmianach personalnych w Organach Spółki oraz w zakresie pozostałych ról opisanych Procedurą. aktualne przypisanie osób do ról jest publikowane na Liście Akceptujących.
- 6.2.11 Spółka zobowiązana jest skutecznie poinformować Kierującego komórką właściwą ds. strategii IT w PGE S.A. o zmianie osoby Kierującej komórką właściwą ds. ICT w Spółce. Jednocześnie osoba upoważniona w Spółce do modyfikacji Listy Akceptujących zobowiązana jest do zaktualizowania informacji publikowanych w ramach takiej Listy.
- 6.2.12 CUW ICT zapewni Spółce możliwość korzystania z narzędzia do zarządzania Listą Akceptujących. W sytuacji, gdy wspomniane narzędzie nie jest Dostępne, zmiany na Liście Akceptujących są realizowane przez Service Desk na podstawie złożonego Wniosku zaakceptowanego przez Kierującego komórką ds. ICT Spółki.
- 6.2.13 Lista Akceptujących obejmuje:
- a. Kierującego komórką ds. ICT w Spółce i osoby przez niego upoważnione do realizacji zadań wynikających z Procedury,
 - b. Osoby uprawnione do akceptowania Wniosków o Konta i uprawnienia na drugim poziomie dla poszczególnych Systemów Teleinformatycznych i Zasobów ICT,
 - c. Kierującego komórką właściwą ds. obsługi Organów Spółki,
 - d. Kierującego komórką ds. ZZL,
 - e. Kierującego ODO – w zależności od decyzji Spółki,
 - f. Kierującego komórką właściwą ds. bezpieczeństwa w Spółce.
- 6.2.14 Eksploatowane Systemy Teleinformatyczne podlegają cyklicznym przeglądom realizowanym nie rzadziej niż raz na 12 miesięcy. W ramach przeglądu weryfikacji podlega:
- a. poprawność przypisanych ról w zakresie działania Procedury,
 - b. poziom bezpieczeństwa Systemu Teleinformatycznego w odniesieniu do aktualnych zagrożeń,
 - c. planowane zadania związane z utrzymaniem Systemu (np. planowane aktualizacje Systemu, przełączenie w tryb archiwalny lub jego wyłączenie),
 - d. zgodność dokumentacji z aktualnymi wymaganiami dla danego Systemu.
- 6.2.15 Za inicjowanie przeglądu odpowiada Kierujący komórką odpowiedzialną za Cyberbezpieczeństwo w CUW ICT. Za realizację zadań po stronie Spółek dla Zasobów ICT nieadministrowanych przez CUW ICT odpowiada Kierujący komórką ds. ICT w Spółce.
- 6.2.16 Podczas wykonywania przeglądów dodatkowo należy zwrócić uwagę na stan urządzeń oraz na:
- a. usunięcie zanieczyszczeń mogących spowodować awarię sprzętu,
 - b. usunięcie wykrytych usterek lub nieprawidłowości,
 - c. sprawdzenie środowiska pracy urządzenia,
 - d. sprawdzenie wykorzystania pojemności użytkowanych przez Zasób ICT Nośników.
- 6.2.17 CUW ICT we współpracy ze Spółkami sporządza raporty z przeglądu prezentujące aktualny poziom bezpieczeństwa Systemów i przekazuje je do właściwej Spółki oraz CIO. Na podstawie raportu Właściciel Zasobu ICT planuje działania operacyjne i inwestycyjne mające na celu utrzymanie wymaganego poziomu bezpieczeństwa Zasobu ICT, za który odpowiada.
- 6.2.18 CUW ICT prowadzi rejestr wszystkich Systemów Teleinformatycznych w GK PGE. Rejestr jest aktualizowany z uwzględnieniem wyników z przeglądów Systemów. W szczególności rejestr zawiera:

- a. nazwę Systemu,
- b. Właściciela Zasobu ICT,
- c. Administratorów Technicznych,
- d. Menadżera Danych,
- e. informację, czy System przetwarza Dane Osobowe i jakie są to kategorie danych Osobowych.

6.3 DOSTĘP DO SYSTEMÓW TELEINFORMATYCZNYCH

6.3.1 ZASADY OGÓLNE

- 6.3.1.1 Dostęp do Danych w Systemach Teleinformatycznych i Zasobów ICT nadawany jest poprzez założenie Konta i nadanie uprawnień.
 - 6.3.1.2 Każdy Administrator oraz Użytkownik posiada unikatowy Identyfikator oraz Dane Uwierzytelniające do Systemu w celu zapewnienia Rozliczalności.
 - 6.3.1.3 Konto Podstawowe i Dodatkowe może być używane tylko i wyłącznie przez osobę, dla której zostało założone.
 - 6.3.1.4 Identyfikator Użytkownika, którego Konto wygasło lub zostało zamknięte nie może zostać przydzielony innemu Użytkownikowi.
 - 6.3.1.5 Dla Pracowników Spółki zatrudnionych na czas nieokreślony oraz Kontraktorów Konto zakładane jest bezterminowo, chyba że wnioskujący wyznaczy datę zamknięcia Konta (np. ze względu na wygaśnięcie potrzeb biznesowych).
 - 6.3.1.6 Dla osób, z którymi Spółka podjęła współpracę na podstawie terminowych umów o pracę, innych umów niż umowa o pracę oraz Osób Trzecich, Konto zakładane jest na:
 - a. czas określony w umowie ze Spółką nie dłuższy niż 1 rok,
 - b. okres, w jakim występuje potrzeba biznesowa korzystania z Konta,
 - c. w zależności od tego, który z tych okresów jest krótszy.
 - 6.3.1.7 W przypadku Spółek nie posiadających podpisanej Umowy SLA z CUW ICT:
 - a. Pracownicy tych Spółek mają zakładane Konta Podstawowe na czas nieokreślony,
 - b. Menadżerem wszystkich typów Kont zakładanych dla tych Spółek są wyznaczone osoby ze Spółek GK PGE mających podpisaną Umowę SLA, dla których rzeczono Spółki świadczą usługi.
 - 6.3.1.8 Jeżeli okres realizacji działań Osoby Trzeciej na rzecz Spółki jest dłuższy niż 1 rok, po upływie tego terminu konieczne jest wystąpienie z Wnioskiem o przedłużenie Dostępu na kolejny okres. Brak złożenia Wniosku o przedłużenie Dostępu skutkuje automatycznym zamknięciem Konta w terminie 14 dni po przekroczeniu daty ważności konta.
 - 6.3.1.9 W przypadku, gdy Użytkownik ma zawarte umowy z wieloma Spółkami, musi mieć założone oddzielne Konta do realizacji zadań dla poszczególnych Spółek. Konta zakładane są na Wniosek Spółek.
 - 6.3.1.10 Dopuszcza się rezygnację z rozdzielenia Kont dla członka Organów Spółki, o którym mowa w pkt 6.3.1.9 za udokumentowaną zgodą Kierującego komórką właściwą ds. strategii ICT GK PGE oraz potwierdzoną przez Zarząd danej Spółki – zgodnie z reprezentacją. Decyzja taka może skutkować brakiem możliwości separacji informacji poszczególnych Spółek przetwarzanych na tym Koncie.
 - 6.3.1.11 Użytkownik może pełnić rolę Menadżera Danych, co oznacza kompetencje do nadawania i odbierania uprawnień w użytkowanym Systemie ICT dla innych Użytkowników.
 - 6.3.1.12 Użytkownicy zarządzają Danymi na swoich stacjach roboczych, skrzynkach poczty elektronicznej, zasobach sieciowych, witrynach SharePoint, Nośnikach przenośnych i wydrukach zgodnie z nadanymi upoważnieniami do przetwarzania danych i uprawnieniami do Systemów ICT. Odpowiedzialność Użytkownika za udostępnienie informacji jest niezależna od formy Nośnika Informacji.
- #### 6.3.2 DOSTĘP PODSTAWOWY
- 6.3.2.1 Dostęp podstawowy oparty jest o Konto w domenie korporacyjnej gkpge.pl i jest podstawowym mechanizmem Uwierzytelnienia się i zarządzania uprawnieniami Użytkownika do Sieci Korporacyjnej. Konto Dostępu Podstawowego jest niezbędne do prawidłowej pracy w Sieci Korporacyjnej w oparciu o nadane uprawnienia.
 - 6.3.2.2 Konto Dostępu Podstawowego jest związane z:
 - a. Kontem Użytkownika w domenie korporacyjnej,
 - b. dodaniem Konta do domyślnych grup w AD wynikających ze stanowiska, miejsca w hierarchii organizacji Spółki,
 - c. utworzeniem korporacyjnego Konta pocztowego Użytkownika,
 - d. dodaniem do domyślnych grup dystrybucyjnych wynikających ze stanowiska, miejsca w hierarchii organizacji Spółki,
 - e. nadaniem jednorazowego Hasła domenowego,
 - f. oraz nadaniem pozostałych uprawnień uzgodnionych dla danej Spółki.

- 6.3.2.3 Dostęp do pozostałych Systemów Teleinformatycznych oraz Zasobów ICT należy realizować w oparciu o Konto Dostępu Podstawowego, a w Systemach, gdzie to nie jest możliwe, w oparciu o konta lokalne w Systemie.
- 6.3.2.4 Realizacja usług włączenia, wyłączenia oraz zamknięcia Konta Dostępu Podstawowego skutkuje odpowiednią modyfikacją Dostępu do wszystkich innych Zasobów ICT i Systemów Teleinformatycznych wykorzystujących Uwierzytelnianie Użytkownika oparte o usługę Active Directory działającą na potrzeby GK PGE.
- 6.3.3 **ZARZĄDZANIE KONTAMI UPRIWILEJOWANYMI**
- 6.3.3.1 W celu zarządzania Zasobem ICT tworzy się Konta administracyjne (z uprawnieniami Administratora Zasobu ICT).
- 6.3.4 Jedynie Administratorzy są upoważnieni do posiadania kont administracyjnych.
- 6.3.5 Konto Administracyjne może być użyte wyłącznie do zarządzania Zasobami ICT oraz Systemami. Administratorzy zobowiązani są do używania Systemu nadzoru Dostępu administracyjnego podczas wykonywania prac administratorskich, które wiążą się z koniecznością bezpośredniego logowania do serwerów produkcyjnych Systemu.
- 6.3.6 Wbudowane Konta Techniczne dla Zasobów ICT, o ile jest to możliwe, muszą być trwale wyłączone. Hasła do tych Kont muszą być tak zabezpieczone, aby możliwe było ich ewentualne użycie.
- 6.3.7 W przypadku istnienia Kont współdzielonych oraz braku możliwości rozdzielania uprawnień należy ściśle zdefiniować grupę Użytkowników lub Administratorów korzystających z tych Kont oraz zapewnić mechanizm zapewniający Rozliczalność wykorzystania Konta.
- 6.3.8 Systemy wykorzystujące uprzywilejowane Konta Techniczne i współdzielone muszą zostać podłączone do Systemu klasy PIM w celu zapewnienia kontroli i Rozliczalności ich wykorzystania. Wyjątek stanowią Systemy, których nie można podłączyć z powodu ograniczeń technicznych. Za zgłoszenie potrzeby podłączenia Systemu odpowiedzialny jest Administrator Techniczny.
- 6.3.9 Konta z uprawnieniami administracyjnymi na Komputerach Biurowych mogą być utworzone wyłącznie dla Administratorów na Wniosek, jeśli wynika to z zakresu obowiązków danego Pracownika lub zakresu umowy z Kontraktorem.
- 6.3.10 Konta, o których mowa w pkt 6.3.9, muszą posiadać różne Identyfikatory (Loginy) od Kont Podstawowych.
- 6.3.11 Administrator odpowiada za zapewnienie zabezpieczenia kont administratora Systemu ICT oraz danych dostępowych dla zapewnienia ciągłości działania.

6.4 WNIOSKI O DOSTĘP DO SYSTEMÓW TELEINFORMATYCZNYCH

6.4.1 ZASADY OGÓLNE

- 6.4.1.1 Za złożenie Wniosku o założenie, zamknięcie, włączenie, wyłączenie Konta odpowiedzialny jest Menadżer Konta. Wniosek może być złożony przez wskazanego Kontraktora lub Pracownika.
- 6.4.1.2 Dopuszcza się automatyczne procesowanie Wniosków dotyczących Kont z pominięciem procesu akceptacji dla Wniosków pochodzących ze Źródła tożsamości.
- 6.4.1.3 Wniosek kierowany jest do realizacji po pozytywnym zakończeniu procesu akceptacji, o którym mowa w pkt 6.4.3, przy czym:
 - a. w przypadku Wniosku o utworzenie Konta podstawowego Użytkownika przekazanie do realizacji następuje nie wcześniej niż 7 dni roboczych przed wskazaną we Wniosku datą aktywacji Konta,
 - b. przekazanie do realizacji Wniosku o zamknięcie Konta podstawowego Użytkownika następuje w dniu następnym po wskazanej we Wniosku dacie ostatniego dnia pracy.
- 6.4.1.4 W przypadku Kont Dostępu Podstawowego ze zdefiniowaną datą ważności, CUW ICT, z wyprzedzeniem co najmniej 30 dni kalendarzowych, wysyła powiadomienie (e-mail) do Użytkownika oraz Menadżera Konta z informacją o krokach niezbędnych do podjęcia w celu przedłużenia ważności Konta. Nieprzedłużenie ważności Konta skutkuje automatycznym wygenerowaniem Wniosku o zamknięcie Dostępu. Wniosek ten do realizacji jest kierowany z pominięciem procesu akceptacji.
- 6.4.1.5 Czas na realizację Wniosków opisanych w Procedurze jest definiowany w Umowach SLA zawartych pomiędzy Spółką a CUW ICT.
- 6.4.1.6 Do składania Wniosków o Dostęp uprawnieni są wszyscy Użytkownicy posiadający Konto Dostępu Podstawowego.
- 6.4.1.7 Użytkownik jest uprawniony do składania Wniosków:
 - a. na rzecz Pracowników, Kontraktorów, członków Organów oraz Osób Trzecich tej samej Spółki, w której zadania realizuje wnioskujący,
 - b. dotyczących Kont Technicznych, których Menadżer Konta jest Pracownikiem tej samej Spółki.
- 6.4.1.8 Jedynym dopuszczonym sposobem składania Wniosków dotyczących Dostępu Podstawowego i uprawnień jest złożenie elektronicznego wniosku z wykorzystaniem SOZ . W przypadkach, w których SOZ nie gwarantuje

skutecznego dokumentowania procesu (np. Wnioski niekatalogowe) Spółki odpowiadają zgodnie z obowiązującymi w GK PGE regulacjami wewnętrznymi za zabezpieczenie dokumentacji z Wniosków:

- a. pozwalającej na trwałą identyfikację osób podejmujących czynności akceptacyjne w ramach niniejszej Procedury,
- b. dotyczącej faktów decydujących o tym, która z osób miała prawo w danym momencie akceptować działania w procedurach.

6.4.2 RODZAJE WNIOSKÓW O DOSTĘP PODSTAWOWY:

6.4.2.1 Nadanie Dostępu Podstawowego – Wniosek o utworzenie Konta Dostępu Podstawowego dla nowego Użytkownika lub Użytkownika, którego Konto zostało wcześniej zamknięte.

6.4.2.2 Przedłużenie Dostępu Podstawowego – Wniosek o przedłużenie terminu ważności Konta Dostępu Podstawowego utworzonego na czas określony. Wniosek można złożyć jedynie w czasie, kiedy Konto jest aktywne. Po zamknięciu Konta Dostępu Podstawowego wymagane jest złożenie Wniosku o Nadanie Dostępu na podstawie, którego będzie założone nowe Konto Dostępu Podstawowego.

6.4.2.3 Zamknięcie Dostępu Podstawowego – Wniosek o trwale i ostateczne uniemożliwienie pracy na Koncie Dostępu Podstawowego. We Wniosku należy podać oczekiwaną datę zamknięcia Konta.

- a. Konto jest zamykane na podstawie Wniosku niezwłocznie po ustaniu uzasadnienia biznesowego do jego wykorzystania,
- b. zamknięcie Konta Dostępu Podstawowego skutkuje zamknięciem Dodatkowych Kont imiennych Użytkownika, a tym samym odebraniem uprawnień do wszystkich Systemów Teleinformatycznych i Zasobów ICT, do których Dostęp był realizowany z użyciem tych kont,
- c. CUW ICT w ramach realizacji prac musi opisać Konto wraz z podaniem przyczyny jego zamknięcia oraz dokonuje archiwizacji zabezpieczonej zawartości skrzynki pocztowej. Archiwum zawartości skrzynki pocztowej jest standardowo przechowywane przez okres 3 lat od dnia przyjęcia Wniosku do realizacji, chyba że Spółka określi inaczej. Archiwum skrzynki pocztowej zawiera aktualne wiadomości elektroniczne Użytkownika z dnia zamknięcia Konta wraz z odzyskanymi wiadomościami usuniętymi w okresie 30 ostatnich dni od przyjęcia wniosku do realizacji.

6.4.2.4 W ramach zamykania Konta Menadżer Konta musi:

- a. zweryfikować, czy są konieczne zmiany w uprawnieniach innych Użytkowników, aby zachować ciągłość biznesową po zamknięciu Konta i wystawić konieczne Wnioski,
- b. zweryfikować, czy są przypadki, dla których użytkujący zamykane Konto jest Menadżerem Konta i wskazać nową osobę do pełnienia tej roli poprzez Wniosek na SD,
- c. zweryfikować, czy są przypadki, dla których użytkujący zamykane Konto jest Właścicielem Zasobu ICT lub pełni inne role wskazane w Procedurze i wskazać nową osobę do pełnienia tej roli,
- d. zdecydować o sposobie postępowania z Danymi, których użytkujący zamykane Konto był Menadżerem Danych, w szczególności czy Dane mogą być skasowane, zarchiwizowane lub zostanie wskazana inna osoba do pełnienia roli Menadżera Danych.

6.4.2.5 Administracyjne wyłączenie Dostępu Podstawowego – Wniosek o czasowe wyłączenie Konta Dostępu Podstawowego w celu uniemożliwienia zalogowania na Konto. Administracyjne wyłączenie Konta nie zmienia układu uprawnień do Zasobów ICT i stosowane jest w celu czasowego wyłączenia możliwości korzystania z Systemów Teleinformatycznych, np. na czas długotrwałych urlopów lub w trakcie wyjaśniania Incydentów Cyberbezpieczeństwa:

- a. wyłączenie Konta ma za zadanie natychmiastowe zabezpieczenie Danych będących własnością Spółki przed nieuprawnionym Dostępem,
- b. ze względu na konieczność szybkiej reakcji operacja wyłączenia Konta realizowana jest na podstawie Wniosku o Dostęp lub zgłoszenia na SD od:
 - Użytkownika będącego właścicielem Konta (np. w przypadku kradzieży komputera lub podejrzenia o przejęcie przez osoby nieuprawnione danych Uwierzytelniających),
 - Menadżera Konta,
 - Kierującego komórką ds. ZZL w Spółce lub osoby przez niego upoważnionej,
 - Kierujący komórką ds. ICT w Spółce lub osoby przez niego upoważnionej,
 - Pracownika lub Kontraktora z PGE-CERT, w związku z Incydem Cyberbezpieczeństwa.

6.4.2.6 W przypadku wyłączenia Konta w wyniku zgłoszenia na SD zgłaszający zobowiązany jest do dopełnienia formalności w postaci złożenia odpowiedniego Wniosku o Dostęp.

6.4.2.7 Wniosek o administracyjne wyłączenie Konta nie wymaga akceptacji drugiego poziomu.

- 6.4.2.8 W celu zabezpieczenia Konta przed nieuprawnionym Dostępem zaleca się wyłączenie Kont Użytkowników w przypadkach długotrwałych urlopów i zwolnień, oraz powszechnie znanych Kont Technicznych narażonych na ataki cyberprzestępców.
- 6.4.2.9 W trakcie wyłączania Konta CUW ICT realizując prace musi opisać Konto i podać przyczynę jego wyłączenia.
- 6.4.2.10 Administracyjne włączenie Dostępu Podstawowego – Wniosek o włączenie Konta Dostępu Podstawowego czasowo wyłączonego realizowanego w celu przywrócenia Użytkownikowi możliwości korzystania z Systemów Teleinformatycznych. Administracyjne włączenie Konta nie zmienia układu uprawnień do Zasobów ICT, a włącza jedynie możliwość zalogowania na Konto.
- 6.4.2.11 Włączenie Konta jest realizowane na podstawie Wniosku o Dostęp od:
- osoby na Wiosek, której dokonano Administracyjnego wyłączenia Konta Użytkownika,
 - Menadżera Konta,
 - Kierującego komórką ds. ZZL w Spółce lub osoby przez niego upoważnionej,
 - Kierującego komórką ds. ICT w Spółce lub osoby przez niego upoważnionej,
 - Pracownika PGE-CERT, w związku z zakończeniem obsługi Incydentu Cyberbezpieczeństwa.
- 6.4.2.12 Wniosek podlega akceptacji w ramach, której należy potwierdzić ustanie przyczyn jego wyłączenia podanych na Wniosku o Administracyjne wyłączenie Konta.
- 6.4.2.13 W trakcie włączenia Konta CUW ICT musi opisać Konto numerem Wniosku o odblokowanie Konta.
- 6.4.2.14 Zmiana Menadżera Konta – Wniosek o przypisanie nowego Pracownika do roli Menadżera Konta.
- zmiana Menadżera Konta jest realizowana na Wniosek dotychczasowego Menadżera Konta, nowego Menadżera Konta lub ich Przełożonych,
 - Wniosek podlega standardowej dwupoziomowej akceptacji przy czym:
 - na pierwszym poziomie akceptacji decyzję wydaje dotychczasowy Menadżer Konta,
 - na drugim poziomie akceptacji decyzję wydaje nowy Menadżer Konta.
- 6.4.2.15 W ramach zgłoszenia na SD realizowane są dodatkowo:
- Odblokowanie Konta – Wniosek o odblokowanie zablokowanego w wyniku wielu prób Uwierzytelniania z podaniem niepoprawnych poświadczeń (Login/Hasło) lub innych nieprawidłowości (do realizacji wymagana jest akceptacja Użytkownika a dla Kont dodatkowych i technicznych akceptacja Menadżera Konta),
 - Reset Hasła – zgłoszenie o wygenerowanie nowego, jednorazowego Hasła do Systemu Teleinformatycznego (do realizacji wymagana jest akceptacja Użytkownika a dla Kont dodatkowych i technicznych akceptacja Menadżera Konta).
- 6.4.2.16 W ramach zarządzania uprawnieniami w SOZ realizowane są Wnioski o uprawnienia:
- nadanie/modyfikację uprawnień – Wniosek składany w celu nadania uprawnień, których Użytkownik jeszcze nie posiada,
 - odebranie uprawnień – Wniosek umożliwiający wskazanie uprawnień posiadanych przez Użytkownika, które należy odebrać. Dla Systemów, które nie są obsługiwane w SOZ operacje nadawania/modyfikacji i odbierania uprawnień realizowane są na podstawie zgłoszeń na SD.
- 6.4.2.17 Za terminowe wystawienie Wniosku odpowiedzialni są Menadżer Konta i Menadżer Dostępu.
- 6.4.3 **ZASADY AKCEPTACJI WNIOSKÓW O DOSTĘP DO ZASOBÓW**
- 6.4.3.1 Dostęp do Danych nadawany jest po uzyskaniu wymaganych akceptacji przez poszczególne role zgodnie z zasadą minimalnych uprawnień.
- 6.4.3.2 Akceptacja Wniosków odbywa się drogą elektroniczną. W procesie akceptacji ocenia się zasadność Wniosku na dwóch poziomach:
- potrzeb biznesowych Użytkownika,
 - wartości aktywów informacyjnych dla Spółki i ochrony dostępu do aktywów.
- 6.4.3.3 Pierwszy stopień akceptacji realizowany jest przez Menadżera Konta, a w przypadku Kont Dodatkowych i Technicznych Menadżera Konta Użytkownika, którego Wniosek dotyczy. Akceptując Wniosek o Konto lub uprawnienia akceptujący potwierdza, że zakres potrzeb biznesowych wskazany w uzasadnieniu Wniosku jest zgodny z potrzebami biznesowymi realizowanymi przez Użytkownika.
- 6.4.3.4 Opcjonalnie, zgodnie z decyzją Spółki, dopuszcza się dodatkowe stopnie akceptacji realizowane przez wyznaczone w Jednostce organizacyjnej osoby, których celem jest weryfikacja zgodności Wniosku z lokalnymi regulacjami w obszarach: Poufności informacji, ochrony Danych Osobowych, Cyberbezpieczeństwa, zarządzania licencjami, zarządzania Usługami ICT itp.
- 6.4.3.5 Drugi stopień akceptacji realizowany jest przez Menadżera Dostępu, który akceptując Wniosek o Konto lub uprawnienia potwierdza, że:

- a. zakres uprawnień wskazany na Wniosku nie jest nadmiarowy i jest wystarczający do realizacji zadań biznesowych wskazanych w uzasadnieniu Wniosku,
- b. zostały potwierdzone wszystkie dodatkowe wymagania Spółki konieczne do realizacji Wniosku, w tym wymagania w obszarach: Poufności informacji, ochrony Danych Osobowych, Cyberbezpieczeństwa, zarządzania licencjami, zarządzania Usługami ICT.
- 6.4.3.6 Drugi stopień akceptacji dla Kont technicznych realizowany jest przez Przełożonego Menadżera Konta.
- 6.4.3.7 CUW ICT nie weryfikuje zasadności Wniosków, a jedynie zgodność z Procedurą. Potrzeby i warunki decydujące o złożeniu Wniosku są w kompetencjach Spółek.
- 6.4.3.8 Osoby upoważnione do akceptowania na drugim poziomie Wniosków o Konto Podstawowe Użytkownika są umieszczane na Liście Akceptujących. Wszystkie osoby z Listy Akceptujących pełniące taką samą rolę mają jednakowe uprawnienia do akceptacji działań wynikających z realizacji procedur.
- 6.4.3.9 Jeżeli Wniosek został złożony przez Menadżera Konta, akceptacja pierwszego poziomu może zostać pominięta.
- 6.4.3.10 Jeżeli Wniosek został złożony przez Menadżera Dostępu, akceptacje pierwszego i drugiego poziomu mogą zostać pominięte.
- 6.4.3.11 Akceptacja pierwszego i drugiego poziomu przy udziale Menadżera Konta i Menadżera Dostępu ma zagwarantować właściwy, możliwie najniższy poziom dostępu do Systemów Teleinformatycznych umożliwiający realizację zadań na rzecz Spółki.
- 6.4.3.12 Czynności opisane w Procedurze takie jak nadawanie, zamykanie, administracyjne wyłączenie Konta mogą być realizowane automatycznie przez Systemy informatyczne z pominięciem Procesu akceptacji, pod warunkiem, że informacje wymagane do ich realizacji pochodzą ze Źródła tożsamości. W szczególności:
 - a. nadanie Dostępu Podstawowego dla Pracownika może być realizowane automatycznie w przypadku wprowadzenia w Źródle tożsamości zdarzenia kadrowego o rozpoczęciu stosunku pracy. Automatyczne nadanie Dostępu Podstawowego przez Źródło tożsamości nie pociąga za sobą obowiązku wystawienia Wniosku w SOZ,
 - b. administracyjne wyłączenie Konta może być realizowane automatycznie w odniesieniu do Kont tych Pracowników, którzy zgodnie z *PROG 00105 Procedura Ogólna Zarządzania Użytkownikami Końcowymi w SAP w Grupie Kapitałowej PGE* są długotrwale nieobecni,
 - c. zamknięcie Konta Podstawowego Pracownika oraz Kont Dodatkowych może być realizowane automatycznie w przypadku wprowadzenia w Źródle tożsamości zdarzenia kadrowego o zakończeniu stosunku pracy. Automatyczne wyłączenie Konta przez Źródło tożsamości nie pociąga za sobą obowiązku wystawienia Wniosku w SOZ.
- 6.4.3.13 Czas na akceptację Wniosku na każdym z poziomów wynosi 5 Dni Roboczych. Brak akceptacji we wskazanym terminie oznacza automatyczne odrzucenie Wniosku. O odrzuceniu Wniosku informowani są: wnioskujący oraz Menadżer Konta.

6.5 ZARZĄDZANIE UPRAWNIENIAMI

- 6.5.1 Operacja nadawania i odbierania uprawnień w Systemie Teleinformatycznym realizowana jest na podstawie Wniosku o Dostęp do Systemu Teleinformatycznego i dokumentowana w Dzienniku Systemu Teleinformatycznego.
- 6.5.2 Zarządzanie uprawnieniami Użytkowników powinno być oparte o role, jakie pełnią oni w organizacji, np. stanowisko lub przynależność do Komórki organizacyjnej oraz uwzględniać zasadę rozdziału obowiązków.
- 6.5.3 Użytkownik otrzymuje uprawnienia do Zasobu ICT, zgodnie z zakresem jego obowiązków służbowych oraz zasadą minimum koniecznego, oznaczającą udostępnianie minimalnych uprawnień wystarczających do skutecznej realizacji powierzonych zadań.
- 6.5.4 Użytkownicy zobowiązani są zgłaszać Menadżerowi Danych fakt posiadania szerszych uprawnień do Zasobu, niż wynika to z zakresu zatwierdzonych uprawnień.
- 6.5.5 Uprawnienia powinny być nadawane jedynie na okres w jakim są niezbędne do realizacji zadań służbowych na rzecz Spółki. Uprawnienia nadmiarowe niepotrzebne do realizacji zadań na rzecz Spółki powinny być niezwłocznie odbierane.
- 6.5.6 Uprawnienia dla osób, z którymi Spółka podjęła współpracę na podstawie terminowych umów o pracę, innych umów niż umowa o pracę oraz Osób Trzecich nadawane są na:
 - a. czas określony wskazany w umowie ze Spółką nie dłuższy niż 1 rok,
 - b. okres w jakim występuje potrzeba biznesowa korzystania z uprawnień,
 w zależności od tego, który z nich jest krótszy.
- 6.5.7 Jeżeli okres realizacji działań Osoby Trzeciej na rzecz Spółki jest dłuższy niż 1 rok, po upływie tego terminu konieczne jest wystąpienie z Wnioskiem o przedłużenie Dostępu. Użytkownik pełniący rolę Menadżera Danych i mający odpowiednie uprawnienia może samodzielnie udostępnić Dane, którymi zarządza innym Użytkownikom

poprzez nadawanie uprawnień do Zasobu ICT. W tym przypadku CUW ICT nie uczestniczy w procesie udostępniania Danych.

- 6.5.8 Dla każdego z Zasobów ICT Menadżer Dostępu definiuje szczegółowe zasady zarządzania uprawnieniami, przy czym zasady te nie mogą być sprzeczne z zasadami przedstawionymi w Procedurze.

6.6 OKRESOWY PRZEGLĄD KONT I UPRAWNIEŃ

- 6.6.1 W celu zapewnienia właściwego poziomu bezpieczeństwa Spółka zobowiązana jest do realizowania cyklicznych przeglądów Kont oraz nadanych uprawnień weryfikujących, czy Użytkownicy mają nadany taki zakres uprawnień, jaki wynika z wykonywanych obowiązków. Nadzór nad terminowym wykonywaniem przeglądu sprawuje Kierujący komórką ds. ICT w Spółce.
- 6.6.2 Przegląd musi być inicjowany:
- a. co najmniej raz do roku przez Kierującego komórką ds. ICT w Spółce,
 - b. w przypadku istotnych zmian organizacyjnych przez Kierującego komórką odpowiedzialną za strukturę organizacyjną,
 - c. przez Menadżera Dostępu, gdy będą zachodziły podejrzenia, że uprawnienia w Systemie, za który odpowiada, są nadane nieprawidłowo,
 - d. przez Menadżera Konta przy zmianie obowiązków lub stanowiska Użytkownika.
- 6.6.3 Kierujący komórką właściwą ds. strategii ICT może zlecić wykonanie dodatkowego przeglądu uprawnień dla dowolnej grupy Użytkowników.
- 6.6.4 W ramach realizacji przeglądu uprawnień uczestniczący w przeglądzie Przełożony oraz Menadżer Konta zatwierdza prawidłowe uprawnienia Użytkownika oraz w razie konieczności zgłasza Wnioski o zamknięcie Kont lub odebranie uprawnień.
- 6.6.5 Do realizacji przeglądów Kont i uprawnień zobowiązani są również Użytkownicy pełniący rolę Menadżera Dostępu i udostępniający Dane innym Użytkownikom np. poprzez Zasoby sieciowe, witryny SharePoint, współdzielone skrzynki pocztowe.
- 6.6.6 Przegląd może być realizowany przy wykorzystaniu narzędzi Teleinformatycznych i powinien uwzględniać specyfikę danego Systemu Teleinformatycznego. Raport z przeprowadzonego przeglądu przekazywany jest do Kierującego komórką ds. ICT Spółki oraz Kierującego komórką DC.
- 6.6.7 Nadmiarowe uprawnienia zostaną niezwłocznie odebrane przez Administratora na Wniosek Menadżera Danych lub Menadżera Konta.
- 6.6.8 Procedura dopuszcza masowe zamykanie, zablokowanie czy modyfikację Kont po dokonanych przeglądach na następujących zasadach:
- 6.6.8.1 Po przeprowadzonym przeglądzie uprawnień należy złożyć Wniosek wspólny dla danej Spółki w SOZ.
 - 6.6.8.2 Zasady mają zastosowanie dla liczby co najmniej 20 Kont przeznaczonych jednorazowo do zmiany (zamknięcia, zablokowania lub aktualizacji).
 - 6.6.8.3 Zamykania, blokowania lub aktualizacji Kont dokonuje CUW ICT zgodnie ze złożonym Wnioskiem.
 - 6.6.8.4 Po realizacji zmian należy przeprowadzić dodatkową weryfikację potwierdzającą, iż Dostępy Podstawowe dla Kont zostały obsłużone zgodnie z zaakceptowanym Wnioskiem.
 - 6.6.8.5 CUW ICT zapewnia możliwość cofnięcia działań spowodowanych realizacją procesu masowej zmiany Kont Dostępu Podstawowego w przypadku wstąpienia błędu lub pomyłki wnioskującego.
 - 6.6.8.6 Włączenie Dostępu Podstawowego w przypadku wystąpienia pomyłki następuje na podstawie nowego Wniosku niekatalogowego potwierdzonego przez Kierującego komórką odpowiedzialną za obszar ICT w Spółce.
 - 6.6.8.7 W przypadku, gdy istnieją obiektywne przesłanki uniemożliwiające zamknięcie Konta – sytuacja jest wyjaśniana, a w opisie rozwiązania zamykanego Wniosku dodawane są Identyfikatory Kont niezamkniętych w ramach Wniosku.
 - 6.6.8.8 Wniosek musi być zaakceptowany przez Kierującego komórką ds. ICT dla danej Spółki lub przez osoby umocowane do jej reprezentowania.
 - 6.6.8.9 Wniosek podlega akceptacji Kierującego komórką DC.

6.7 ZASADY UWIERZYTELNIANIA W SYSTEMACH TELEINFORMATYCZNYCH

- 6.7.1 Wszyscy Pracownicy Spółki, Kontraktorzy, Osoby Trzecie, członkowie Organów Spółki posiadający Dostęp do Zasobów udostępnianych przez System Teleinformatyczny są zobowiązani Uwierzytelniać się (logować) do niego przy użyciu Identyfikatora i Hasła.
- 6.7.2 W przypadku stosowania innych niż Identyfikator i Hasło metod Uwierzytelniania Użytkownika, np. karty procesorowe, karty zbliżeniowe, metody biometryczne – Administrator zobowiązany jest do opracowania instrukcji związanych z ich Użytkowaniem i zarządzaniem.

- 6.7.3 Administratorzy zobowiązani są do konfiguracji następujących zasad dla Hasel Użytkowników jeśli Systemy, którymi administrują, umożliwiają taką konfigurację:
- Hasło Użytkownika składa się z minimum 12 znaków,
 - Hasło Administratora składa się z minimum 15 znaków,
 - Hasło zawiera przynajmniej 1 małą literę (od a do z),
 - Hasło zawiera przynajmniej 1 dużą literę (od A do Z),
 - Hasło zawiera przynajmniej 1 cyfrę (od 0 do 9),
 - Hasło zawiera przynajmniej 1 znak specjalny: !@#\$%^&*(){}[]\|:;';<>?.,/,
 - Hasło nie może zawierać kolejno dwóch identycznych znaków oraz powtarzających się sekwencji znaków,
 - Hasło nie może być identyczne z nazwą Konta lub jego częścią,
 - Hasło nie może zawierać znaków diakrytycznych (np. ą, ę),
 - Hasło wymaga zmiany co 90 dni,
 - minimalny okres pomiędzy kolejnymi zmianami Hasła to 2 dni,
 - nowe Hasło musi być inne, niż co najmniej 5 ostatnio wprowadzonych Hasel,
 - Hasło musi składać się z co najmniej 5 różnych znaków,
 - Hasło nie może zawierać nazwy Konta,
 - Hasło musi różnić się od poprzedniego co najmniej 3 znakami.
- 6.7.4 Każde Hasło musi spełniać wszystkie wymienione wymagania. Jeżeli z powodu ograniczeń technicznych niemożliwe jest przestrzeganie jednej z zasad, to pozostałe zasady nadal są wymagane.
- 6.7.5 Po założeniu nowego Konta i zalogowaniu się przy użyciu Hasła początkowego Użytkownik ma obowiązek jego zmiany.
- 6.7.6 Przekazywanie Użytkownikowi danych Uwierzytelniających (Identyfikator i Hasło) odbywa się dwoma niezależnymi, różnymi kanałami / strumieniami, w sposób uniemożliwiający Dostęp do nich osobom nieupoważnionym, np. Identyfikator wysyłany jest na adres e-mail osoby, dla której tworzony jest Dostęp do Zasobu, a Hasło podawane telefonicznie.
- 6.7.7 Zabrania się wykorzystywania tych samych hasel do różnych Systemów Teleinformatycznych. Hasła do poszczególnych Systemów powinny być różne.
- 6.7.8 W celu zarządzania dużą ilością Hasel dopuszcza się stosowanie dedykowanego oprogramowania do zarządzania Hasłami. Oprogramowanie aktualnie dopuszczone do stosowania jest publikowane na Liście Oprogramowania. Nie jest dopuszczone budowanie list stosowanych Hasel i publikowanie ich w dowolnej formie.
- 6.7.9 Podczas instalacji Zasobu ICT (sprzęt, oprogramowanie) Administrator Techniczny dokonuje zmiany domyślnych Hasel Dostępu.
- 6.7.10 Dopuszcza się przechowywanie Hasel awaryjnego Dostępu do Zasobu ICT w Kopertach Bezpiecznych zgodnie z obowiązującymi regulacjami w danej Spółce. Sposób przechowywania Koperty musi uniemożliwić dostęp osób postronnych. Do otwarcia Koperty upoważniony jest Właściciel Zasobu ICT. Po otwarciu Koperty należy zmienić Hasło, a fakt otwarcia Koperty wraz z uzasadnieniem winien być odnotowany w dokumentacji Zasobu ICT.
- 6.7.11 W przypadku maksymalnie 10 krotnego błędnego wpisania Hasła do Systemu, Konto musi być blokowane. Dopuszczany również jest mechanizm czasowego blokowania Konta oraz wydłużenia czasu pomiędzy poszczególnymi próbami Uwierzytelnienia w celu przeciwdziałania próbom ataków na Konto Użytkownika. Administrator jest odpowiedzialny za włączenie takiej funkcjonalności w Systemie, którym administruje.
- 6.7.12 Odblokowanie Konta Dostępu Podstawowego możliwe jest po skontaktowaniu się z Service Desk i poprawnym przejściu weryfikacji PIN.

6.8 UDOSTĘPNIANIE DANYCH Z SYSTEMÓW TELEINFORMATYCZNYCH

6.8.1 ZASADY OGÓLNE

- 6.8.1.1 Proces udostępniania Danych z Systemów Teleinformatycznych opiera się na następujących zasadach obowiązujących w GK PGE:
- Dane mogą być wykorzystywane przez Użytkowników wyłącznie w celach, dla których zostały im udostępnione, w zakresie przydzielonych uprawnień oraz zgodnie z interesem Spółki, przyjętą dla Danych klasyfikacją ochrony informacji, obowiązującymi przepisami prawa powszechnego i regulacjami wewnętrznymi,
 - Systemy Teleinformatyczne wykorzystywane w Spółce mogą być przeznaczone tylko i wyłącznie do realizacji zadań służbowych:
 - Komputery Biurowe, Urządzenia Mobilne i Zasoby ICT (np. Zasoby sieciowe, SharePoint, Nośniki przenośne) mogą przetwarzać jedynie Dane wykorzystywane w ramach wykonywanych zadań,
 - korespondencja w formie elektronicznej obsługiwana z korporacyjnej skrzynki pocztowej jest własnością Spółki,

- Dane przetwarzane w udostępnionych Spółce Zasobach ICT stanowią własność Spółki i mogą zostać udostępnione innym wskazanym przez Spółkę Użytkownikom, osobom lub podmiotom na wyraźne polecenie Spółki.
- 6.8.1.2 Wszelkie Dane udostępniane z Zasobów ICT na podstawie Wniosku o Udostępnienie Danych z Systemów Teleinformatycznych należy traktować zgodnie z wymaganiami Spółki składającej Wniosek. Wymagania te powinny brać pod uwagę prawo Użytkowników do tajemnicy korespondencji, ochrony prywatności i ochrony Danych Osobowych.
- 6.8.1.3 Informacje dotyczące Wniosków o Udostępnianie Danych składanych przez Spółki oraz informacje związane z procesem udostępniania Danych należy traktować jako informacje szczególnie chronione zgodnie z regulacjami stosowanymi w Spółce.
- 6.8.2 OBSŁUGA WNIOSKÓW O UDOSTĘPNIANIE DANYCH
- 6.8.2.1 Dane z Systemów Teleinformatycznych udostępniane są na Wniosek o Udostępnianie Danych od Spółek GK PGE. Wniosek musi zawierać co najmniej poniższe informacje:
- a. Jednostka organizacyjna,
 - b. Źródło pozyskania wnioskowanych Danych, np. nazwa Systemu Teleinformatycznego, Komputera Biurowego, skrzynki pocztowej,
 - c. jeżeli wnioskowane Dane dotyczą Użytkownika, to wymagane jest wskazanie danych pozwalających na jego identyfikację (adres email, imię i nazwisko, nr osobowy),
 - d. wskazanie okresu z jakiego mają być wnioskowane Dane,
 - e. uzasadnienie udostępnienia,
 - f. Dane osoby lub podmiotu, któremu należy przekazać Dane,
 - g. określenie sposobu przekazania Danych, w tym mechanizmów zapewniających bezpieczeństwo Danych, na Nośniku oraz podczas transportu,
 - h. data przekazania Wniosku,
 - i. akceptację Zarządu Spółki lub osoby przez niego umocowanej potwierdzającą wymagania Spółki zawarte na Wniosku.
- 6.8.2.2 Wniosek o Udostępnianie Danych może być kierowany:
- a. w formie papierowej bezpośrednio do Kierującego komórką DC,
 - b. w formie elektronicznej zaszyfrowanej i/lub zabezpieczonej podpisem elektronicznym bezpośrednio na skrzynkę poczty korporacyjnej Kierującego komórką DC,
 - c. w formie elektronicznej zaszyfrowanej i/lub zabezpieczonej podpisem elektronicznym na skrzynkę poczty korporacyjnej bezpieczenstwo.pgesystemy@gkpge.pl.
- 6.8.2.3 Udostępnianie informacji przez CUW ICT odbywa się po akceptacji Spółki, która jest właścicielem Danych oraz CIO, z uwzględnieniem możliwości udostępnienia Danych w ramach Umowy SLA, chyba, że przepisy prawa tego nie dopuszczają.
- 6.8.2.4 Kierujący komórką DC po stwierdzeniu kompletności Wniosku o Udostępnianie Danych oraz braku zastrzeżeń co do uprawnienia wnioskującego do wnioskowanych Danych, przekazuje Wniosek o Udostępnianie Danych do realizacji. Wnioskowi mogą towarzyszyć dodatkowe informacje dotyczące trybu przygotowania Danych, zabezpieczenia Danych, itp.
- 6.8.2.5 Wnioski niekompletne, niewłaściwie sporządzone (np.: przesłane przez nieupoważnioną osobę lub dotyczące Danych z innej Jednostki organizacyjnej) Kierujący komórką DC zwraca nadawcy z podaniem powodów ich odesłania.
- 6.8.2.6 Udostępnienie danych na Wniosek Spółki GK PGE wymaga akceptacji Zarządu Spółki będącej właścicielem Danych lub osoby upoważnionej przez ten Zarząd Spółki do akceptacji Wniosku o udostępnianie Danych.
- 6.8.2.7 W przypadku udostępniania informacji na potrzeby postępowania prowadzonego przez organ państwowy stosuje się powszechnie obowiązujące przepisy prawa w tym zakresie.
- 6.8.3 REALIZACJA WNIOSKÓW O UDOSTĘPNIANIE DANYCH
- 6.8.3.1 Administrator wykonuje czynności związane z realizacją Wniosku o Udostępnianie Danych niezwłocznie, aby dotrzymać terminu wskazanego przez wnioskodawcę, a jeżeli nie jest to możliwe, w ciągu 2 dni określa planowany termin realizacji Wniosku.
- 6.8.3.2 W przypadku niejednoznaczności parametrów wskazanych we Wniosku o Udostępnianie Danych, Administrator może poprosić o uzupełnienie informacji Kierującego komórką DC.
- 6.8.3.3 Administrator realizując Wniosek o Udostępnianie Danych, wykonuje go zgodnie z najlepszą wiedzą, poprzez zadanie właściwych parametrów zapytania do Systemu. Weryfikacja poprawności realizacji Wniosku polega na sprawdzeniu poprawności zapytania o Dane (kryteria). Weryfikacja wyników realizacji Wniosku nie polega

- na analizie czy interpretacji uzyskanych danych wynikowych. Ewentualna weryfikacja danych wynikowych może zostać dokonana przez Spółkę po przekazaniu Danych przez Administratora.
- 6.8.3.4 W przypadku realizacji Wniosku składanego przez organ państwowy wymagane jest by przygotowany zestaw Danych do udostępnienia był zweryfikowany przez innego Administratora, celem zapewnienia poprawnej realizacji Wniosku pod względem zakresu udostępnianych Danych (weryfikacja na dwie pary oczu).
- 6.8.3.5 W przypadku, gdy nie jest możliwe pozyskanie Danych zgodnie z przekazanymi parametrami we Wniosku o Udostępnianie Danych (np. brak jest wiadomości e-mail ze wskazanego zakresu dat), Administrator niezwłocznie informuje o tym fakcie Kierującego komórką DC, przekazując szczegółowe wyjaśnienia, a ten informuje wnioskodawcę.
- 6.8.3.6 W przypadku konieczności bezpośredniego zabezpieczenia Danych z Komputera Biurowego pracującego Użytkownika – czynności te wykonuje Administrator w asyście Przełożonego Użytkownika lub innej osoby wskazanej we Wniosku.
- 6.8.3.7 W przypadkach szczególnych (np. popełnienie lub podejrzenie popełnienia przestępstwa) w celach dowodowych, sposób postępowania przy zabezpieczaniu i udostępnianiu Danych regulują zapisy *PROG 00116 Procedura Ogólna Zarządzania Incydentami Cyberbezpieczeństwa w GK PGE*.
- 6.8.4 PRZEKAZANIE DANYCH I DOKUMENTACJA
- 6.8.4.1 Pozyskane Dane Administrator Techniczny zabezpiecza pod względem Integralności i Poufności. Preferowane jest szyfrowanie mechanizmami PKI lub zaszyfrowane archiwum plików Hasłem o długości 12 znaków lub więcej. Jeżeli do szyfrowania użyto Hasła, to Administrator przekazuje je odbiorcy innym kanałem informacyjnym niż przekazywane Dane.
- 6.8.4.2 Administrator umieszcza zabezpieczone Dane zgodnie z wytycznymi zawartymi we Wniosku o Udostępnianie Danych. Dane należy zabezpieczyć przed nieuprawnionym Dostępem (np. Bezpieczna Koperta, szyfrowany Nośnik, fizyczne zabezpieczone pomieszczenie). Administrator odpowiada za zabezpieczenie Poufności i Integralności Danych do momentu przekazania ich odbiorcy.
- 6.8.4.3 Z przeprowadzonych czynności Administrator sporządza protokół udostępnienia Danych potwierdzający realizację zadań zgodnie z Wnioskiem o Udostępnianie Danych. Wnioskowane Dane wraz z protokołem Udostępnienia Danych przekazywane są przez Administratora:
- do Kierującego komórką DC, który obsługuje docelową korespondencję do wnioskodawcy (w przypadku, gdy Wniosek do CUW ICT o udostępnianie Danych składa organ państwowy),
 - do bezpośrednio wskazanego odbiorcy zgodnie z Wnioskiem o Udostępnianie Danych (w pozostałych przypadkach). Protokół musi zawierać zakres zabezpieczonych Danych i być przechowywany wraz z tymi Danymi. Odbiorca podpisując protokół potwierdza odbiór Danych. Od tej pory Odbiorca odpowiada za bezpieczeństwo przekazanych Danych.
- 6.8.4.4 Administrator Techniczny przekazuje protokół na adres skrzynki poczty korporacyjnej:
- odbiorcy,
 - Kierującego komórką DC,
 - bezpieczenstwo.pgesystemy@gkpge.pl,
- 6.8.4.5 Korespondencję związaną z realizacją Wniosków o Udostępnienie Danych przechowuje Kierujący komórką DC przez okres co najmniej 3 lat. Rejestr Udostępnianych Danych, zawiera poniższe informacje:
- Jednostka organizacyjna,
 - data wpłynięcia Wniosku,
 - osoba zgłaszająca,
 - źródło pozyskania wnioskowanych Danych, np. nazwa Systemu Teleinformatycznego, Komputera Biurowego, skrzynki pocztowej,
 - jeżeli wnioskowane Dane dotyczą Użytkownika to wymagane jest wskazanie danych pozwalających na jego identyfikację (adres email, imię i nazwisko, nr osobowy),
 - wskazanie okresu z jakiego mają być wnioskowane Dane,
 - data przekazania Danych,
 - imię i nazwisko przekazującego Dane,
 - imię i nazwisko odbierającego Dane,
 - uwagi,
 - kopie lub skany Wniosku i protokołu.
- 6.8.4.6 Informacje z Rejestru są udostępniane Spółkom na życzenie, po uzyskaniu akceptacji Kierującego komórką DC.

6.9 ZARZĄDZANIE OCHRONĄ DANYCH OSOBOWYCH W SYSTEMACH TELEINFORMATYCZNYCH

6.9.1 ZASADY OGÓLNE

- 6.9.1.1 Przetwarzanie Danych Osobowych z użyciem Systemów Teleinformatycznych, w tym projektowanie i wdrażanie takiego przetwarzania, odbywa się z uwzględnieniem aktualnie obowiązujących przepisów o ochronie Danych Osobowych, zapisów *PROG 00035 Procedura Ogólna – Wytyczne w zakresie ochrony danych osobowych w GK PGE* oraz regulacji wewnętrznych Spółek w tym zakresie, w tym także regulacji obowiązujących w GK PGE w zakresie bezpieczeństwa.
- 6.9.1.2 Wszelkie czynności dotyczące Danych Osobowych muszą być realizowane zgodnie z zapisami *PROG 00035 Procedura Ogólna – Wytyczne w zakresie ochrony danych osobowych w GK PGE* oraz regulacji wewnętrznych Spółek w tym zakresie i przepisów o ochronie danych osobowych, w tym RODO, a także zawartych umów regulujących przepływ Danych Osobowych
- 6.9.1.3 Dla uwzględnienia ochrony danych w fazie projektowania oraz domyślnej ochrony danych (art. 25 RODO), Administrator Danych Osobowych w zleceniach i zamówieniach, składanych CUW ICT na nowe systemy lub usługi, czy też na modyfikacje istniejących Systemów lub usług (w szczególności w kartach definicji inicjatywy), wskazuje wymagania ochrony Danych Osobowych konieczne do wdrożenia przy realizacji danego zamówienia lub zlecenia. Do określenia ww. wymagań Spółka oraz CUW ICT uwzględniają [Załącznik 2](#) Wymagania RODO do Systemu Teleinformatycznego.
- 6.9.1.4 CUW ICT pełni w stosunku do Spółek rolę Podmiotu Przetwarzającego na podstawie zawartych umów powierzenia przetwarzania Danych Osobowych określających rodzaje przetwarzanych Danych oraz sposób postępowania i obowiązki Podmiotu Przetwarzającego.
- 6.9.1.5 CUW ICT nie odpowiada za weryfikację prawa Użytkownika do czynności przetwarzania Danych Osobowych. Właściciel Danych, akceptując Wniosek o Dostęp do Systemów Teleinformatycznych o nadanie uprawnień, gwarantuje, że Użytkownik spełnia wszystkie wymagania zgodne z lokalnymi, korporacyjnymi i prawnymi regulacjami w obszarze przetwarzania Danych Osobowych w tym:
- a. posiadania przez Użytkownika stosownych upoważnień do przetwarzania Danych Osobowych,
 - b. ukończenia wymaganych szkoleń.
- Po otrzymaniu poprawnie zaakceptowanego Wniosku o Dostęp do Systemów Teleinformatycznych CUW ICT przystępuje do realizacji Wniosku bez dodatkowych weryfikacji.
- 6.9.1.6 W przypadku zaistnienia zmian formalnych (np. wycofania lub wygaśnięcia upoważnienia do przetwarzania Danych Osobowych lub wybranej kategorii Danych) Właściciel Danych zobowiązany jest złożyć Wniosek o modyfikację Dostępów Użytkownika zgodnie z zapisami punktu 6.5.
- 6.9.1.7 Każda Spółka w ramach przyjętych regulacji samodzielnie realizuje:
- a. obowiązki informacyjne względem osób, których Dane przetwarza,
 - b. weryfikację zasadności żądań i sposobów obsługi praw jednostki,
 - c. weryfikację posiadania przez Użytkownika stosownych upoważnień do przetwarzania Danych Osobowych i ukończenia wymaganych szkoleń, z zastrzeżeniem odmiennych postanowień zawartych w umowach łączących Spółkę i CUW ICT.
- 6.9.2 WSPARCIE W OBSŁUDZE WNIOSKÓW WYNIKAJĄCYCH Z PRZEPISÓW ODO
- 6.9.2.1 Wszystkie zadania zlecane do CUW ICT w obszarze Danych Osobowych realizowane są na podstawie Wniosku.
- 6.9.2.2 Informacje dotyczące Wniosków składanych przez Spółki oraz informacje związane z procesem obsługi Danych Osobowych należy traktować jako informacje szczególnie chronione zgodnie z regulacjami stosowanymi w Spółce.
- 6.9.2.3 Wnioski o udostępnienie Danych Osobowych na podstawie przepisów o ochronie danych osobowych, w tym RODO, realizowane są zgodnie z zapisami punktu 6.8.3
- 6.9.2.4 Wnioski o obsługę żądania dotyczą wszystkich zadań z obszaru przetwarzania Danych Osobowych zleczanych do CUW ICT innych niż udostępnienie Danych. W szczególności mogą to być Wnioski Spółki o aktualizację, usunięcie, Anonimizację lub ograniczenie przetwarzania Danych na żądanie osoby.
- 6.9.2.5 Wniosek o obsługę żądania może być złożony do zasobów, których właścicielem jest Jednostka organizacyjna i musi zawierać co najmniej poniższe informacje:
- a. Jednostka organizacyjna,
 - b. wskazanie jakich Danych Osobowych dotyczy Wniosek,
 - c. opis zadań dla CUW ICT jakich dotyczy Wniosek,
 - d. wskazanie podstawy prawnej wynikającej z art. 12-23 RODO
 - e. Dane osoby lub podmiotu, któremu należy przekazać informacje o realizacji Wniosku,
 - f. data przekazania Wniosku,
- 6.9.2.6 Wniosek o obsługę żądania może być kierowany przez Kierującego ODO i odbiorcę usługi ICT w Spółce:
- a. w formie papierowej bezpośrednio do Kierującego ODO w CUW ICT,

- b. w formie elektronicznej zaszyfrowanej lub zabezpieczonej podpisem elektronicznym bezpośrednio na skrzynkę poczty korporacyjnej Kierującego ODO w CUW ICT.
- 6.9.2.7 CUW ICT po stwierdzeniu kompletności Wniosku o obsługę żądania oraz braku zastrzeżeń co do uprawnienia Wnioskującego do wnioskowanych Danych, przekazuje Wniosek do realizacji. Wnioskowi mogą towarzyszyć dodatkowe informacje dotyczące trybu postępowania z Danymi Osobowymi.
- 6.9.2.8 Wnioski niekompletne, niewłaściwie sporządzone (tj. przesłane przez nieupoważnioną osobę lub dotyczące Zasobów z innej Jednostki organizacyjnej) CUW ICT zwraca nadawcy z podaniem powodów ich odesłania.
- 6.9.3 REALIZACJA I DOKUMENTOWANIE WNIOSKÓW O OBSŁUGĘ ŻĄDANIA WYNIKAJĄCYCH Z PRZEPISÓW ODO
- 6.9.3.1 Administrator wykonuje czynności związane z realizacją Wniosku o obsługę żądania niezwłocznie, aby dotrzymać terminu wskazanego przez wnioskodawcę, a jeżeli nie jest to możliwe, w ciągu 2 dni określa planowany termin realizacji Wniosku.
- 6.9.3.2 W przypadku niejednoznaczności parametrów wskazanych we Wniosku o obsługę żądania Administrator może poprosić o uzupełnienie informacji przez wnioskującą Jednostkę organizacyjną.
- 6.9.3.3 Administrator realizując Wniosek o obsługę żądania, wykonuje go zgodnie z najlepszą wiedzą, dobierając środki techniczne adekwatne do celu wskazanego we Wniosku. Weryfikacja wyników realizacji Wniosku polega na analizie skuteczności osiągnięcia celu.
- 6.9.3.4 W przypadku, gdy nie jest możliwa realizacja zadań wskazanych we Wniosku o obsługę żądania (np. grozi to utratą Integralności Systemu Teleinformatycznego), Administrator niezwłocznie informuje o tym fakcie wnioskodawcę, przedstawiając propozycję realizacji Wniosku w inny sposób.
- 6.9.3.5 Z przeprowadzonych czynności Administrator sporządza protokół obsługi żądania potwierdzający realizację zadań zgodnie z Wnioskiem o obsługę żądania i ustaleniami z wnioskującym.
- 6.9.4 **Administrator przekazuje** protokół **na adres skrzynki poczty korporacyjnej:**
- a. Wnioskującego,
 - b. ODO w CUW ICT,
 - c. Kierującego komórką DC,
 - d. bezpieczenstwo.pgesystemy@gkpge.pl.
- 6.9.4.1 Korespondencję związaną z realizacją Wniosków o obsługę żądania przechowuje CUW ICT przez okres co najmniej 3 lat na dedykowanym Zasobie sieciowym. Rejestr obsługi żądań, zawiera poniższe informacje:
- a. Jednostka organizacyjna,
 - b. data wpłynięcia Wniosku,
 - c. osoba zgłaszająca,
 - d. zakres zadań,
 - e. data realizacji,
 - f. imię i nazwisko realizującego zadanie,
 - g. uwagi,
 - h. Kopie lub skany Wniosku i protokołu,
- 6.9.4.2 Informacje z Rejestru są udostępniane niezwłocznie, nie później niż w terminie 5 dni roboczych na wniosek Kierującego ODO lub odbiorcy usługi.

6.10 ZARZĄDZANIE NOŚNIKAMI INFORMACJI

6.10.1 ZASADY OGÓLNE

6.10.1.1 Wszystkie Nośniki Informacji podlegają rejestracji.

6.10.1.2 Każda Spółka, która we własnym zakresie kupuje Nośniki Informacji (poza CUW ICT) ma obowiązek wprowadzenia mechanizmów zarządzania Nośnikami Informacji w celu wprowadzenia nadzoru nad Dostępem do Danych przechowywanych i przetwarzanych na tych Nośnikach. Spółki mają możliwość skorzystania z bazy CMDB prowadzonej przez CUW ICT.

6.10.1.3 CUW ICT utrzymuje centralny rejestr Nośników Informacji w bazie CMDB, do którego wprowadza informacje o Nośnikach którymi zarządza lub administruje.

6.10.1.4 Każdy Nośnik musi mieć numer seryjny producenta w celu jednoznacznej jego identyfikacji. W przypadku braku numeru seryjnego Nośnika należy umieszczać na nim dodatkowy Identyfikator, który w jednoznaczny sposób go oznaczy i wskaże jego opis w rejestrze.

6.10.1.5 Dane muszą być chronione na takim samym poziomie niezależnie od Nośnika, na jakim są przechowywane.

6.10.1.6 Każdy Użytkownik jest zobowiązany do zabezpieczenia wszelkich Nośników Informacji podlegających ochronie znajdujących się na stanowisku pracy.

6.10.1.7 Poufność danych przechowywanych na Nośnikach może być realizowana poprzez:

- a. szyfrowanie symetryczne,

- b. szyfrowanie asymetryczne,
 - c. sejfy, szafy pancerne, pomieszczenia zapewniające kontrolę Dostępu.
- 6.10.1.8 Integralność danych przechowywanych na Nośnikach może być realizowana poprzez:
- a. przechowywanie skrótów,
 - b. MAC (Message Authentication Code),
 - c. podpis elektroniczny,
 - d. Bezpieczne Koperty.
- 6.10.1.9 Dopuszcza się do użytku jedynie Nośniki przekazane przez Spółki lub CUW ICT. Ze względów bezpieczeństwa zakazane jest wykorzystywanie w Sieci Komputerowej GK PGE Nośników innych niż służbowe.
- 6.10.2 EKSPLOATACJA
- 6.10.2.1 Każdy Nośnik wprowadzany do eksploatacji należy sprawdzić za pomocą aktualnego oprogramowania antywirusowego zawierającego najnowsze bazy antywirusowe lub innego oprogramowania przeciwdziałającego złośliwemu oprogramowaniu. Fakt sprawdzenia musi być odnotowany w bazie CMDB.
- 6.10.2.2 W celu zachowania Poufności i Integralności Danych każdy dysk przenośny lub pamięci przenośne USB (pendrive) przed wprowadzeniem do eksploatacji musi zostać zaszyfrowany poprzez zastosowanie środków kryptograficznych wskazanych przez CUW ICT. Zasyfrowanie Nośnika musi się odbyć przed przeniesieniem danych na Nośnik. Powyższe nie dotyczy Systemów, dla których wprowadzenie zabezpieczenia w postaci szyfrowania będzie miało negatywny wpływ na stabilną pracę Systemu.
- 6.10.2.3 Z Nośników wycofywanych z eksploatacji należy niezwłocznie usunąć wszelkie Dane w sposób wskazany w punkcie 6.10.5 Procedury. Przed usunięciem danych należy podjąć decyzję o ich ewentualnej archiwizacji.
- 6.10.2.4 Wniosek o archiwizację danych jest realizowany zgodnie z pkt 6.10.4.5.
- 6.10.3 REALIZACJA NAPRAW
- 6.10.3.1 Komórka organizacyjna dokonująca zakupu Nośników i urządzeń komputerowych musi zapewnić w umowach z dostawcami odpowiednie warunki gwarancji pod względem zachowania Poufności i Integralności Danych na Nośniku w przypadku jego napraw. Urządzenia zawierające Nośnik powinny być nabywane w opcji umożliwiającej zachowanie Nośnika przez Spółkę w przypadku wymiany sprzętu na inny.
- 6.10.3.2 W ramach przygotowania do naprawy uszkodzonego urządzenia ICT:
- a. urządzenia, których Nośniki są szyfrowane, mogą być przekazane bez konieczności usuwania danych pod warunkiem, że w trakcie naprawy nie będą dostępne klucze szyfrujące pozwalające na odzyskanie Danych,
 - b. dla urządzeń, z których Nośniki nie mogą być usunięte a Dane nie są szyfrowane, należy usunąć Dane z Nośników w sposób wskazany w punkcie 6.10.5 Procedury.
- 6.10.3.3 W przypadku braku możliwości usunięcia Danych z Nośnika, na którym Dane nie są zaszyfrowane naprawa powinna być realizowana na terenie Jednostki organizacyjnej pod nadzorem wyznaczonego Pracownika lub Kontraktora i osoby korzystającej z nośnika.
- 6.10.3.4 Na dokumencie przekazania do naprawy należy umieścić numer seryjny Nośnika. W przypadku braku numeru seryjnego należy zamieścić opis, który jednoznacznie identyfikuje Nośnik. Przy zwrocie należy sprawdzić czy numer seryjny Nośnika bądź jego opis zgadza się z numerem seryjnym znajdującym się na dokumencie przekazania do naprawy.
- 6.10.3.5 W przypadku wymiany na nowy Nośnik należy go zarejestrować w rejestrze Bazy CMDB. Jeśli stary Nośnik zawierał Dane, należy żądać zwrotu Nośnika i przeprowadzić proces usunięcia danych zgodnie z wymaganiami zamieszczonymi w punkcie 6.10.5 Procedury oraz zmodyfikować opis starego Nośnika w Bazie CMDB.
- 6.10.3.6 Nośnik po naprawie należy sprawdzić za pomocą aktualnego oprogramowania antywirusowego zawierającego najnowsze bazy antywirusowe.
- 6.10.4 TRANSPORT I SKŁADOWANIE
- 6.10.4.1 Nośniki należy składować w następujący sposób:
- a. Nośniki i urządzenia komputerowe wycofane z eksploatacji muszą być pozbawione Danych zgodnie z wymaganiami punktu 6.10.5 Procedury,
 - b. dla Nośników przechowujących Dane:
 - Nośniki flash zaszyfrowane przed wprowadzeniem do eksploatacji oraz pozostałe Nośniki w postaci zaszyfrowanej wymagają zagwarantowania wyłączenia Dostępu do kluczy szyfrujących pozwalających na odszyfrowanie danych,
 - Nośniki flash oraz Nośniki niezaszyfrowane muszą być zabezpieczone przed nieuprawnionym dostępem w pomieszczeniach chronionych. Zaleca się stosowanie dodatkowo zabezpieczeń, o których mowa w punkcie 6.10.4.9 Procedury,
 - z Nośników przeznaczonych do utylizacji Dane muszą być niezwłocznie usunięte.

- 6.10.4.2 Nośniki należy przechowywać w miejscach zabezpieczających je przed kradzieżą, zniszczeniem, modyfikacją lub uszkodzeniem. W szczególności Nośniki muszą być zabezpieczone przed niekorzystnym wpływem pola magnetycznego.
- 6.10.4.3 Nośniki przenoszone pomiędzy lokalizacjami muszą podlegać ochronie kryptograficznej uniemożliwiającej odczyt Danych przez osoby nieuprawnione. W trakcie transportu należy stosować również środki zabezpieczające zapewniające Poufność i Integralność danych.
- 6.10.4.4 Na Wniosek Spółki możliwe jest zdeponowanie przez CUW wskazanych Nośników lub całych urządzeń zawierających Nośniki w sposób zabezpieczający je przed naruszeniem Integralności danych i nieuprawnionym dostępem. Zabezpieczenie takie jest zalecane w sytuacji, gdy urządzenie lub Nośnik zawierające Dane wymaga transportu lub dłuższego składowania, lecz nie została jeszcze podjęta decyzja dotycząca dalszego postępowania z Nośnikiem. Do zabezpieczania Nośników zalecane są jednorazowe Bezpieczne Koperty lub worki bankowe zabezpieczone jednorazowymi plombami z unikalnymi numerami seryjnymi. Brak oznak naruszenia zabezpieczenia oraz potwierdzenie właściwych numerów seryjnych wskazuje na brak ingerencji osób w zawartość depozytu.
- 6.10.4.5 Zabezpieczenie Nośników odbywa się na Wniosek Spółki podpisany przez członka Organów Spółki lub Kierującego komórką ds. ICT Spółki. Wniosek o zabezpieczenie Danych i zdeponowanie sprzętu teleinformatycznego należy złożyć nie później niż w momencie zwrotu urządzeń komputerowych przez Użytkownika. Wniosek o zabezpieczenie Nośników użytkowanych w Spółkach może zostać złożony również przez Kierującego komórką właściwą ds. strategii ICT w PGE S.A. lub Kierującego komórką właściwą ds. bezpieczeństwa w PGE S.A., każdorazowo wymaga on akceptacji członka Organów Spółki lub Kierującego komórką ds. ICT Spółki, której dotyczy wniosek.
- 6.10.4.6 Jeżeli osoby nadzorujące Nośniki same podejmą decyzję o zastosowaniu dodatkowego zabezpieczenia w postaci Bezpiecznych Kopert lub worków bankowych Wniosek Spółki nie jest wymagany.
- 6.10.4.7 Urządzenia komputerowe oraz Nośniki informacji są przechowywane przez CUW ICT przez okres 1 roku, chyba że we wniosku o przechowywanie wskazano datę zakończenia przechowywania. Przed zakończeniem okresu przechowywania osoby uprawnione mogą złożyć Wniosek o przechowywanie, w którym określą inną datę do której urządzenie ma być przechowywane.
- 6.10.4.8 Urządzenia komputerowe oraz Nośniki informacji zdeponowane przez CUW ICT, dla których zgłoszono Wniosek o zabezpieczenie danych i zdeponowanie sprzętu teleinformatycznego, muszą być przekazane do Kierującego komórką DC przesyłką kurierską w Bezpiecznej Kopercie, chyba że wnioskujący wskazał inne zalecenia we Wniosku o przechowywanie.
- 6.10.4.9 Zabezpieczenie i zdeponowanie Nośników odbywa się komisyjnie zgodnie z wymaganiami określonymi we Wniosku. Zabezpieczenie i zdeponowanie odbywa się poprzez zabezpieczenie Nośnika lub urządzenia w Bezpiecznej Kopercie, w sejfie. Protokół depozytu musi zawierać co najmniej:
- opis zawartości depozytu wraz z określeniem skąd pochodzą Nośniki, numerami seryjnymi i inwentarzowymi urządzeń, przeznaczeniem urządzeń, nazwami sieciowymi, Identyfikatorem Użytkownika itp.,
 - datę i godzinę zabezpieczenia Nośnika,
 - numer Wniosku o zabezpieczenie Nośnika lub innej udokumentowanej formy polecenia,
 - podpisy członków komisji,
 - oznaczenie Spółki będącej właścicielem Danych – uprawnionej do decydowania o postępowaniu z depozytem,
 - warunki otwarcia depozytu (np. czas i osoby upoważnione).
- 6.10.4.10 Protokół musi być wykonany w przynajmniej dwóch kopiach. Jedna kopia musi być przechowywana wewnątrz zabezpieczenia wraz z Nośnikiem na wypadek zaginięcia pozostałych egzemplarzy protokołu. Druga Kopia musi być przechowywana wraz z depozytem w celu informowania o zawartości depozytu. Pozostałe kopie są przechowywane zgodnie z zasadami obowiązującymi w Spółce.
- 6.10.4.11 W przypadku zmiany miejsca przechowywania lub transportu depozytu do protokołu przekazania powinna być dołączana kopia protokołu depozytu, o ile regulacje Spółki nie stanowią inaczej.
- 6.10.4.12 Kierujący komórką odpowiedzialną za Cyberbezpieczeństwo w CUW ICT prowadzi ewidencję przechowywanego sprzętu teleinformatycznego, która zawiera co najmniej:
- oznaczenie urządzenia tj.: właściciel sprzętu – Spółka, nr identyfikacyjny SAP, Identyfikator EK, Grupa sprzętu, Model, Nr Seryjny w zakresie opisanym na protokole depozytu,
 - informacje o ostatnim Użytkowniku Komputera Biurowego lub cyfrowego Nośnika Informacji,
 - informację o wnioskującym o przechowywanie sprzętu teleinformatycznego,
 - datę rozpoczęcia przechowywania,
 - planowaną datę zakończenia przechowywania,

f. rzeczywistą datę zakończenia przechowywania.

6.10.5 USUWANIE DANYCH I UTYLIZACJA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI

- 6.10.5.1 Usuwanie danych z Nośnika ma na celu zabezpieczenie tych Danych przed nieuprawnionym dostępem osób, które będą miały dostęp do Nośnika w przyszłości.
- 6.10.5.2 Usuwanie danych z Nośnika jest niezbędne za każdym razem, kiedy zmieniany jest sposób korzystania z Nośnika (np. przekazanie Komputera Biurowego innemu Użytkownikowi).
- 6.10.5.3 Usuwanie danych z Nośników przeznaczonych do utylizacji, odsprzedaży, przesyłanych do podwykonawców w celu realizacji napraw lub innych czynności realizowanych bez nadzoru CUW, w zależności od jego typu i stanu należy wykonać w następujący sposób:

Typ Nośnika	Sprawny - możliwy do dalszej eksploatacji	Uszkodzony – przeznaczony do utylizacji
Dysk HDD	Metoda programowa	<ul style="list-style-type: none"> Niszczenie fizyczne, Degaussing
Pamięć flash, dysk SSD	Zaszyfrowany przed wprowadzeniem do eksploatacji: <ul style="list-style-type: none"> TAK – Metoda programowa NIE – Niszczenie fizyczne 	Niszczenie fizyczne
CD-ROM, DVD-ROM	Niszczenie fizyczne	Niszczenie fizyczne
CD-RW, DVD-RW	Metoda programowa	Niszczenie fizyczne
Pamięć taśmowa	Metoda programowa	<ul style="list-style-type: none"> Niszczenie fizyczne, Degaussing

a. metoda programowa:

- trzykrotne nadpisanie całej przestrzeni adresowej: najpierw dowolnym wzorcem, następnie jego dopełnieniem, a na koniec losowym ciągiem.

b. niszczenie fizyczne – niszczenie fizyczne na całej powierzchni Nośnika gwarantujące uszkodzenie Nośnika w sposób uniemożliwiający odczytanie jakiegokolwiek informacji. Uszkodzenie powierzchni można wykonać poprzez spalenie, stopienie, starcie powierzchni nośnej. Dla niszczonek Nośników zaleca się stosowanie urządzeń spełniających, co najmniej 5 stopień bezpieczeństwa zgodnie z normą DIN 66399 ze względu na duże prawdopodobieństwo przechowywania na Nośniku danych osobowych.

c. degaussing – metoda fizycznego niszczenia Nośników magnetycznych poprzez ich rozmagnesowanie. Stosowany degausser MUSI wytwarzać pole magnetyczne o następujących parametrach: 10000 gaussów.

6.10.5.4 W każdym przypadku, w którym są wątpliwości co do skuteczności mechanizmu usunięcia Danych, należy powtórzyć czynność usunięcia Danych lub poddać Nośnik operacji niszczenia fizycznego.

6.10.5.5 Operacja usunięcia danych musi zostać odnotowana w rejestrze Nośników Informacji w Bazie CMDB.

6.10.5.6 Utylizacja Nośników ma na celu fizyczne zniszczenie Nośników w sposób potwierdzający bezpieczne i trwałe usunięcie Danych oraz możliwość zdjęcia Nośników z ewidencji materiałowej Spółki.

6.10.5.7 W ramach utylizacji Nośników wymagane jest, aby:

- przed przekazaniem do utylizacji należy sprawdzić, czy z Nośnika usunięto wszelkie Dane w sposób uniemożliwiający ich odzyskanie,
- w przypadku braku możliwości usunięcia danych w sposób trwały Nośnik na czas składowania i transportu należy zabezpieczyć Nośnik zgodnie z zapisami punktu 6.10.4.4, a transport i utylizacja Nośników muszą odbywać się pod nadzorem Pracownika lub Kontraktora w Spółce, zabezpieczającego Nośniki przed nieuprawnionym dostępem.

6.10.5.8 Dokumentowanie procesu utylizacji.

- przed przekazaniem Nośników do utylizacji należy wykonać spis Nośników przeznaczonych do utylizacji zawierający ich numery seryjne,
- w ramach utylizacji numery utylizowanych Nośników powinny być oznaczane na spisie,
- spis z oznaczonymi Nośnikami, które uległy utylizacji musi być załącznikiem do protokołu z przeprowadzenia utylizacji,
- na podstawie protokołu z utylizacji wprowadzane są zmiany w rejestrze Nośników Informacji w bazie CMDB.

6.10.5.9 Usuwanie Danych lub utylizowanie Nośników może być przez poszczególne Spółki realizowane we własnym zakresie, w oparciu o regulacje wewnętrzne tych Spółek, przy zachowaniu wymogu dokumentowania takich czynności z zastosowaniem dedykowanych rejestrów oraz z zachowaniem zgodności z Procedurą.

6.11 ZARZĄDZANE KOMPUTERAMI BIUROWYMI

- 6.11.1 Użytkownikowi przysługuje komputer biurowy niezbędny do realizacji powierzonych obowiązków służbowych.
- 6.11.2 Rodzaj i standard Komputerów Biurowych wraz z akcesoriami określa Komórka organizacyjna CUW ICT odpowiedzialna za infrastrukturę biurową w CUW ICT, z uwzględnieniem wymogów Bezpieczeństwa Informacji, a zatwierdza Kierujący komórką właściwą ds. strategii ICT GK PGE.
- 6.11.3 Czynności wydawania, odbierania Komputerów Biurowych wraz z akcesoriami są realizowane na Wniosek rejestrowany w SOZ. Wniosek kierowany jest do realizacji po pozytywnym zakończeniu procesu akceptacji, o którym mowa w pkt 6.4 przy czym:
 - 6.11.3.1 Na pierwszym poziomie akceptacji występuje:
 - a. w przypadku Pracownika, Kontraktora lub Osoby Trzeciej – Kierownik Komórki organizacyjnej, na rzecz której realizuje zadania Pracownik, Kontraktor lub Osoba Trzecia,
 - b. w przypadku Kierującego komórką – członek Organów Spółki (lub osoba przez niego upoważniona), któremu dany Kierujący komórką podlega,
 - c. w przypadku członka Organu Spółki – osoba pełniąca funkcję lub rolę Kierującego komórką właściwą ds. obsługi Organów Spółki.
 - 6.11.3.2 Na drugim poziomie akceptacji – osoba wskazana na Liście Akceptujących.
- 6.11.4 Wydanie Komputera Biurowego wraz z akcesoriami potwierdzone jest podpisaniem protokołu wydania sprzętu. Dla Osób Trzecich Komputery Biurowe są wpisywane na stan Pracownika lub Kontraktora z Komórki organizacyjnej wskazanego we Wniosku przez Kierownika i udostępnienie jest realizowane na czas określony nie dłuższy niż 1 rok. Odebranie Komputera Biurowego jest dokumentowane na protokole zwrotu sprzętu.
- 6.11.5 W celu wykonywania czynności administracyjnych rekomenduje się Zdalny Dostęp do udostępnionych Komputerów Biurowych przez administratorów CUW ICT.
- 6.11.6 W celu zapewnienia bezpieczeństwa, standardowo Użytkownik nie posiada praw administracyjnych do wykorzystywanego Komputera Biurowego.
- 6.11.7 Wszelkich zmian konfiguracji Komputerów Biurowych i jego stałej lokalizacji dokonują wyłącznie CUW ICT. Zabroniona jest samodzielna rozbudowa oraz modyfikacja udostępnionych Komputerów Biurowych przez Użytkownika.
- 6.11.8 Administrator Techniczny zobowiązany jest do ograniczenia Użytkownikom dostępu do programów narzędziowych umożliwiających zmianę parametrów Użytkowanego Zasobu ICT. Użytkownicy nie mogą mieć możliwości samodzielnego modyfikowania ustawień w Systemach operacyjnych.
- 6.11.9 Uprawnienia do serwisowego dostępu zdalnego do stacji roboczych posiadają wyłącznie Administratorzy, których Wnioski o to Uprawnienie zostały zaakceptowane zgodnie z zapisami Procedury.
- 6.11.10 Uprawnieni Administratorzy wykonują czynności serwisowe na Komputerze Biurowym na podstawie zgłoszenia Użytkownika w SOZ, zweryfikowanego przez Service Desk i po uzyskaniu zgody tego Użytkownika.
- 6.11.11 Działania Administratorów przy czynnościach Zdalnego Dostępu do stacji roboczych są rejestrowane i archiwizowane dla celów kontrolnych i sprawozdawczych.
- 6.11.12 CUW ICT definiuje standardy oprogramowania stosowanego w GK PGE. Oprogramowanie aktualnie dopuszczone do stosowania jest publikowane na Liście Oprogramowania. W celu zgłoszenia konieczności nowego oprogramowania należy złożyć dedykowany Wniosek w SOZ.
- 6.11.13 W przypadku obowiązywania innych regulacji wewnętrznych w tym zakresie dopuszcza się realizowanie procesu zarządzania Komputerami Biurowymi zgodnie z regulacjami wewnętrznymi Spółek GK PGE.

6.12 BEZPIECZEŃSTWO URZĄDZEŃ MOBILNYCH

- 6.12.1 Dostęp do usług z Urządzeń Mobilnych jest nadawany i odbierany na podstawie Wniosków w SOZ
- 6.12.2 CUW ICT realizuje czynności wydawania, odbierania Urządzeń Mobilnych wraz z akcesoriami na Wniosek rejestrowany w SOZ. Wniosek kierowany jest do realizacji po pozytywnym zakończeniu Procesu akceptacji, o którym mowa w pkt 6.4, przy czym:
 - 6.12.2.1 na pierwszym poziomie akceptacji występuje:
 - a. w przypadku Pracownika, Kontraktora lub Osoby Trzeciej – Kierownik komórki organizacyjnej na rzecz, której realizuje zadania Pracownik, Kontraktor lub Osoba Trzecia,
 - b. w przypadku Kierującego komórką – członek Organów Spółki (lub osoba przez niego upoważniona), któremu dany Kierujący komórką podlega,

- c. W przypadku członka Organu Spółki – osoba pełniącą funkcję lub rolę Kierującego komórką właściwą ds. obsługi Organów Spółki.
- 6.12.2.2 na drugim poziomie akceptacji – osoba wskazana na Liście Akceptujących.
- 6.12.3 CUW ICT prowadzi ewidencję wydanych Urządzeń Mobilnych i udostępnia te wykazy wg potrzeb Użytkownikom.
- 6.12.4 Rodzaj i standard Urządzeń Mobilnych wraz z akcesoriami określa CUW ICT, , z uwzględnieniem wymogów Bezpieczeństwa Informacji, a zatwierdza CIO. CUW ICT prowadzi ewidencję dopuszczonych Urządzeń Mobilnych oraz Systemów operacyjnych mobilnych i udostępnia te wykazy wg potrzeb Użytkownikom.
- 6.12.5 Każde Urządzenie Mobilne wykorzystywane w celu uzyskania Dostępu do Sieci Korporacyjnej musi posiadać:
- a. zainstalowany, zarejestrowany i skonfigurowany System monitorujący bezpieczeństwo i stan urządzeń, wskazany przez CUW ICT,
 - b. uruchomioną blokadę ekranu z wykorzystaniem kodu PIN,
 - c. szyfrowanie przestrzeni pamięci urządzenia z wykorzystaniem mechanizmu systemowego,
 - d. szyfrowanie zewnętrznej pamięci masowej,
 - e. blokadę synchronizacji danych zawartych na urządzeniu z usługami Apple,
 - f. blokadę Konta Google dla urządzeń Android.
- 6.12.6 DC w CUW ICT może na pisemny Wniosek członka Organów Spółki danej Spółki:
- a. dopuścić Urządzenie niewymienione na liście urządzeń dopuszczonych do korzystania z Sieci Korporacyjnej,
 - b. wyrazić zgodę na odstąpienie od stosowania wybranych zabezpieczeń. Realizacja zaakceptowanych Wniosków o odstąpienie wybranych zabezpieczeń realizowane są w oparciu o złożony w SOZ Wniosek z załączoną kopią zgody.
- 6.12.7 CUW ICT na stronie sd.gkpge.pl publikuje Listę Oprogramowania zawierającą oprogramowanie dozwolone do instalowania i używania na Urządzeniach Mobilnych. Oprogramowanie zainstalowane bezpośrednio przez producenta Urządzenia stanowi integralną część Systemu operacyjnego i nie podlega publikacji na Liście Oprogramowania.
- 6.12.8 Na Urządzeniach Mobilnych mogą zostać zainstalowane dodatkowe aplikacje, lub uruchomione funkcjonalności niezbędne do korzystania z tych Usług. Użytkownik zobowiązany jest udostępnić Urządzenie Mobilne na żądanie CUW ICT.
- 6.12.9 Użytkownik nie ma prawa ingerować w System operacyjny Urządzenia Mobilnego (w szczególności obchodzić jego wbudowanych zabezpieczeń), jak również stosować innych Systemów operacyjnych, niż są zatwierdzone i dopuszczone do użytku przez Kierującego komórką DC.
- 6.12.10 Użytkownik zobowiązany jest do przestrzegania podstawowych zasad bezpieczeństwa, a w szczególności do:
- a. nieudostępniania Urządzenia Mobilnego osobom postronnym,
 - b. zabezpieczenia Urządzenia Mobilnego przed nieuprawnionym dostępem osób postronnych,
 - c. zabezpieczenia Urządzenia Mobilnego przed uszkodzeniem, zniszczeniem, utratą lub kradzieżą,
 - d. nieingerowania w System operacyjny Urządzenia Mobilnego (w szczególności obchodzenia jego wbudowanych zabezpieczeń), jak również stosowania innych Systemów operacyjnych niż oryginalny Urządzenia.
- 6.12.11 Użytkownikowi zabrania się:
- a. dokonywania zmian w konfiguracji udostępnionego Urządzenia Mobilnego, które mogłyby skutkować naruszeniem zasad bezpieczeństwa lub utratą gwarancji producenta,
 - b. konfiguracji prywatnych Kont Google, Samsung, Apple oraz innych usług na urządzeniach służbowych,
 - c. korzystania z niezabezpieczonych – otwartych sieci Wi-Fi,
 - d. korzystania ze sprzętu służbowego do celów prywatnych,
 - e. korzystania z prywatnej Karty SIM w służbowych Urządzeniach,
 - f. korzystania ze służbowej Karty SIM w prywatnych Urządzeniach,
 - g. umieszczanie drugiej - prywatnej karty SIM w urządzeniach posiadających technologię typu DUAL-SIM,
 - h. włączania przekierowania rozmów na telefony prywatne.

6.13 BEZPIECZEŃSTWO USŁUG SIECIOWYCH

6.13.1 ZASADY OGÓLNE

6.13.1.1 Zasoby Sieci Korporacyjnej udostępniane są zgodnie z zasadą minimum koniecznego oznaczającą udostępnianie minimalnych uprawnień wystarczających do skutecznej realizacji danego zadania.

6.13.1.2 Za zarządzanie bezpieczeństwem Sieci Korporacyjnej na potrzeby Spółki odpowiedzialny jest Administrator Techniczny sieci.

- 6.13.1.3 W urządzeniach sieciowych muszą być wyłączone wszystkie potencjalnie niebezpieczne usługi sieciowe, które są zbędne z punktu widzenia architektury i funkcjonalności konkretnego rozwiązania.
- 6.13.1.4 Administrator Techniczny obsługujący Sieć Korporacyjną musi stosować się do poniższych zaleceń:
- wykorzystując podsieci należy logicznie rozdzielać serwery od stacji roboczych i drukarek,
 - dostęp do funkcji administracyjnych Zasobu ICT musi być realizowany w sposób odpowiednio zabezpieczony,
- 6.13.1.5 Bezpieczeństwo na styku sieci LAN z siecią Internet / WAN zapewnia się poprzez:
- stosowanie zapory sieciowej,
 - wydzielenie segmentu sieci, strefy zdemilitaryzowanej (DMZ), w celu lokalizacji serwerów usług sieciowych udostępnianych w sieci Internet,
 - stosowanie technologii filtrującej pozwalającej na zablokowanie dostępu do niebezpiecznych domen i adresów,
 - ograniczenie ruchu do usług niezbędnych do prawidłowej komunikacji (minimum raz w roku właściwy Administrator Techniczny musi dokonać przeglądu otwartych portów i zablokować nieużywane oraz zbędne),
 - zastosowanie blokady bezpośredniego dostępu stacji roboczych do Internetu, zaimplementowanej w regułach dostępu na urządzeniach firewall,
 - tworzenie konfiguracji węzła, w ramach którego należy przyjąć zasady:
 - ochrony wewnętrznej sieci informatycznej przed nieautoryzowanym dostępem z zewnątrz,
 - ochrony przed próbami ataku z sieci zewnętrznej, jak również przed próbami zmodyfikowania jej konfiguracji z wewnętrznej sieci,
 - ochrony Poufności i Integralności przechowywanych i przesyłanych informacji,
 - ochrony przed atakami zaburzającymi dostępność komponentów Systemów informatycznych (ataki typu denial-of-service),
 - ochrony przed nieautoryzowanym przeprowadzaniem analizy sieci informatycznej,
 - zdarzenia związane z działaniem węzła są zapisywane w dokumentacji Zasobu ICT, a ich analizę przeprowadza właściwy Administrator Techniczny.
- 6.13.1.6 W przypadku stwierdzenia zagrożenia dla bezpiecznej pracy węzła dostępowego, właściwy Administrator Techniczny zobowiązany jest zablokować połączenia pomiędzy Internetem / WAN i siecią wewnętrzną LAN.
- 6.13.1.7 Zabronione są wszelkie działania Użytkowników zmierzające do destabilizacji pracującego w sieci sprzętu komputerowego, jak również wykonywanie przez Użytkowników prób podsłuchu ruchu w sieci (inwigilowanie, monitorowanie lub podglądu operacji).
- 6.13.1.8 Na Administratorach spoczywa obowiązek konfiguracji ustawień połączeń sieciowych tak, aby nieaktywne sesje były zamykane po przekroczeniu zdefiniowanego limitu czasu, który wynosi 30 min. W celu ponownego nawiązania sesji Użytkownik musi się ponownie Uwierzytelnić. W przypadku, gdy przerwanie sesji może spowodować utratę przetwarzanych danych w Systemie, dopuszcza się odstępstwo od stosowania zapisów niniejszego punktu.
- 6.13.1.9 Ruch sieciowy podlega ciągłemu monitorowaniu pod kątem wykrywania i przeciwdziałania zagrożeniom bezpieczeństwa Teleinformatycznego w zakresie:
- ataków cybernetycznych,
 - szkodliwego oprogramowania,
 - wycieku danych.
- 6.13.1.10 W Sieci Korporacyjnej na styku z innymi sieciami wymagana jest obecność zapory sieciowej typu firewall. Administrator sieci odpowiada za prawidłową konfigurację reguł filtracji ruchu w zaporze firewall. Ruch powinien zostać ograniczony do minimum w kontekście wymagań co do funkcjonalności Sieci Korporacyjnej oraz charakteru ruchu przesyłanego za jej pośrednictwem.
- 6.13.1.11 Wymagana jest separacja sieci ICT od sieci OT zgodnie z poniższymi zasadami:
- preferowana jest fizyczna separacja sieci ICT i OT,
 - ruch pomiędzy sieciami OT i ICT powinien być kontrolowany i ograniczony do niezbędnego minimum,
 - sieć OT nie może mieć bezpośredniego wyjścia do Internetu, w razie konieczności ruch taki zestawiany jest przez korporacyjny styk z Internetem ICT,
 - w razie konieczności Dostęp VPN do obszaru OT powinien odbywać się z wykorzystaniem VPN ICT i stacji przesiadkowych, a cały ruch powinien być nagrywany.
- 6.13.1.12 Dostęp sieciowy do urządzeń sieciowych w celach administracyjnych możliwy jest jedynie za pośrednictwem połączenia szyfrowanego z użyciem protokołu SSH lub SSL. Dostęp do urządzeń sieciowych za pośrednictwem protokołu SSH, SSL i SNMP jest kontrolowany i ograniczony do największej możliwej grupy osób i Systemów.

- 6.13.1.13 Wymagane jest, aby w kontekście protokołu SNMP stosowany był protokół SNMP w wersji 3 (SNMPv3). Komunikacja za pośrednictwem protokołu SNMP musi być szyfrowana, a komponenty muszą podlegać wzajemnemu Uwierzytelnieniu.
- 6.13.1.14 Wymagane jest, aby dynamiczne protokoły routingu dla urządzeń Sieci WAN zapewniały wzajemne Uwierzytelnienie pomiędzy urządzeniami.
- 6.13.1.15 Zaleca się, aby każde urządzenie sieciowe wyposażone było w dwa rodzaje interfejsów, spośród których jeden przeznaczony jest wyłącznie do celów administracyjnych, a drugi obsługuje zwykły ruch sieciowy. Działania administracyjne, w szczególności zmiana konfiguracji urządzenia, powinna być wykonywana za pośrednictwem specjalnie wydzielonego w tym celu interfejsu urządzenia fizycznego lub logicznego.
- 6.13.1.16 Zdalny Dostęp do urządzeń sieciowych realizowany jest w oparciu o VPN SSL lub IPSEC. Szczegóły techniczne stosowanych mechanizmów Uwierzytelnienia są definiowane przez Administratora.
- 6.13.1.17 Urządzenia sieciowe są skonfigurowane w taki sposób, aby zapewnić stabilność pracy zgodnie z założonymi wymaganiami co do obciążenia Sieci Korporacyjnej. W celu zapewnienia wydajności pracy urządzeń, wymagania w kontekście Zasobów obliczeniowych projektowane są ze stosownym nadmiarem w stosunku do planowanego zużycia Zasobów.
- 6.13.1.18 Okresowo Administrator sieci sporządza kopię bezpieczeństwa konfiguracji wszystkich Urządzeń sieci. Częstotliwość wykonywania kopii bezpieczeństwa nie rzadziej niż raz w miesiącu.
- 6.13.2 UDOSTĘPNIANIE SIECI INTERNET UŻYTKOWNIKOM
- 6.13.2.1 Uprawnienia Dostępu do Internetu nadawane są poprzez przypisanie Użytkowników do Profilu Internetowego. Listą Profili Internetowych zarządza Kierujący komórką DC.
- 6.13.2.2 Nadanie/odebranie/modyfikacja uprawnień do Profilu Internetowego jest wynikiem realizacji Wniosku o Dostęp zgodnie z punktem 6.4 Procedury. Wnioski do realizacji kierowane są po uzyskaniu pełnej akceptacji. W przypadku jego odrzucenia osoba składająca Wniosek jest automatycznie o tym fakcie informowana wiadomością email.
- 6.13.2.3 Zarządzanie Profilami jest realizowane na podstawie Wniosku o Profil Internetowy w SOZ z uwzględnieniem następujących zasad:
- a. operacje realizowane na podstawie Wniosku o Profil Internetowy nie skutkują bezpośrednim przydzielaniem uprawnień lecz modyfikacją Sieci Korporacyjnej w celu dostosowania jej do aktualnych potrzeb biznesowych,
 - b. każdy Profil Internetowy ma wykazanego Menadżera Dostępu,
 - c. Wnioskodawca występuje z Wnioskiem o utworzenie lub modyfikację Profilu Internetowego, gdy jest to uzasadnione obowiązkami służbowymi danej grupy Pracowników lub Kontraktor, a Profil Internetowy o wymaganym poziomie uprawnień nie istnieje,
 - d. Menadżer Dostępu występuje z Wnioskiem o usunięcie Profilu Internetowego, gdy nie jest wykorzystywany przez żadnego Pracownika lub Kontraktora,
 - e. Wniosek o utworzenie/modyfikację/usunięcie Profilu Internetowego podlega II stopniowej akceptacji,
 - na I poziomie Kierujący komórką ds. ICT w Spółce, lub osoby przez niego Upoważnionej,
 - na II poziomie Kierujący komórką DC, lub osoby przez niego Upoważnionej.
- 6.13.2.4 Czas na akceptację na każdym z poziomów wynosi 5 dni roboczych. W przypadku braku akceptacji w wymaganym terminie Wniosek jest automatycznie odrzucany. Wnioskodawca jest informowany o braku akceptacji.
- 6.13.3 ZARZĄDZANIE DOSTĘPEM DO KORPORACYJNEJ SIECI BEZPRZEWODOWEJ
- 6.13.3.1 Korporacyjna sieć bezprzewodowa WiFi zabezpieczona jest z wykorzystaniem mechanizmów określonych przez CUW ICT.
- 6.13.3.2 Dostęp do korporacyjnej sieci bezprzewodowej nadawany jest dla konkretnego Użytkownika lub Urządzenia.
- 6.13.3.3 Dostęp do korporacyjnej sieci bezprzewodowej nie może być wykorzystywany do innych celów niż te, które wynikają z pełnionej funkcji lub zajmowanego stanowiska.
- 6.13.3.4 Nadanie/odebranie/modyfikacja uprawnień do korporacyjnej sieci bezprzewodowej jest wynikiem realizacji Wniosku o Dostęp zgodnie z punktem 6.4 Procedury.
- 6.13.3.5 Wnioski do realizacji kierowane są po uzyskaniu pełnej akceptacji. W przypadku jego odrzucenia osoba składająca Wniosek jest automatycznie o tym fakcie informowana wiadomością email.

6.14 ZDALNY DOSTĘP DO SIECI TELEINFORMATYCZNEJ

- 6.14.1 Funkcjonalność Zdalnego Dostępu ma na celu zapewnienia bezpieczeństwa dostępu komputerów do zasobów Sieci Korporacyjnej z wykorzystaniem niezaufanych/niebezpiecznych mediów, takich jak internet, linie dzierżawione czy łącza radiowe. Funkcjonalność Zdalnego Dostępu podnosi bezpieczeństwo transmisji Danych poprzez wprowadzenie dodatkowych zabezpieczeń gwarantujących:

- 6.14.1.1 Poufność poprzez zastosowanie szyfrowania Danych,
- 6.14.1.2 Integralność poprzez uniemożliwienie modyfikacji Danych w trakcie ich transmisji,
- 6.14.1.3 Uwierzytelnienie stron,
- 6.14.1.4 niezaprzeczalność, która oznacza, że strony nie mogą zaprzeczyć, że nie wysłały danej informacji.
- 6.14.2 System Zdalnego Dostępu umożliwia uprawnionym Użytkownikom szybki, łatwy i bezpieczny Dostęp do Systemów Teleinformatycznych znajdujących się w Sieci Korporacyjnej spoza ich miejsca pracy oraz umożliwia podjęcie szybkich działań minimalizujących niewłaściwe funkcjonowanie Systemów Teleinformatycznych, z których korzysta Spółka (w tym umożliwienia firmom zewnętrznym sprawowanie zdalnej opieki serwisowej).
- 6.14.3 Dostępy VPN typu serwisowego stanowią osobną grupę Dostępów i przeznaczone są dla firm / osób, które na mocy odrębnej umowy administrują Systemami. W umowach z firmami trzecimi, zawarte muszą być porozumienia, na mocy których Dostępy VPN będą objęte procedurami zarządzania Użytkownikami.
- 6.14.4 W przypadku korzystania ze Zdalnego Dostępu cały ruch sieciowy, w szczególności do sieci internet, musi być kierowany przez zestawiony tunel VPN.
- 6.14.5 Zdalny Dostęp może być realizowany jedynie z urządzeń spełniających warunki określone w Procedurze i stanowiących własność Spółki lub takich, które posiadają zabezpieczenia pod względem aktualizacji poprawek bezpieczeństwa dla Systemu operacyjnego oraz ochrony antywirusowej.
- 6.14.6 Stacje robocze używane do zdalnego łączenia się z Siecią Korporacyjną muszą być na bieżąco aktualizowane oraz objęte aktualną ochroną antywirusową.
- 6.14.7 Uwierzytelnienie Zdalnego Dostępu odbywa się jedną z metod:
 - 6.14.7.1 Hasła – ciągu znaków, który służy do Uwierzytelniania w Sieci Korporacyjnej GK PGE,
 - 6.14.7.2 Certyfikatu cyfrowego – Dane podpisane cyfrowo przez tzw. „zaufaną trzecią stronę” zawierające m.in. informacje o Kluczu publicznym właściciela Certyfikatu, nazwę organizacji, inną, dopuszczoną przez Kierownika Komórki organizacyjnej w PGE Systemy odpowiedzialnego za obszar bezpieczeństwa w CUW ICT.
- 6.14.8 Profile VPN definiują mechanizmy Dostępu do wskazanych Systemów Teleinformatycznych. Dla ułatwienia zarządzania Profile VPN łączone są w Grupy Profili VPN o podobnych wymaganiach w stosunku do konfiguracji ruchu sieciowego.
- 6.14.9 Grupy Profili VPN są definiowane indywidualnie dla każdej z Jednostek organizacyjnych lub dla Spółki (jeśli nie ma potrzeby większej granulacji).
- 6.14.10 CUW ICT prowadzi ewidencję Dostępów do Sieci Korporacyjnej z wykorzystaniem VPN. Ewidencja w szczególności zawiera listę Dostępów nadanych i odebranych oraz listę Profili VPN i Grup Profili VPN.
- 6.14.11 ZARZĄDZANIE PROFILAMI VPN I GRUPAMI PROFILI VPN
 - 6.14.11.1 Zarządzanie Profilami VPN i Grupami Profili VPN jest realizowane na podstawie Wniosku o Profil VPN w SOZ.
 - 6.14.11.2 Operacje realizowane na podstawie Wniosku o Profil VPN nie skutkują bezpośrednim przydzielaniem uprawnień lecz modyfikacją środowiska VPN w celu dostosowania go do aktualnych potrzeb biznesowych.
 - 6.14.11.3 Każdy Profil VPN i Grupa Profili VPN na wykazanego Menadżera Dostępu.
 - 6.14.11.4 Wnioskodawcą może być każdy Menadżer Dostępu w zakresie Systemu za który odpowiada.
 - 6.14.11.5 Wnioskodawca występuje z Wnioskiem o utworzenie lub modyfikację Profilu VPN lub Grupy Profili VPN, gdy jest to uzasadnione obowiązkami służbowymi danej grupy Pracowników lub Kontraktorów, a Profil VPN lub Grupa Profili VPN o wymaganym poziomie uprawnień nie istnieje.
 - 6.14.11.6 Za zdefiniowanie parametrów technicznych niezbędnych do skonfigurowania Profili VPN odpowiadają Administratorzy Systemów zarządzający Systemami Teleinformatycznymi i/lub OT, do których Zdalny Dostęp ma być zapewniony.
 - 6.14.11.7 Menadżer Dostępu występuje z Wnioskiem o usunięcie Profilu VPN lub Grupy Profili VPN, gdy nie jest wykorzystywany przez żadnego Pracownika lub Kontraktora.
 - 6.14.11.8 Wniosek o Profil VPN musi zawierać następujące Dane:
 - a. Dane wnioskującego,
 - b. opis zmiany środowiska VPN:
 - **w celu utworzenia nowego Profilu VPN:** propozycję nazwy Profilu VPN, Menadżera Dostępu oraz listę Usług lub Systemów, do których niezbędne jest zapewnianie Zdalnego Dostępu na poziomie sieciowym,
 - **w celu utworzenia nowej Grupy Profili VPN:** propozycję nazwy Grupy Profili VPN, Menadżera Dostępu oraz listę Profili VPN wchodzących w skład Grupy Profili VPN,
 - **w celu modyfikacji Profilu VPN:** nazwę Profilu VPN wraz z ostateczną listą Usług lub Systemów, do których niezbędne jest zapewnianie Zdalnego Dostępu na poziomie sieciowym po zakończeniu realizacji Wniosku,

- **w celu modyfikacji Grupy Profili VPN:** nazwę Grupy Profili VPN wraz z ostateczną listą Profili VPN wchodzących w skład Grupy Profili VPN po zakończeniu realizacji Wniosku,
 - **w celu usunięcia Profilu VPN lub Grupy Profili VPN:** nazwę Profilu VPN lub Grupy Profili VPN do usunięcia,
 - **w celu zmiany Menadżera Dostępu:** Identyfikator nowego Menadżera Dostępu.
- c. uzasadnienie potrzeby.
- 6.14.11.9 Wniosek o utworzenie/modyfikację/usunięcie Profilu VPN lub Grupy Profili VPN podlega III stopniowej akceptacji:
- a. na I poziomie Przełożonego Menadżera Dostępu VPN lub osoby przez niego Upoważnionej,
 - b. na II poziomie Kierującego komórką ds. ICT w Spółce lub osoby przez niego Upoważnionej,
 - c. na III poziomie Kierujący komórką DC lub osoby przez niego Upoważnionej.
- 6.14.11.10 Wniosek o zmianę Menadżera Dostępu podlega III stopniowej akceptacji:
- a. na I poziomie Przełożonego obecnego Menadżera Dostępu,
 - b. na II poziomie Przełożonego nowego Menadżera Dostępu,
 - c. na III poziomie Kierującego komórką ds. ICT w Spółce, lub osoby przez niego Upoważnionej.
- 6.14.11.11 Wniosek do realizacji kierowany jest po uzyskaniu pełnej akceptacji. W przypadku jego odrzucenia osoba składająca Wniosek jest automatycznie o tym fakcie informowana wiadomością e-mail.
- 6.14.11.12 Czas na akceptację na każdym z poziomów wynosi 5 dni roboczych. W przypadku braku akceptacji w wymaganym terminie Wniosek jest automatycznie odrzucany. Wnioskodawca jest informowany o braku akceptacji.
- 6.14.12 NADAWANIE, MODYFIKACJA I ODBIERANIE UPRAWNIENÍ
- 6.14.12.1 Sesje nawiązywane w celu zdalnej administracji Zasobami ICT powinny wykorzystywać dedykowane środowiska o podwyższonym poziomie zabezpieczeń i wyposażone w potrzebne programy narzędziowe.
- 6.14.12.2 W przypadku konieczności nadania Zdalnego Dostępu Pracownikowi firmy zewnętrznej w celach serwisowych, Administrator Techniczny powinien dokonać:
- a. odseparowania serwera od sieci wewnętrznej w celu zatrzymania i rejestracji niepożądanego ruchu sieciowego w miarę możliwości technicznych,
 - b. blokowania możliwości uruchomienia innego oprogramowania umożliwiającego penetrację sieci wewnętrznej z serwisowanego serwera,
 - c. udzielenia zdalnego Dostępu tylko na czas przeprowadzenia prac, lub o ile tak przewiduje umowa - na czas trwania umowy.
- 6.14.12.3 Sesje serwisowe realizowane przez Osoby Trzecie powinny być prowadzone pod nadzorem Administratora Technicznego. O ile jest to możliwe, Konta wykorzystywane przez Osoby Trzecie do nawiązywania zdalnego Dostępu muszą być włączane na żądanie Administratora Technicznego w celu wykluczenia nieautoryzowanych połączeń.
- 6.14.12.4 Sesje serwisowe muszą być nagrywane w celu gromadzenia materiału o czynnościach wykonywanych w trakcie sesji. Administrator Techniczny Systemu Teleinformatycznego jest odpowiedzialny za zapewnienie bezpieczeństwa Dostępu serwisowego dla Systemu, którym administruje, w tym za podłączenie Systemu do Mechanizmów monitorujących bezpieczeństwo i nagrywania sesji.
- 6.14.12.5 Zarejestrowane sesje są przechowywane co najmniej 6 miesięcy.

6.15 WYMAGANIA BEZPIECZEŃSTWA DLA SYSTEMÓW TELEINFORMATYCZNYCH

6.15.1 ZASADY OGÓLNE

- 6.15.1.1 Zaleca się, o ile to możliwe, oddzielenie środowiska eksploatacyjnego od środowiska testowego i rozwojowego, a implementację prac testowych lub rozwojowych w pierwszej kolejności wykonywać we właściwym środowisku, za co odpowiedzialny jest Administrator Techniczny.
- 6.15.1.2 W środowisku rozwojowym należy stosować te same Zasady Dostępu jak w środowisku eksploatacyjnym, za co odpowiedzialny jest Administrator Techniczny.
- 6.15.1.3 W celu zapewnienia jednolitego i spójnego poziomu bezpieczeństwa wszystkie Zasoby ICT muszą spełniać wymagania bezpieczeństwa dla Systemów Teleinformatycznych opisane w Procedurze. W szczególności dotyczy to Systemów produkcyjnych, archiwalnych, testowych i developerskich. W sytuacji w której System nie jest w stanie spełnić wymagań należy zastosować alternatywne zabezpieczenia na innej warstwie bezpieczeństwa aby utrzymać oczekiwany poziom bezpieczeństwa.
- 6.15.1.4 Wymagania bezpieczeństwa należy definiować na możliwie najwcześniejszym etapie projektowania Systemu. W szczególności należy zapewnić:
- a. mechanizmy umożliwiające aktualizację oprogramowania, w szczególności związanych z bezpieczeństwem,

- b. mechanizmy Kontroli i rejestracji zmian konfiguracji oraz aktualizacji oprogramowania,
 - c. mechanizmy realizujące wymagania RODO, w tym obsługujące prawa jednostki,
 - d. mechanizmy zapewniające kontrolę i walidację wprowadzanych danych,
 - e. mechanizmy Uwierzytelniania Użytkowników oraz innych Systemów,
 - f. Integralność i Poufność informacji o Kontach, w szczególności o Hasłach oraz innych danych w oparciu o które następuje Uwierzytelnienie,
 - g. interfejs zarządzania uprawnieniami na potrzeby integracji z Systemem IAM, przeznaczonym do zarządzania tożsamością i uprawnieniami,
 - h. możliwość podłączenia do Systemu SIEM,
 - i. dedykowany dla Systemu ICT wydzielony segment sieci fizycznej lub logicznej.
- 6.15.1.5 Szczegółowe i aktualne wymagania dla Systemów ICT utrzymywane są przez CUW ICT.
- 6.15.2 SYNCHRONIZACJA CZASU
- 6.15.2.1 Wymaga się, aby w Sieci Korporacyjnej Dostępny był centralny serwer czasu, za administrację którego odpowiada CUW ICT.
- 6.15.2.2 Administratorzy Techniczni są zobowiązani do zapewnienia synchronizacji z centralnym serwerem czasu rzeczywistego wszystkich urządzeń aktywnych sieci, serwerów, stacji roboczych oraz innych Systemów wymagających synchronizacji czasu.
- 6.15.2.3 Jeżeli nie jest możliwa automatyczna synchronizacja zegarów w danych Zasobach ICT, Administrator Techniczny zobowiązany jest nie rzadziej niż raz w miesiącu dokonać porównania czasu w Systemie z wzorcem czasu i wnieść ewentualną korektę, mając na uwadze zachowanie wymaganych środków ostrożności w celu uniknięcia nieprawidłowego działania danego Systemu.
- 6.15.3 AKTUALIZACJA SYSTEMÓW
- 6.15.3.1 Aktualizacja Systemu obejmuje aktualizację Systemu operacyjnego oraz aktualizację aplikacji i ma na celu eliminowanie Podatności lub wadliwego działania Systemów Teleinformatycznych.
- 6.15.3.2 Aktualizacja odbywa się:
- a. automatycznie na bieżąco,
 - b. w przypadku braku możliwości automatycznej aktualizacji Systemy aktualizowane są ręcznie pakietami sprawdzonych poprawek,
 - c. specjalistyczne Systemy aktualizowane są zgodnie z zaleceniami Dostawcy Systemu Teleinformatycznego.
- 6.15.3.3 Za przeprowadzanie aktualizacji oraz jej udokumentowanie odpowiedzialni są Administratorzy Techniczni przypisani do danych Systemów.
- 6.15.3.4 Za umożliwienie przeprowadzenia aktualizacji Systemu od strony prawnej, w tym wykupienie koniecznych licencji i umów serwisowych odpowiedzialny jest Właściciel Zasobu ICT.
- 6.15.3.5 Administratorzy Techniczni zobowiązani są do weryfikowania stabilności wprowadzanych aktualizacji. W przypadku uzasadnionych wątpliwości, co do poprawności aktualizacji Administrator może podjąć decyzję o rezygnacji lub przywróceniu do wersji poprzedniej, odnotowując ten fakt w Dzienniku Systemu Teleinformatycznego z odpowiednim uzasadnieniem.
- 6.15.4 KOPIE ZAPASOWE
- 6.15.4.1 Zaleca się, aby kopie zapasowe były zaszyfrowane.
- 6.15.4.2 Dostęp do kopii zapasowych musi być nadzorowany i rozliczany.
- 6.15.4.3 Dla Zasobu ICT przetwarzających Dane, Administrator Techniczny jest zobowiązany do opracowania i stosowania planu wykonywania kopii zapasowych, który powinien zostać utrwalony w formie pisemnej i przechowywany wraz z dokumentacją Zasobu ICT w sposób uniemożliwiający Dostęp osób nieupoważnionych.
- 6.15.4.4 Kopie zapasowe przechowywane na Nośnikach powinny być przechowywane w innych miejscach niż Systemy Teleinformatyczne, dla które Dane są zabezpieczane w ramach kopii zapasowych. Zaleca się wykonywanie kopii zapasowych na dwóch różnych Nośnikach, przechowywanych w dwóch różnych lokalizacjach. Dla Zasobów ICT sklasyfikowanych jako krytyczne w ramach zawartych Umów SLA, kopie bezpieczeństwa muszą być przechowywane w dwóch różnych lokalizacjach. Miejsca przechowywania kopii wyznacza Administrator Techniczny. Dopuszcza się możliwość przechowywania dodatkowych kopii zapasowych w obszarze przetwarzania danych (np. serwerowniach), gdy konieczność ich utworzenia i przechowywania wynika z zastosowanych narzędzi i metod archiwizacji, pod warunkiem zastosowania zabezpieczeń technicznych, uniemożliwiających Dostęp do danych osobom nieupoważnionym.
- 6.15.4.5 Podczas transportu i przechowywania Nośniki zawierające kopie zapasowe należy chronić przed nieuprawnionym Dostępem, nadużyciem oraz utratą Integralności zgodnie z regulacjami punktu 6.10.4 Procedury.

- 6.15.4.6 Jeżeli Nośniki kopii zapasowych są uszkodzone lub nie można ich ponownie wykorzystać, muszą być niezwłocznie zniszczone przez Administratora Technicznego w sposób uniemożliwiający odtworzenie zapisanych na nich danych, przy zachowaniu trybu komisyjnego, protokolarnego zgodnie z zapisami punktu 6.10.5 Procedury.
- 6.15.4.7 Administrator Techniczny odpowiedzialny za wykonanie kopii zapasowej Zasobu ICT zobowiązany jest do prowadzenia dokumentacji z wykonywanych kopii. W przypadku, gdy kopie zapasowe wykonywane są automatycznie, za wystarczające można uznać logi Systemu wykonywania kopii zapasowych. Dokumentacja musi zawierać, co najmniej:
- a. datę i godzinę rozpoczęcia wykonywania kopii zapasowej,
 - b. datę i godzinę zakończenia wykonywania kopii zapasowej,
 - c. oznaczenie typu kopii będącej odnośnikiem do procedury wykonywania kopii zapasowych (np. kopia pełna, przyrostowa, trzecia w cyklu),
 - d. informację o błędach powstałych w trakcie tworzenia kopii bezpieczeństwa.
- 6.15.4.8 W celu oceny stanu technicznego Nośniki kopii zapasowych należy testować zgodnie z rekomendacjami producentów i dostawców.
- 6.15.4.9 Dla zarchiwizowanych kopii zapasowych, właściwy Administrator Techniczny zobowiązany jest do zabezpieczenia urządzeń / narzędzi, które umożliwią ich późniejsze odtworzenie.
- 6.15.4.10 Administrator Techniczny Systemu ma obowiązek weryfikacji poprawności wykonania kopii. Częstotliwość przeprowadzania weryfikacji oraz zakres przywracanych danych należy określić w planie wykonywania kopii zapasowych. Jeżeli System nie ma takiej możliwości, weryfikacja może polegać na sprawdzeniu prawidłowości logów w aplikacji wykonującej kopie.
- 6.15.4.11 Kopie zapasową krytycznego Zasobu ICT należy testować nie rzadziej niż raz na rok. Testowanie kopii może polegać, o ile istnieje taka techniczna możliwość, na całkowitym odtworzeniu jej w środowisku testowo-rozwojowym i sprawdzeniu działania odtworzonego Zasobu ICT. Z powyższych czynności należy sporządzić raport, który należy umieścić w dokumentacji Zasobu ICT.
- 6.15.4.12 Administrator Techniczny Systemu ma obowiązek przygotowania planu odzyskiwania Systemu z wykonanych kopii zapasowych.
- 6.15.5 PLANY CIĄGŁOŚCI DZIAŁANIA PROCEDURY ODTWORZENIOWE
- 6.15.5.1 Administrator Techniczny ma obowiązek utworzenia i utrzymywania procedur odtworzeniowych dla Zasobów ICT którymi administruje w zakresie uzgodnionym z Właścicielem Zasobu ICT. Procedura odtworzeniowa opisuje sposób postępowania i działania poszczególnych komponentów w przypadku ewentualnej awarii, w tym instrukcje awaryjne zmierzające do odtworzenia infrastruktury Teleinformatycznej.
- 6.15.5.2 W sytuacji, gdy zdarzenie uniemożliwi Dostęp do Zasobów ICT na okres dłuższy niż dopuszczalny czas przerwy w działaniu, uruchamiana jest procedura odtworzeniowa obowiązująca dla danego Zasobu ICT (dotyczy Zasobów ICT, dla których uzgodniono z Właścicielem Zasobu ICT konieczność posiadania takich procedur). Wówczas Użytkownicy zobowiązani są podjąć działania przypisane im w procedurze odtworzeniowej.
- 6.15.5.3 Procedury odtworzeniowe należy poddawać okresowym testom i przeglądom mającym potwierdzić ich aktualność i skuteczność.
- 6.15.5.4 Dokumentacja z przeprowadzonych testów powinna być załączona do dokumentacji Systemu ICT.
- 6.15.6 ZARZĄDZANIE OKRESEM PRZECHEWYWANIA (RETENCJI) DANYCH
- 6.15.6.1 CUW ICT wraz ze Spółkami określi dla każdego Systemu Teleinformatycznego zasady i okresy usuwania danych osobowych wynikające z przepisów prawa lub celów Administratora gwarantujące usunięcie danych gdy:
- a. minął okres ich przydatności,
 - b. cel biznesowy nie wymaga już przetwarzania takich danych.
- 6.15.6.2 W odniesieniu do Danych Osobowych przetwarzanych w Systemie przez CUW ICT oraz Spółki:
- a. Dane Osobowe są przechowywane przez okres nie dłuższy, niż jest to niezbędne do celów, w których te Dane Osobowe są przetwarzane,
 - b. Dane Osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne umożliwiające obsługę Wniosków dotyczących realizacji praw osób, których Dane Osobowe dotyczą.
- 6.15.6.3 CUW ICT oraz Spółki współpracują pod kątem monitorowania i aktualizowania okresów przechowywania Danych Osobowych, w szczególności w oparciu o zobowiązania wynikające z zawartych umów powierzenia przetwarzania Danych Osobowych oraz w przypadkach, w których usunięcie Danych Osobowych przez którąś ze stron może generować ryzyka.

- 6.15.6.4 Systemy Teleinformatyczne musi posiadać mechanizmy pozwalające na usunięcie wskazanych Danych bez wpływu na funkcjonowanie i bezpieczeństwo Systemu. W sytuacjach, w których usunięcie danych jest niemożliwe dopuszcza się Anonimizację lub Pseudonimizację danych. Fakt wykonania operacji na Danych musi być odnotowany w Dzienniku Systemu Teleinformatycznego.
- 6.15.7 ZARZĄDZANIE ZMIANĄ I KONFIGURACJĄ
- 6.15.7.1 Administrator Techniczny ma obowiązek monitorować, regulować i przewidywać przyszłą pojemność Zasobu ICT w celu zapewnienia właściwej wydajności.
- 6.15.7.2 W Przypadku konieczności rozbudowy Systemu Administrator Techniczny z odpowiednim wyprzedzeniem zgłasza taką potrzebę do Właściciela Zasobu. Właściciel Zasobu zobowiązany jest zabezpieczyć odpowiednie środki finansowe, zgłaszając je w planie finansowym Spółki.
- 6.15.7.3 Dla utrzymania krytycznego Zasobu ICT w odpowiedniej sprawności, Właściciel Zasobu ICT zapewnia na potrzeby Administratora Technicznego niezbędną ilość podstawowych części zapasowych, redundancję urządzeń lub wspiera się umową serwisową o odpowiednim poziomie SLA.
- 6.15.7.4 Każdorazowo przed wykonaniem istotnej zmiany Zasobu ICT należy przeprowadzić analizę wpływu zmiany na Zasób ICT i powiązane z nim Systemy Teleinformatyczne, za co odpowiedzialny jest Administrator Techniczny. Za istotną zmianę uważa się aktualizację oprogramowania, bazy danych, Systemu operacyjnego, istotną zmianę konfiguracji, itd. Wyniki analizy należy dołączyć do dokumentacji Zasobu ICT.
- 6.15.7.5 Przed wprowadzeniem zmiany mogącej mieć wpływ na stabilność w Zasobach ICT, należy wykonać kopię bezpieczeństwa. W szczególności należy zapisać lub zarchiwizować konfigurację pierwotną (wszelkie ustawienia sprzętu, w tym ustawienia BIOS, połączenia, konfigurację urządzeń, konfigurację Systemu operacyjnego, kodu źródłowego, ustawień aplikacji, itd.) oraz wykonać kopię bazy danych i Systemu operacyjnego wraz z oznaczeniem wersji (o ile to możliwe), za co odpowiedzialny jest Administrator Techniczny.
- 6.15.7.6 Wykonanie istotnej zmiany mogącej mieć wpływ na stabilność Zasobu ICT zatwierdza Właściciel Zasobu ICT po przedstawieniu rekomendacji Administratora Technicznego Systemu.
- 6.15.7.7 W przypadku powierzenia dokonania zmiany (w tym prac rozwojowych) podmiotowi zewnętrznemu, Właściciel Zasobu ICT we współpracy z Administratorem Technicznym zobowiązany jest do nadzorowania tych prac.
- 6.15.7.8 W przypadku konieczności integracji ze sobą różnych Systemów Teleinformatycznych należy bezwzględnie zadbać o wprowadzenie mechanizmu kontroli przesyłanych pomiędzy tymi Systemami Danych. Sposób kontroli może się różnić w zależności od konkretnych Systemów, Baz Danych, itp. Odpowiedzialność za wprowadzenie właściwych mechanizmów kontroli spoczywa na właściwych Administratorach Technicznych.
- 6.15.8 ZABEZPIECZENIA KRYPTOGRAFICZNE
- 6.15.8.1 W przypadku Systemów ICT Poufność oraz Integralność informacji zapewnia się poprzez wdrożenie rozwiązań kryptograficznych. Uwzględniając dostępne możliwości techniczne wymagane jest stosowanie zabezpieczeń kryptograficznych do ochrony:
- a. Nośników w Komputerach Biurowych, Serwerach i pozostałych Zasobach ICT,
 - b. Nośników przenośnych (pendrive),
 - c. zdalnych połączeń do Zasobu ICT,
 - d. połączeń bezprzewodowych WiFi,
 - e. komunikacji (np. poprzez stosowanie protokołów: Kerberos, SSH – secure shell, SSL – Secure Socket Layer),
 - f. szyfrowania plików zawierających Dane przeznaczone do wąskiego grona osób (np. z wykorzystaniem standardowych funkcjonalności pakietów biurowych),
 - g. Systemów obsługujących bankowość elektroniczną.
- 6.15.8.2 Administrator Techniczny odpowiedzialny jest za właściwe stosowanie ochrony kryptograficznej w powierzonych Zasobach ICT w tym opracowanie zasad dotyczących korzystania, ochrony i okresów ważności kluczy kryptograficznych i wdrożenie tych zasad na wszystkich etapach cyklu życia kluczy.
- 6.15.8.3 Certyfikaty wydawane przez Urzędy certyfikacji GK PGE mają zastosowanie do następujących celów:
- a. podpisywania dokumentów i wiadomości pocztowych Subskrybentów bez użycia karty inteligentnej,
 - b. podpisywania dokumentów i wiadomości pocztowych Subskrybentów z użyciem karty inteligentnej,
 - c. szyfrowania wiadomości poczty elektronicznej,
 - d. szyfrowania dysków i plików na stacjach roboczych,
 - e. logowania do domeny z użyciem karty inteligentnej,
 - f. Uwierzytelniania do Wi-Fi oraz VPN,
 - g. Uwierzytelniania Serwerów i Urządzeń infrastruktury,
 - h. Uwierzytelniania Użytkowników wykorzystujących urządzenia mobilne zarządzane przez System MDM.
- 6.15.8.4 Repozytorium zawierające Certyfikaty i dokumenty formalne Urzędów Certyfikacji GK PGE posiada:

- a. adres główny Repozytorium Urzędów certyfikacji GK PGE: <http://pki.gkpge.pl/pki>,
 - b. Certyfikat Urzędu GK PGE ROOT CA jest publikowany w lokalizacji AIA: <http://pki.gkpge.pl/pki/gkpgerca.crt>,
 - c. Certyfikat Urzędu GK PGE Enterprise CA jest publikowany w lokalizacji AIA: <http://pki.gkpge.pl/pki/gkpgeeca.crt>,
 - d. Certyfikat Urzędu GK PGE Infrastructure CA jest publikowany w lokalizacji AIA: <http://pki.gkpge.pl/pki/gkpgeica.crt>,
 - e. nowe Certyfikaty są publikowane w tej samej lokalizacji pod tą samą nazwą. Archiwalne Certyfikaty z nazwami rozszerzonymi o kolejny numer pozostaną w aktualnej lokalizacji,
 - f. lista Certyfikatów odwołanych przez Urząd GK PGE Root CA: <http://pki.gkpge.pl/pki/gkpgerca.crl>,
 - g. lista Certyfikatów odwołanych przez Urząd GK PGE Enterprise CA: <http://pki.gkpge.pl/pki/gkpgeeca.crl>,
 - h. lista Certyfikatów odwołanych przez Urząd GK PGE Infrastructure CA: <http://pki.gkpge.pl/pki/gkpgeica.crl>,
 - i. dokumenty dotyczące Systemu dostępne są pod adresem: <http://pki.gkpge.pl/pki/cps.htm>.
- 6.15.8.5 Urząd Certyfikacji GK PGE publikuje Certyfikaty Subskrybentów w repozytorium Active Directory i w globalnej książce adresowej Certyfikaty przeznaczone do szyfrowania.
- 6.15.8.6 Subskrybent może stosować Certyfikat wyłącznie do celów określonych we właściwościach Certyfikatu jako przeznaczenie Certyfikatu. W przypadku użycia przez Subskrybenta Certyfikatu niezgodnie z przeznaczeniem strona weryfikująca może stwierdzić błąd operacji wykonanej tym Certyfikatem.
- 6.15.8.7 Ważność Certyfikatów wygaśnie automatycznie po osiągnięciu daty końca okresu ważności i po tym terminie Certyfikaty zostaną zarchiwizowane.
- 6.15.8.8 Odnowienie Certyfikatu polega na wydaniu przez Urząd Certyfikacji GK PGE nowego Certyfikatu, z tą samą nazwą Subskrybenta, w celu zastąpienia użytkowanego Certyfikatu, którego okres ważności zbliża się do końca. Odnowienie musi być dokonane przed upływem terminu ważności zastępowanego Certyfikatu.
- 6.15.8.9 Urzędy Certyfikacji GK PGE mają możliwość unieważnienia lub zawieszenia Certyfikatu. Zawieszenie Certyfikatu jest tymczasowe i może zostać uchylone, natomiast unieważnienie Certyfikatu jest ostateczne i nieodwracalne.
- 6.15.8.10 Certyfikat Subskrybenta może zostać unieważniony w przypadkach:
- a. utraty kontroli nad Kluczem prywatnym powiązany z danym Certyfikatem (np. zagubienie, kradzież, itp.),
 - b. ujawnienia Klucza prywatnego,
 - c. konieczności wymiany Certyfikatu (np. w przypadku zmiany danych w nim zawartych),
 - d. zakończenia działalności Urzędu Certyfikacji GK PGE, który wydał Certyfikat (w takim przypadku zostaną unieważnione wszystkie Certyfikaty wydane przez ten Urząd a także Certyfikat samego Urzędu) przed upływem deklarowanego terminu zakończenia działalności,
 - e. kompromitacji Klucza prywatnego Urzędu Certyfikacji GK PGE lub nadrzędnego Urzędu GK PGE Root CA,
 - f. kompromitacji algorytmu kryptograficznego (lub parametrów z nim związanych) stosowanych przez dany Certyfikat,
 - g. zamknięcia Konta Subskrybenta w domenie GK PGE zgodnie z zasadami nadawania i odbierania uprawnień do zasobów korporacyjnych IT,
 - h. w szczególnym przypadku Certyfikat może być unieważniony przez Administratora PKI po wystąpieniu awarii Systemu i odtworzeniu Systemu z kopii bezpieczeństwa.
- 6.15.8.11 Certyfikat Subskrybenta może zostać zawieszony w przypadkach:
- a. podejrzenia utraty kontroli nad Kluczem prywatnym,
 - b. podejrzenia ujawnienia Klucza prywatnego,
 - c. zablokowania Konta Subskrybenta w domenie GK PGE zgodnie z zasadami nadawania i odbierania uprawnień do zasobów korporacyjnych IT.
- 6.15.9 DOKUMENTACJA ZASOBÓW ICT
- 6.15.9.1 Administrator Techniczny kompletuje oraz prowadzi dokumentację dla przypisanego mu Zasobu ICT. Dokumentacja Zasobu ICT zawiera:
- a. nazwę i opis Zasobu,
 - b. informacje o przetwarzanych danych w zakresie: kategorii osób, rodzaju danych, zakresie danych, okresie retencji danych ,
 - c. dokumentację techniczną pokazującą architekturę rozwiązania,
 - d. dokumentację bezpieczeństwa opisującą mechanizmy zapewnienia bezpieczeństwa i monitorowania Systemu, logowania zdarzeń, plan awaryjny, procedura odtworzeniowa (o ile ustalono taki wymóg), itp.,
 - e. dokumentację utrzymaniową opisującą prawidłową eksploatację Systemu, np. plan wykonywania kopii zapasowych,
 - f. dokumenty potwierdzające legalność oprogramowania (Nośniki instalacyjne, opakowania, itp.),

- g. opis konfiguracji Zasobu ICT oraz wszelkich istotnych zdarzeń związanych z Zasobem ICT, tj. zmiany dotyczące Zasobu, takie jak: wymiana procesorów, podwyższenie wersji oprogramowania, instalacja nowych funkcjonalności, przeglądy, naprawy, itp.,
 - h. dodatkową dokumentację wynikającą ze specyfikacji Zasobu ICT.
- 6.15.9.2 Informacje zawarte w dokumentacji Zasobu ICT należy chronić przed manipulacją i nieautoryzowanym Dostępem. Każda zapisana informacja oznaczona jest datą i godziną wpisu, a także autoryzacją wprowadzającego daną informację (czytelny podpis ręczny, podpis elektroniczny, lub w przypadku jego braku – informacja, kto dokonał wpisu). Dokumentację Zasobu ICT można prowadzić w formie elektronicznej lub papierowej.
- 6.15.10 ZASADY MONITOROWANIA DOSTAWCÓW
- 6.15.10.1 Właściciel Zasobu ICT zapewnia w umowach z dostawcami produktów i usług zapisy dotyczące gwarancji wymagań bezpieczeństwa informacji i ochrony danych osobowych w kontekście ryzyk związanych z dostarczaniem przez nich z usługami i dostawami.
- 6.15.10.2 Administrator Techniczny zobowiązany jest dokonywać okresowych przeglądów usług świadczonych przez dostawców w tym:
- a. skuteczności działań deklarowanych przez dostawców,
 - b. zgodności działań dostawców z wymaganiami stawianymi w umowach serwisowych oraz umowach powierzenia przetwarzania Danych Osobowych,
 - c. wpływu działań dostawców na bezpieczeństwo Zasobów ICT.
- 6.15.10.3 Przeglądy należy przeprowadzać zgodnie z zakresem i terminami zawartymi w instrukcjach eksploatacyjnych urządzeń/oprogramowania lub umowach serwisowych, chyba, że przepisy innych regulacji Spółki stanowią inaczej.
- 6.15.10.4 Jeżeli dla potrzeb przeglądów, napraw itp. niezbędne jest nadanie jakichkolwiek praw Dostępu dla Osób Trzecich, należy po wykonaniu określonych czynności Konto zablokować. Fakt utworzenia i zablokowania Konta należy każdorazowo wpisać w dokumentację Zasobu ICT, wraz z informacją, dla kogo i do jakich celów było utworzone.
- 6.15.11 BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE
- 6.15.11.1 Dostęp fizyczny do Zasobów ICT jest ograniczony do najwęższego możliwego grona osób. Osoby te sprawują nadzór nad pracami wykonywanymi przez dostawców. Zabronione jest wykonywanie prac przez dostawców bez nadzoru.
- 6.15.11.2 Dostęp do pomieszczeń, w których znajdują się Zasoby ICT, podlega kontroli. Kontrola Dostępu obejmuje pomieszczenia techniczne, pomieszczenia przylegające, strefę dostaw i załadunku, wszelkie wejścia do chronionych stref oraz urządzeń zapewniających bezpieczeństwo fizyczne i środowiskowe Zasobów ICT. Szczególnemu nadzorowi i ochronie podlegają Serwerownie oraz węzły Sieci Korporacyjnej warstwy rdzenia i dystrybucji.
- 6.15.11.3 Polityka Dostępu fizycznego do Zasobów ICT musi gwarantować bezpieczeństwo Zasobów ICT na ustalonym poziomie, Rozliczalność dostępu fizycznych oraz możliwość skutecznego prowadzenia działań naprawczych Zasobów ICT i urządzeń je wspierających w sytuacjach awaryjnych. Podmiotem odpowiedzialnym za kontrolę oraz politykę Dostępów fizycznych do Zasobów ICT jest podmiot sprawujący nadzór nad pomieszczeniami.
- 6.15.11.4 W szczególności prowadzona jest ewidencja osób wchodzących każdorazowo do pomieszczeń w postaci dziennika Dostępów fizycznych. Podmiotem odpowiedzialnym za prowadzenie dziennika jest podmiot sprawujący nadzór nad pomieszczeniem, w którym znajdują się Urządzenia. Dziennik zawiera w szczególności datę Dostępu fizycznego do pomieszczenia, w którym znajduje się Urządzenie, jak również imię i nazwisko osoby uzyskującej Dostęp.
- 6.15.11.5 W przypadku, gdy pomieszczenie znajduje się na parterze i posiada okno, należy je zabezpieczyć, np.: poprzez folię antywłamaniową, zamontowanie krat, itp. Dostępowe węzły sieci komputerowej znajdujące się w miejscach ogólnodostępnych (np. korytarze budynków) muszą być chronione w zamykanych na klucz szafach krosowniczych.
- 6.15.11.6 Zasoby ICT należy umieścić i chronić w taki sposób, aby zredukować ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych oraz okazać do nieuprawnionego Dostępu.

6.16 MONITOROWANIE BEZPIECZEŃSTWA

6.16.1 MONITOROWANIE ZDARZEŃ

- 6.16.1.1 Zasoby ICT muszą być skonfigurowane w taki sposób, aby zbierać logi i zapewnić Rozliczalność wszystkich operacji administracyjnych wykonywanych na danym urządzeniu zdarzeń (dzienniki logów systemowych, tj. błędów, nieudanych prób Uwierzytelnienia oraz uzyskania dostępu, informacji o możliwej awarii

- itp.). Środki służące rejestrowaniu zdarzeń oraz informacje w dziennikach zdarzeń należy chronić przed manipulacją i nieuprawnionym dostępem.
- 6.16.1.2 Konfiguracja każdego Zasobu ICT musi zapewniać zbieranie logów zdarzeń. Poziom szczegółowości logowania zdarzeń powinien być spójny dla wszystkich Zasobu ICT i adekwatny do sposobu wykorzystywania i możliwości technologicznych. Urządzenia powinny mieć uruchomioną funkcję przesyłania logów zdarzeń (np. za pomocą protokołu Syslog). Administrator ma obowiązek niezwłocznie udostępnić logi operacji administracyjnych na żądanie DC.
- 6.16.1.3 W celu usprawnienia monitorowania zdarzeń dla poszczególnych grup urządzeń ustanawiany jest centralny serwer magazynowania logów zdarzeń, zwany dalej Centralnym Serwerem Logów oraz serwery analizujące zgromadzone informacje. Zaleca się, aby przesyłanie logów z Zasobów ICT do Centralnego Serwera Logów odbywało się w sposób gwarantujący pewność dostarczenia, integralność i niezaprzeczalność informacji.
- 6.16.1.4 Dzienniki logów systemowych muszą być objęte procesem tworzenia kopii zapasowych. Kopia logów systemowych tworzona jest zgodnie z planem tworzenia kopii zapasowych dla danego Zasobu ICT.
- 6.16.1.5 Administrator Techniczny okresowo dokonuje analizy logów systemowych, zgodnie z częstotliwością minimalną jeden raz w tygodniu dla krytycznego Zasobu ICT, oraz dwa razy w miesiącu dla pozostałych Zasobów ICT.
- 6.16.2 MONITOROWANIE PODATNOŚCI
- 6.16.2.1 Wszystkie Systemy ICT są na bieżąco monitorowane pod kontem ewentualnych Podatności w obszarze bezpieczeństwa Teleinformatycznego przez odpowiednio CUW ICT lub właściciela Systemu. Jeżeli monitorowanie jest niemożliwe, Spółka doloży należytej staranności w zapewnieniu bezpieczeństwa Teleinformatycznego Systemu ICT.
- 6.16.2.2 Zalecane jest podłączenie Systemów ICT do automatycznego Systemu wykrywania Podatności stosowanego w GK PGE. Administrator Techniczny zobowiązany jest za zgłoszenie Systemu do podłączenia, współpracę z DC w ramach realizowanych prac i utrzymanie mechanizmu monitorowania Podatności Systemu, za który odpowiada.
- 6.16.2.3 Administrator Techniczny zobowiązany jest do monitorowania Podatności administrowanego Zasobu ICT poprzez śledzenie publikowanych przez dostawców informacji o znanych Podatnościach, publikowanych aktualizacjach oraz wprowadzania niezbędnych zmian do Systemu w celu utrzymania uzgodnionego poziomu bezpieczeństwa.
- 6.16.2.4 Wszystkie zidentyfikowane Podatności w Systemach ICT są na bieżąco usuwane przez Administratora Technicznego Systemu.
- 6.16.3 OCHRONA PRZED ATAKAMI I KODEM ZŁOŚLIWYM
- 6.16.3.1 Komputery oraz serwery w Sieci Korporacyjnej muszą być objęte ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego i antyspamowego oraz zapory sieciowej, których konfiguracji Użytkownikowi nie wolno zmieniać bez zgody Administratora Technicznego.
- 6.16.3.2 Każdy komputer z Systemem operacyjnym Windows, musi mieć uruchomioną zaporę sieciową.
- 6.16.3.3 Za instalację i właściwe skonfigurowanie oprogramowania antywirusowego i antyspamowego oraz zapory sieciowej na stacjach roboczych, serwerach i komputerach przenośnych, odpowiada właściwy Administrator Techniczny.
- 6.16.3.4 Za aktualizację baz wirusów odpowiada właściwy Administrator Techniczny. Aktualizacja powinna odbywać się automatycznie, przynajmniej raz dziennie, w przypadku ręcznej aktualizacji za jej częstotliwość odpowiada właściwy Administrator Techniczny.
- 6.16.3.5 W szczególnych przypadkach, gdy stacje robocze oraz serwery nie są objęte ochroną w czasie rzeczywistym (np. urządzenia pracujące w wydzielonej podsieci, zakłócenie działania użytkowanego oprogramowania przez Systemy ochrony), Administrator Techniczny, zgodnie z ustalonym harmonogramem dokonuje rutynowej kontroli pod kątem obecności złośliwego oprogramowania, przy czym kontrola może być realizowana w sposób:
- automatyczny, zgodnie z harmonogramem zdefiniowanym w scentralizowanym Systemie antywirusowym,
 - ręczny na żądanie (minimum raz w tygodniu).
- 6.16.3.6 Po każdej naprawie i konserwacji urządzenia, a przed ponownym podłączeniem do Sieci Korporacyjnej, Administrator Techniczny zobowiązany jest do sprawdzenia zawartości stałych Nośników komputerowych za pomocą aktualnego oprogramowania antywirusowego.
- 6.16.3.7 Przed rozpoczęciem pracy z Nośnikami wymiennymi używanymi poza Spółką, należy dokonać sprawdzenia za pomocą aktualnego oprogramowania antywirusowego.
- 6.16.3.8 Monitorowaniu mechanizmami wykrywającymi podlegają wszystkie elementy Sieci Korporacyjnej:
- złośliwe oprogramowanie na Zasobach ICT,
 - podejrzany ruch sieciowy wewnątrz Sieci Korporacyjnej oraz wychodzący i przychodzący z Internetu,
 - podejrzane wiadomości poczty elektronicznej,

- d. anomalie w pracy Sieci Korporacyjnej i Zasobów ICT,
 - e. nieuprawniony Dostęp do Danych,
 - f. wyciek danych,
 - g. niewłaściwe zachowania Użytkowników, w tym próby ataków oraz obchodzenia zabezpieczeń.
- 6.16.3.9 Wszelkie niezgodności mogące wskazywać na wystąpienie Incydentu Cyberbezpieczeństwa są obsługiwane zgodnie z procedurą *PROG 00116 Zarządzanie Incydentami Cyberbezpieczeństwa w GK PGE SA*.

6.17 LEGALNOŚĆ OPROGRAMOWANIA

- 6.17.1 Użytkownik jest zobowiązany do stosowania się do wszelkich zaleceń przekazywanych przez CUW ICT związanych z użytkowanym przez niego oprogramowaniem.
- 6.17.2 Zarządzanie licencjami realizowane jest zgodnie z procedurą *PROG 00099 - Zarządzanie licencjami oprogramowania w GK PGE*.
- 6.17.3 Użytkownicy mają prawo do eksploataowania programów dopuszczonych do stosowania w GK PGE wskazanych na Liście Oprogramowania utrzymywanej przez CUW ICT.
- 6.17.4 W celu uzyskania zgody na eksploataowanie programu, którego nie ma na Liście Oprogramowania, należy złożyć do CUW ICT Wniosek o legalizację oprogramowania.
- 6.17.5 Zabronione jest przekazywanie przez Użytkownika innym osobom numerów seryjnych, kodów aktywacyjnych, kluczy zabezpieczających i innych kodów mogących posłużyć do nieuprawnionego zainstalowania bądź uruchomienia programu na innym komputerze.
- 6.17.6 Okresowo, nie rzadziej niż raz w roku, Komputery Biurowe, urządzenia komputerowe oraz serwery są sprawdzane przez Administratora Technicznego, w szczególności pod kątem obecności zabronionego oprogramowania. Zabronione oprogramowanie jest niezwłocznie usuwane przez odpowiedniego Administratora Technicznego.
- 6.17.7 Administrator Techniczny ma prawo prowadzenia przeglądów dysków lokalnych Użytkowników pod kątem zgodności przechowywanych danych z przepisami prawa oraz regulacjami GK PGE. W przypadku stwierdzenia niezgodności, Administrator Techniczny podejmuje działania zmierzające do usunięcia nieprawidłowości oraz w razie potrzeby zgłasza wystąpienie Incydentu Cyberbezpieczeństwa zgodnie z *PROG 00116 Procedura Ogólna Zarządzania Incydentami Cyberbezpieczeństwa w GK PGE S.A.*
- 6.17.8 Przed zbyciem lub przekazaniem sprzętu do ponownego użycia CUW ICT sprawdza wszystkie jego składniki zawierające Nośniki Informacji dla zapewnienia, że wszystkie wrażliwe Dane i licencjonowane programy zostały usunięte lub bezpiecznie nadpisane.

6.18 SZKOLENIA I PODNOSZENIE ŚWIADOMOŚCI BEZPIECZEŃSTWA

- 6.18.1 CUW ICT przygotowuje materiały podnoszące świadomość Bezpieczeństwa Informacji i udostępnia Użytkownikom Sieci Korporacyjnej:
- a. na platformie IPK,
 - b. na witrynach SD,
 - c. na platformie elearningowej.
- 6.18.2 Za szkolenia Użytkowników odpowiada Kierujący komórką ds. ICT w Spółce.
- 6.18.3 CUW ICT na Wniosek Spółki może przygotować i przeprowadzić dedykowane szkolenia Użytkowników w uzgodnionej formie.

6.19 POSTANOWIENIA KOŃCOWE

- 6.19.1 Procedura podlega okresowym przeglądom i aktualizacji w celu dostosowania jej zapisów do zmieniających się zagrożeń Cyberbezpieczeństwa i przepisów prawa. Za przeprowadzenie przeglądu Procedury odpowiedzialny jest Kierujący komórką właściwą ds. strategii ICT.
- 6.19.2 W zakresie nieobjętym niniejszą Procedurą lub innymi regulacjami zawartymi w aktach normatywnych Spółki, należy postępować zgodnie z interesem Spółki, kierując się wiedzą oraz najlepszymi praktykami z dochowaniem należytej staranności we wszystkich podejmowanych działaniach.
- 6.19.3 Wszelkie odstępstwa od niniejszej Procedury muszą być zaakceptowane przez Kierującego komórką właściwą ds. strategii ICT w PGE S.A. lub członka Zarządu ds. Finansowych w PGE S.A.
- 6.19.4 Odstępstwa od Procedury muszą być udokumentowane przez cały okres jej obowiązywania.
- 6.19.5 Dokumentacja odstępstw jest przechowywana w komórce właściwej ds. strategii ICT w PGE S.A. Dokumentacja odstępstw musi zawierać co najmniej datę wydania odstępstwa, zakres odstępstwa, termin obowiązywania odstępstwa.
- 6.19.6 Załącznik 1 do Procedury zawiera listę mierników zabezpieczeń, które weryfikują poziom realizacji Procedury przez CUW ICT i nie dotyczy pozostałych Spółek.

- 6.19.7 Przeglądu mierników o których mowa w pkt 6.19.6, co najmniej raz w roku dokonuje Kierujący komórką właściwą ds. strategii ICT w PGE S.A. przy współpracy z DC. Uprawnienia w Systemach Teleinformatycznych i obowiązki przestrzegania postanowień regulacji wewnętrznych przez Kontraktora są adekwatne z uprawnieniami i obowiązkami Pracownika.
- 6.19.8 Wszystkie zmiany w załącznikach, niezbędne dla prawidłowej realizacji Procedury (poza zmianami dotyczącymi dołączania nowych i usuwania istniejących załączników lub powodującymi zmianę przebiegu procesu), wymagają akceptacji jej właściciela i nie powodują konieczności zmiany Procedury.
- 6.19.9 Z dniem wejścia w życie niniejszej Procedury, traci moc obowiązująca *PROG 00039/A Procedura Ogólna Bezpieczeństwa Teleinformatycznego*.
- 6.19.10 Procedura wchodzi w życie po upływie 14 dni od dnia jej publikacji w Banku DSZ.