

# PROCEDURA OGÓLNA KORZYSTANIA Z ZASOBÓW TELEINFORMATYCZNYCH (ICT) W GK PGE

PROG 00103/C

Sygn.: PGE/CENT/DSIT/3.8.7

Data zatwierdzenia: 2022/06/20  
Obowiązuje od: 2022/06/30

## I CEL I ZAKRES

- 1.1 Celem Procedury jest określenie zasad prawidłowej eksploatacji Zasobów ICT w Spółkach GK PGE oraz minimalizacja ryzyka ich awarii.
- 1.2 Procedura stanowi zbiór zasad opisujących bezpieczny sposób korzystania z Systemów Teleinformatycznych, w szczególności są to zasady i procedury niezbędne do zapewnienia właściwej ochrony Przetwarzanych Informacji w Systemach Teleinformatycznych wykorzystywanych w PGE S.A.
- 1.3 Procedura obejmuje swoim zakresem:
  - a. obowiązki Użytkowników Zasobów ICT, Przełożonych i Opiekunów Osób Trzecich,
  - b. wnioskowanie o dostęp do Zasobów ICT,
  - c. zasady użytkowania Zasobów ICT, w tym Komputerów Biurowych, Urządzeń Mobilnych oraz Nośników informacji,
  - d. zabezpieczenia danych przetwarzanych na Nośnikach, w tym Nośnikach Komputerów Biurowych i Urządzeń Mobilnych,
  - e. zasady związane z przydziałem, wymianą i likwidacją Zasobów ICT,
  - f. zasady korzystania ze służbowej poczty elektronicznej.
- 1.4 Procedura nie obejmuje:
  - a. obowiązków Właścicieli Zasobów ICT,
  - b. obowiązków Administratorów Technicznych,
  - c. zasad użytkowania Zasobów OT.

## II ODPOWIEDZIALNOŚĆ

- 2.1 Za stosowanie wymagań niniejszej Procedury odpowiedzialni są wszyscy Użytkownicy Zasobów ICT GK PGE.
- 2.2 Za aktualizację niniejszej Procedury odpowiedzialny jest CIO.
- 2.3 Wszelkie odstępstwa od niniejszej Procedury wymagają akceptacji CIO.
- 2.4 Za stosowanie wymagań niniejszej Procedury odpowiedzialne są Spółki.
- 2.4.1 Do Spółek z Grupy PGE, Procedura ma bezpośrednie zastosowanie.
- 2.4.2 Do Spółek innych niż Spółki z Grupy PGE, stosowanie postanowień Procedury odbywa się odpowiednio, za pomocą rozwiązań stosownych do danego przypadku za pośrednictwem:
  - a. Spółek z Grupy PGE – dla spółek zależnych od Spółek z Grupy PGE, lub
  - b. Komórki organizacyjnej, która ma w swoich podstawowych zadaniach zarządzanie korporacyjne w Grupie Kapitałowej PGE – dla pozostałych Spółek.
- 2.5 Spółki umożliwiające Osobom Trzecim korzystanie z Zasobów Teleinformatycznych zobowiązane są do zabezpieczenia interesów Spółki w umowach z Kontrahentami regulujących pracę lub świadczenie usług przez Osoby Trzecie, w szczególności do zabezpieczenia przestrzegania przez Osoby Trzecie niniejszej Procedury i zapewnienia możliwości egzekwowania od Kontrahentów lub Osób Trzecich:
  - a. odpowiedzialności majątkowej za powierzone Zasoby Teleinformatyczne,
  - b. zobowiązania Osób Trzecich do zapewnienia Poufności, Integralności i Dostępności informacji, pozyskiwanych z wykorzystaniem udostępnionych Zasobów Teleinformatycznych.
- 2.6 Spółki zobowiązane są do zabezpieczenia w umowach zawieranych z Członkami Organów Spółki, Kontraktorami i osobami zatrudnionymi na innej podstawie niż art. 22 Kodeksu Pracy (umowach o pracę, kontraktach menadżerskich, itp.), interesów Spółki, w szczególności w zakresie stosowania i egzekwowania niniejszej Procedury.

## III DOKUMENTY POWIĄZANE

- 3.1 REGL 00000 Kodeks Grupy PGE
- 3.2 REGL 00001 Regulamin Organizacyjny PGE Polska Grupa Energetyczna S.A.
- 3.3 REGL 00082 Polityka Organizacji Teleinformatyki w Grupie Kapitałowej PGE
- 3.4 PROG 00035 Procedura Ogólna – Wytyczne w zakresie ochrony danych osobowych w GK PGE

- 3.5 *PROG 00037 Procedura Ogólna – Wytyczne w zakresie Klasyfikacji i ochrony informacji w Grupie Kapitałowej PGE*
- 3.6 *PROG 00039 Procedura Ogólna Bezpieczeństwa Teleinformatycznego*
- 3.7 *PROG 00116 Procedura Ogólna Zarządzania Incydentami Cyberbezpieczeństwa*
- 3.8 *Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy*
- 3.9 *Ustawa z dnia 5 lipca 2018 r. o zmianie ustawy o zwalczaniu nieuczciwej konkurencji*
- 3.10 *Ustawa z dnia 5 lipca 2018 o Krajowym Systemie Cyberbezpieczeństwa (UKSC)*
- 3.11 *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)*

#### IV ZAŁĄCZNIKI

- 4.1 [Załącznik 1](#) Oświadczenie o zapoznaniu się z Procedurą
- 4.2 [Załącznik 2](#) Protokół przekazania
- 4.3 [Załącznik 3](#) Protokół zwrotu
- 4.4 [Załącznik 4](#) Zasady bezpiecznej pracy w Sieci korporacyjnej

#### V SKRÓTY I DEFINICJE

PGE, PGE S.A.:

Grupa Kapitałowa PGE (GK lub GK PGE); Grupa PGE / Grupa; Jednostka organizacyjna; Komórka organizacyjna / komórka; Pracodawca; Pracownik; Proces biznesowy / Proces; Przełożony; Przetwarzanie informacji; Sieć korporacyjna; Spółka GK PGE, Spółka, Spółki; Tajemnica Spółki

##### Skróty użyte na potrzeby niniejszego dokumentu:

<b>CERT</b>	- (ang. Computer Emergency Response Team) Zespół reagowania na incydenty cyberbezpieczeństwa
<b>DLP</b>	- (ang. Data Loss Prevention) – ochrona danych w postaci elektronicznej przed kradzieżą lub przypadkowymi wyciekami
<b>ICT</b>	- (ang. Information and Communication Technologies) teleinformatyka
<b>OT</b>	- (ang. Operational Technology) Systemy sterowania przemysłowego
<b>PDA</b>	- (ang. Personal Digital Assistant) mały przenosny, programowalny komputer osobisty
<b>PGE, PGE S.A.</b>	- PGE Polska Grupa Energetyczna S.A.
<b>PKI</b>	- (ang. Public Key Infrastructure) Infrastruktura klucza publicznego
<b>RODO</b>	- Rozporządzenie Parlamentu Europejskiego o którym mowa w pkt. 3.11
<b>SLA</b>	- (ang. Service Level Agreement) umowa o gwarantowanym poziomie świadczenia usług

##### Definicje pojęć użyte na potrzeby niniejszego dokumentu:

- 5.1 **Administrator Lokalny** – wbudowane Konto do administrowania Komputerem Biurowym. Użytkownik, któremu zostaną nadane uprawnienia Administratora Lokalnego na Komputerze Biurowym ma prawo do zarządzania lokalnymi uprawnieniami i instalacjami na tym Komputerze Biurowym. Uprawnienia Administratora Lokalnego nadawane są do konkretnego Komputera Biurowego. Nadanie tych uprawnień wymaga każdorazowo odrębnego odstępowstwa wydawanego przez CIO.
- 5.2 **Administrator Techniczny / Administrator** – Pracownik, Kontraktor z 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 odstępowstwa od Procedury – Administratorem może zostać Pracownik GK PGE niebędący Pracownikiem lub Kontraktorem z CUW ICT pod warunkiem realizowania przez niego wszystkich zadań wynikających z *PROG 00039 Procedura Ogólna Bezpieczeństwa Teleinformatycznego* a przypisanych do roli Administratora.
- 5.3 **Autentyczność** – właściwość potwierdzająca, że podmiot jest tym za kogo się podaje.
- 5.4 **Bezpieczeństwo Informacji** – zapewnienie Poufności, Integralności i Dostępności informacji dla przetwarzanych informacji, czyli zabezpieczanie jej przed nieautoryzowanym dostępem, zmianą, utratą, uszkodzeniem, zniszczeniem lub zatajeniem.
- 5.5 **Centrala** – Spółka (jeżeli nie posiada ona oddziałów) lub komórka organizacyjna Spółki realizująca zadania operacyjne w miejscu siedziby Spółki (jeżeli Spółka posiada oddziały).

- 5.6 **Centrum Usług Wspólnych ICT (CUW ICT)** – podmiot, którego celem jest świadczenie Usług ICT na rzecz pozostałych Spółek GK PGE.
- 5.7 **Chief Information Officer (CIO)** – rola pełniona przez Kierującego komórką właściwą ds. strategii ICT GK PGE. Odpowiada za operacyjne zarządzanie Funkcją ICT w GK PGE.
- 5.8 **Cyberbezpieczeństwo** – odporność systemów informacyjnych na działania naruszające Poufność, Integralność, Dostępność i Autentyczność przetwarzanych Danych lub związanych z nimi usług oferowanych przez te systemy.
- 5.9 **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 wraz z informacjami konfiguracyjnymi Zasobów ICT.
- 5.10 **Dane Osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, w szczególności na podstawie informacji takich jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji lub czynników określających fizyczną, fizjologiczną, ekonomiczną, kulturową i społeczną tożsamość osoby fizycznej.
- 5.11 **Dostępność** – właściwość bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu.
- 5.12 **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 i realizację wszystkich usług teleinformatycznych w Grupie Kapitałowej PGE.
- 5.13 **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.
- 5.14 **Grupa PGE / Grupa** – PGE oraz Spółki objęte zakresem zastosowania Kodeksu Grupy PGE na podstawie Art. 7 Kodeksu Grupy PGE.
- 5.15 **Hasło** – ciąg znaków, który służy do Uwierzytelniania w Systemie Teleinformatycznym.
- 5.16 **ICT** – (ang. Information and Communication Technologies) teleinformatyka.
- 5.17 **Identyfikator w Systemie Teleinformatycznym / Identyfikator** – unikalny ciąg znaków jednoznacznie identyfikujący w Systemie Teleinformatycznym Użytkownika lub inny System Teleinformatyczny.
- 5.18 **Informacje** – aktywa informacyjne, które podobnie jak inne ważne aktywa biznesowe, są niezbędne dla organizacji biznesu i w konsekwencji, wymagają odpowiedniej ochrony. Informacje mogą być przechowywane w wielu formach, włączając w to: postać cyfrową (np. pliki danych przechowywane na nośnikach elektronicznych lub optycznych), postać materialną (np. na papierze), jak również niematerialną Informację w postaci wiedzy posiadanej przez osoby. Informacje mogą być przesyłane za pomocą różnych środków, w tym: komunikacji za pośrednictwem kuriera, komunikacji elektronicznej, czy werbalnej. Niezależnie od tego jaką formę posiadają Informacje lub jaki jest środek ich przesyłania, zawsze wymagają właściwej ochrony.
- 5.19 **Infrastruktura klucza publicznego (PKI)** – zbiór osób, polityk, procedur i systemów komputerowych niezbędnych do świadczenia usług uwierzytelniania, szyfrowania, Integralności i niezaprzeczalności za pośrednictwem kryptografii klucza publicznego i prywatnego i certyfikatów elektronicznych.
- 5.20 **Incydent Cyberbezpieczeństwa** – zdarzenie, które ma lub może mieć niekorzystny wpływ na Cyberbezpieczeństwo.
- 5.21 **Integralność** – właściwość polegająca na zapewnieniu dokładności i kompletności informacji.
- 5.22 **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.
- 5.23 **Kierujący Komórką** – osoba kierująca Komórką organizacyjną (dyrektor lub zastępca dyrektora).
- 5.24 **Komputer Biurowy** – komputer stacjonarny, komputer przenośny (laptop) umożliwiający przetwarzanie Danych, wraz z przynależnymi akcesoriami.
- 5.25 **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.
- 5.26 **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.
- 5.27 **Kontrahent** – podmiot, z którym Spółka zawarła umowę, na podstawie której lub w związku z którą określone Osoby Trzecie świadczą dla Spółki pracę / usługi.
- 5.28 **Kontraktor** – Osoba, niebędącą Osobą Trzecią, realizująca zadania na rzecz Spółki na innej podstawie niż umowa o pracę.

- 5.29 **Lista dystrybucyjna / lista kontaktów** – lista adresów (kontaktów) poczty elektronicznej służąca do przesyłania wiadomości mailowych na adresy, które znajdują się na tej liście. Rozróżnia się następujące Listy dystrybucyjne:
- a. **Liniowa lista dystrybucyjna** – Lista dystrybucyjna tworzona domyślnie przez Administratora Technicznego na serwerze Exchange dla każdej Spółki, dla której PGE Systemy S.A. świadczy usługę udostępnienia konta pocztowego. Właścicielem Liniowych list dystrybucyjnych Spółki jest osoba pełniąca rolę/stanowisko Kierującego Komórką organizacyjną właściwą ds. komunikacji wewnętrznej w Spółce lub osoba przez nią wskazana. Liniowe listy dystrybucyjne tworzone są automatycznie i nie mogą być ręcznie modyfikowane (dodawanie/usuwanie kontaktów),
  - b. **Globalna lista dystrybucyjna** – Lista dystrybucyjna tworzona przez Administratora Technicznego na serwerze Exchange; Globalna lista dystrybucyjna tworzona jest w przypadku, gdy jest przeznaczona do cyklicznego przesyłania informacji do predefiniowanej grupy osób lub gdy zawiera więcej niż 200 adresów,
  - c. **Lokalna lista dystrybucyjna** – Lista dystrybucyjna tworzona samodzielnie przez Użytkownika w aplikacji MS Outlook z przeznaczeniem przesyłania wiadomości do określonej grupy odbiorców; liczba adresów Lokalnej listy dystrybucyjnej nie może przekroczyć 200 adresatów.
- 5.30 **Menadżer Danych / Menadżer Dostępu** – rola sprawująca nadzór nad Danymi w Systemie Teleinformatycznym oraz Dostępem do Danych będących własnością Spółki.
- 5.31 **Menadżer Konta** – osoba merytoryczna odpowiadająca za wszystkie Konta Użytkownika i wskazana w atrybutach Konta dostępu podstawowego. 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 Organów Spółki w GK PGE,
  - d. Osoby Trzeciej – Opiekun Osoby Trzeciej,
  - e. Konta Dodatkowego Użytkownika – odpowiednio Użytkownik jeśli jest Pracownikiem, w pozostałych przypadkach Menadżer Konta Podstawowego,
  - f. Konta Technicznego – upoważniony Pracownik Spółki.
- 5.32 **Nośnik informacji / Nośnik** – wszelkiego rodzaju nośniki informacji, używane w procesie przetwarzania informacji, w szczególności dyski twarde, płyty CD/DVD/BR, taśmy DLT/DDS, pamięci przenośne, dyski magneto-optyczne.
- 5.33 **Opiekun Osoby Trzeciej** – Kierownik Komórki organizacyjnej, w ramach której Osoba Trzecia realizuje swoje zadania lub wyznaczony przez niego Pracownik.
- 5.34 **Organy Spółki / Członkowie Organów Spółki** – Organy Spółki w rozumieniu Regulaminu Organizacyjnego Spółki / osoby pełniące funkcje członków w Organach Spółki.
- 5.35 **Osoba Trzecia** – osoba udostępniona przez dostawcę, dla której Dostępy nadawane są każdorazowo na wniosek Opiekuna Osoby Trzeciej.
- 5.36 **PGE-CERT** – Komórka organizacyjna w strukturach GK PGE, świadcząca usługi monitorowania Cyberbezpieczeństwa i obsługi Incydentów Cyberbezpieczeństwa.
- 5.37 **Poufność** – właściwość, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.
- 5.38 **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.
- 5.39 **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.
- 5.40 **Procedura** – PROG 00103/C Procedura Ogólna Korzystania z Zasobów Teleinformatycznych (ICT) w GK PGE, niniejszy dokument.
- 5.41 **Proces biznesowy / Proces** – logicznie uporządkowany łańcuch działań wzajemnie powiązanych lub wzajemnie oddziałujących. Proces realizuje cel biznesowy organizacji.
- 5.42 **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 zatrudnionych w wyznaczonym obszarze struktury organizacyjnej Spółki.
- 5.43 **Przetwarzanie Informacji** – jakiegokolwiek operacje wykonywane na informacji, w szczególności takie jak ich zbieranie, utrwalanie, przechowywanie, opracowywanie, modyfikowanie, udostępnianie, przesyłanie i usuwanie.

- 5.44 **Rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
- 5.45 **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.
- 5.46 **Service Desk (SD)** – zespół osób w ramach CUW ICT przyjmujący i realizujący obsługę zgłoszeń z zakresu wszelkich zdarzeń związanych z informatyką lub telekomunikacją.
- 5.47 **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.
- 5.48 **Spółka GK PGE, Spółka, Spółki** – podmiot / podmioty prawa handlowego wchodzące w skład Grupy Kapitałowej PGE.
- 5.49 **System Obsługi Zgłoszeń (SOZ)** – System służący m.in. do wsparcia Procesów zarządzania Usługami ICT, obsługi zgłoszeń i wniosków dostępny pod adresem sd.gkpge.pl.
- 5.50 **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.
- 5.51 **Systemy ICT** – Systemy realizujące Funkcje ICT nie będące Systemami OT, utrzymywane i rozwijane przez CUW ICT, wspierające realizację celów biznesowych określanych przez Spółki.
- 5.52 **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.
- 5.53 **Tajemnica Spółki** – oznacza tajemnicę przedsiębiorstwa zgodnie z art. 11 ust 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, przez co rozumie się informacje techniczne, technologiczne, organizacyjne Spółki lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności.
- 5.54 **Teleinformatyka (ICT)** – dziedzina łącząca informatykę, telekomunikację oraz narzędzia i inne technologie związane z Przetwarzaniem Informacji. Nie obejmuje rozwiązań związanych z teleinformatyką przemysłową i automatyką.
- 5.55 **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.
- 5.56 **Usługa ICT / Usługa** – usługa świadczona z wykorzystaniem technologii teleinformatycznych, ludzi i Procesów. Usługa ICT zorientowana jest na Spółkę i bezpośrednio wspiera realizowane przez nią 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.
- 5.57 **Uwierzytelnienie** – sprawdzenie i potwierdzenie zadeklarowanej tożsamości.
- 5.58 **Użytkownik** – osoba uprawniona do korzystania z Systemu Teleinformatycznego. Użytkownikami mogą być Członkowie Organów Spółki, Pracownicy, Kontraktorzy oraz Osoby Trzecie.
- 5.59 **Właściciel Listy dystrybucyjnej** – osoba upoważniona do zarządzania Listą dystrybucyjną.
- 5.60 **Właściciel Zasobu ICT** – funkcja przypisana do osoby merytorycznie odpowiedzialnej za rozwój Zasobu ICT w Spółce.
- 5.61 **Zasoby Teleinformatyczne, Zasoby ICT** – 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.
- 5.62 **Zasoby OT** – Systemy OT wraz ze sprzętem komputerowym oraz elementami infrastruktury sieci OT a także narzędzia i inne technologie związane ze zbieraniem, przetwarzaniem, przesyłaniem, przechowywaniem, zabezpieczaniem i prezentowaniem informacji dla procesów technologicznych i przemysłowych.



- 5.63 **Zdalny Dostęp (VPN)** – (ang. Virtual Private Network), wirtualna sieć prywatna, tunel między dwoma punktami sieci (np. laptopem, a siecią wewnętrzną Banku), 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 OBOWIĄZKI UŻYTKOWNIKÓW KORZYSTAJĄCYCH Z ZASOBÓW ICT

- 6.1.1 Użytkownicy Zasobów ICT są zobowiązani do stosowania zasad i standardów określonych w Procedurze oraz w dokumentach z nią powiązanych, wskazanych w pkt III.
- 6.1.2 Pracodawca prowadzi szkolenia wstępne w zakresie postanowień Procedury. Po przeprowadzeniu szkolenia Użytkownik potwierdza zapoznanie się z treścią Procedury, składając oświadczenie za pomocą udostępnionego narzędzia informatycznego lub w sposób przyjęty u Pracodawcy. Wzór oświadczenia stanowi [Załącznik 1](#) do Procedury. Oświadczenie składane drogą elektroniczną dostępne jest pod adresem (<https://itsm.gkpge.pl/sso/ess.do>).
- 6.1.3 Pozostali Pracownicy zobowiązani są do zapoznania się z treścią Procedury w nieprzekraczalnym terminie jednego miesiąca od daty wejścia w życie Procedury oraz potwierdzenia faktu zapoznania godnie z zasadami określonymi w pkt. 6.1.2.
- 6.1.4 Oświadczenia w formie pisemnej przechowywane są zgodnie z regulacjami stosowanymi w Spółce. Złożenie oświadczenia potwierdzone jest wysłaniem informacji na Service Desk.
- 6.1.5 Zasoby ICT mogą być wykorzystywane przez Użytkowników wyłącznie w celach, dla których zostały im udostępnione i w zakresie przydzielonych uprawnień oraz zgodnie z interesem GK PGE, obowiązującymi przepisami prawa i regulacjami GK PGE.
- 6.1.6 W ramach realizacji obowiązków służbowych można używać wyłącznie Komputerów Biurowych, Urządzeń Mobilnych, oprogramowania oraz Nośników stanowiących własność Spółki lub takich, dla których Spółka ma prawo używania.
- 6.1.7 Możliwe jest podłączanie urządzeń niebędących własnością Spółki (np. komputera gościa) do urządzeń wyświetlających obraz, będących w zasobach ICT (np. do projektora), w miejscach do tego przewidzianych (np. sale konferencyjne). W każdym innym przypadku należy zgłosić potrzebę do Service Desk.
- 6.1.8 Użytkownik zobowiązany jest:
- chronić Zasoby ICT przed dostępem osób nieuprawnionych, kradzieżą oraz zniszczeniem; należy korzystać w tym celu z narzędzi i zabezpieczeń dostarczanych przez CUW ICT,
  - stosować się do polityk/ regulaminów/ procedur/ instrukcji dotyczących danego Zasobu ICT,
  - w razie powzięcia informacji o podejrzeniu ujawnienia Hasła natychmiast je zmienić – jeżeli nie jest to możliwe, bezzwłocznie powiadomić o tym fakcie Service Desk zgłaszając Incydent Cyberbezpieczeństwa zgodnie z postanowieniami *PROG 00116 Procedura Ogólna Zarządzania Incydentami Cyberbezpieczeństwa*,
  - w przypadku zagubienia lub kradzieży Zasobu ICT, będącego w dyspozycji Użytkownika, bezzwłocznie powiadomić Service Desk, Przełożonego oraz zgłosić Incydent Cyberbezpieczeństwa zgodnie z postanowieniami *PROG 00116 Procedura Ogólna Zarządzania Incydentami Cyberbezpieczeństwa*,
  - używać oprogramowania zgodnie z prawami licencji dotyczącymi danego oprogramowania.
- 6.1.9 Użytkownikowi zabrania się:
- przetwarzania plików, Danych, Danych Osobowych i wszelkich innych informacji w postaci cyfrowej nie związanych z wykonywaniem obowiązków służbowych na służbowych Komputerach Biurowych, Urządzeniach Mobilnych oraz służbowych Nośnikach,
  - wykorzystywania sprzętu prywatnego do realizacji zadań służbowych,
  - wykorzystywania Zasobów ICT w celach niezwiązanych z wykonywanymi obowiązkami służbowymi lub na zasadach niezgodnych z aktualnymi przepisami prawa, w szczególności zabrania się rozpowszechniania materiałów godzących w dobre imię Grupy Kapitałowej PGE lub naruszających dobra stron trzecich (w tym prawa autorskie, zasady poufności, tajemnicy zawodowej, Tajemnicy Spółki i przepisy o ochronie Danych Osobowych),
  - samodzielnej instalacji oraz aktualizacji oprogramowania systemowego i aplikacji na służbowych Komputerach Biurowych a w przypadku potrzeby instalacji/ aktualizacji należy to zgłosić na Service Desk,
  - dokonywania jakichkolwiek zmian w kodzie źródłowym zainstalowanego oprogramowania za pomocą dowolnej metody, która naruszałaby warunki licencji na użytkowanie danego oprogramowania,
  - wyłączania oprogramowania zabezpieczającego (oprogramowanie antywirusowe, firewall, itp.),

- g. wyłączania mechanizmów aktualizacji na Komputerach Biurowych i Urządzeniach Mobilnych,
- h. podejmowania działań mających na celu uzyskanie nieautoryzowanego dostępu do Zasobów ICT,
- i. dokonywania zmian konfiguracji, odłączania zasilania urządzeń sieciowych, zmian w strukturze sieci,
- j. utrudniania lub uniemożliwiania innym Użytkownikom korzystania z Zasobów ICT, do których są uprawnieni,
- k. pozyskiwania informacji na temat parametrów sieci, używanych protokołów, portów, podsłuchiwanie sieci, deszyfracji ruchu sieciowego, mających na celu destabilizację pracy Zasobów ICT lub nieuprawniony dostęp do informacji,
- l. udostępniania Zasobów ICT nieuprawnionym osobom lub podmiotom,
- m. dokonywania samodzielnych napraw i przeglądów urządzeń informatycznych i telekomunikacyjnych,
- n. włączania urządzeń informatycznych i telekomunikacyjnych do gniazd zasilających innych niż dla nich dedykowane, z wyłączeniem świadczenia pracy poza siedzibą Spółek z GK PGE w tym pracy zdalnej,
- o. podejmowania prób wykorzystania Kont, które nie zostały przydzielone Użytkownikowi, a w szczególności wykonywania działań mających na celu złamanie zabezpieczeń konta np. uruchamiania aplikacji deszyfrujących (łamiących) Hasła, z wyłączeniem działań wynikających z obowiązków służbowych,
- p. udostępniania osobom postronnym informacji na temat struktury technicznej Zasobów ICT (w szczególności adresacji sieci, struktur aplikacji, baz Danych, itp.),
- q. uruchamiania aplikacji i programów oraz podłączania urządzeń, które mogą zakłócić i destabilizować pracę Zasobów ICT, bądź naruszyć bezpieczeństwo Danych w nich przetwarzanych (np. zestawianie z Komputera Biurowego połączenia z siecią Internet za pośrednictwem modemu GSM przy jednoczesnym połączeniu z Siecią korporacyjną, przy użyciu karty sieciowej przewodowej/ bezprzewodowej),
- r. uruchamiania nieautoryzowanych urządzeń sieciowych stanowiących punkty dostępowe (np. punkt dostępowy Wi-Fi / Bluetooth, przełącznik/router przewodowy) bezpośrednio do Zasobów ICT z pominięciem centralnych punktów styku z Internetem z wyłączeniem świadczenia pracy poza siedzibą Spółek z GK PGE w tym pracy zdalnej, z wyłączeniem świadczenia pracy poza siedzibą Spółek z GK PGE w tym pracy zdalnej,
- s. wykorzystywania Komputerów Biurowych oraz Urządzeń Mobilnych, jako punktów, które umożliwiają dostęp do Internetu nieupoważnionym osobom,
- t. rozpowszechniania materiałów godzących w dobre imię Grupy Kapitałowej PGE lub naruszających dobra stron trzecich,
- u. przesyłania/kopiowania danych i informacji służbowych na prywatne nośniki nie posiadające wymaganej autoryzacji,
- v. korzystania z publicznej niezabezpieczonej sieci Wi-Fi korzystając ze sprzętu służbowego,
- w. przetwarzania na urządzeniach służbowych Informacji niezwiązanych z wykonywaniem obowiązków służbowych.

6.1.10 [Załącznik 4](#) zawiera zasady dotyczące bezpiecznej pracy w Sieci korporacyjnej opracowane na podstawie dobrych praktyk i aktualnych zagrożeń Cyberbezpieczeństwa.

## 6.2 DOSTĘP DO ZASOBÓW ICT

- 6.2.1 Dostęp do zasobów ICT realizowany jest w oparciu o Konto do domeny korporacyjnej gkpge.pl, a w Systemach gdzie to nie jest możliwe w oparciu o konta lokalne w Systemie.
- 6.2.2 Dostęp do Zasobów ICT nadawany jest poprzez mechanizm Kont i uprawnień.
- 6.2.3 Wszyscy Administratorzy oraz Użytkownicy posiadają unikatowy Identyfikator oraz Hasło do Systemu w celu zapewnienia Rozliczalności.
- 6.2.4 Konto może być używane tylko i wyłącznie przez osobę, której zostało ono przyznane.
- 6.2.5 Identyfikator Użytkownika, którego uprawnienia wygasły lub zostały odebrane nie może zostać przydzielony innemu Użytkownikowi.
- 6.2.6 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).
- 6.2.7 Dla osób z którymi Spółka podjęła współpracę na podstawie terminowych umów o pracę oraz Osób Trzecich Konto zakładane jest na:
  - a. czas określony, wskazany w umowie ze Spółką nie dłuższy niż 1 rok,
  - b. okres w jakim występuje potrzeba biznesowa korzystania z Konta,w zależności od tego, który z nich jest krótszy.
- 6.2.7.1 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 rzeczona Spółka świadczy usługi.
- 6.2.7.2 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.
- 6.2.8 Menadżer Konta jest odpowiedzialny za wnioskowanie o zamknięcie Konta w sytuacji wygaśnięcia umów o współpracy pomiędzy Spółką a Użytkownikiem lub wygaśnięciu potrzeb biznesowych realizowanych z wykorzystaniem Konta Użytkownika.
- 6.2.9 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, a Hasło podawane telefonicznie.
- 6.2.10 Po zalogowaniu się przy użyciu Hasła początkowego Użytkownik ma obowiązek jego zmiany.
- 6.2.11 Użytkownik ma obowiązek chronić swoje Dane uwierzytelniające zapewniając ich Poufność. Jeśli zachodzi jakiegokolwiek podejrzenie, że Hasło zostało skompromitowane (poznane przez osobę nieuprawnioną), należy bezzwłocznie dokonać jego zmiany i zgłosić podejrzenie Incydentu Cyberbezpieczeństwa zgodnie z postanowieniami *PROG 00116 Procedura Ogólna Zarządzania Incydentami Cyberbezpieczeństwa*.
- 6.2.12 Użytkownik otrzymuje uprawnienia do Zasobu ICT, zgodnie z zakresem jego obowiązków służbowych oraz zasadą wiedzy koniecznej, oznaczającą udostępnianie minimalnych uprawnień wystarczających do skutecznej realizacji powierzonych zadań (w tym zakresu upoważnienia do przetwarzania danych osobowych).
- 6.2.13 Dostępem do Danych w Zasobach ICT zarządza Menadżer Danych.
- 6.2.14 Użytkownik może pełnić rolę Menadżera Danych, co oznacza kompetencje do nadawania i cofania uprawnień w użytkowanym systemie IT dla innych Użytkowników.
- 6.2.15 Użytkownicy zobowiązani są zgłaszać Menadżerowi Danych fakt posiadania szerszych uprawnień do Zasobu ICT, niż wynika to z zakresu zatwierdzonych uprawnień. W przypadku, gdy Użytkownik nie posiada wiedzy o tym, kto jest Menadżerem Danych dla danego Zasobu, fakt posiadania szerszych niż wymagane uprawnień zgłasza Przełożonemu.
- 6.2.16 W szczególnych przypadkach zasady dotyczące zarządzania uprawnieniami do Zasobów ICT mogą być opisane w odrębnych regulacjach Grupy Kapitałowej PGE (np. regulacji nadawania uprawnień w SAP). Dodatkowo Użytkownika obowiązują wewnętrzne regulacje Spółki w przedmiotowym zakresie.
- 6.2.17 Odpowiedzialnymi za bieżącą weryfikację i aktualizację uprawnień dostępowych są Menadżerowie Konta:
- a. dla Pracownika – bezpośredni Przełożony lub osoba przez niego upoważniona,
  - b. dla Kontraktora – wskazany Pracownik,
  - c. dla Członków Rady Nadzorczej Spółki, Członków Zarządu Spółki, Dyrektorów Oddziałów, Dyrektorów Generalnych, Dyrektorów Pionu – Kierujący komórką organizacyjną odpowiedzialną za obszar ICT lub osoba przez niego upoważniona, przy współpracy z Kierującym Komórką organizacyjną właściwą ds. obsługi organów Spółki w GK PGE,
  - d. dla Osoby Trzeciej – Opiekun Osoby Trzeciej,
- każda w swoim zakresie.
- 6.2.18 Wniosek o udzielenie / odebranie/ zmianę praw dostępu do Zasobów ICT można złożyć w SOZ dostępnym jedynie dla Użytkowników uwierzytelnionych w domenie gkpge.pl.
- 6.2.19 Użytkownik jest uprawniony do składania wniosków tylko i wyłącznie na rzecz przedstawicieli tej samej Spółki, w której zadania realizuje wnioskujący. Akceptacja wniosków odbywa się drogą elektroniczną. Realizacja wniosku następuje po uzyskaniu wszystkich wymaganych akceptacji, przy czym za nadanie/odebranie (akceptacja wniosku na I poziomie) dostępu odpowiada Menadżer Konta.
- 6.2.20 Wnioskodawca występuje z wnioskiem o modyfikację lub odebranie uprawnień dla Pracownika lub Kontraktora w następujących sytuacjach:
- a. zmiana stanowiska pracy,
  - b. zmiana obowiązków służbowych,
  - c. zakończenie stosunku pracy.
- 6.2.21 Wnioskodawca występuje z wnioskiem o modyfikację lub odebranie uprawnień dla Osoby Trzeciej po zmianie zakresu działań realizowanych przez Osobę Trzecią na rzecz Spółki w tym w sytuacji zakończenia współpracy.



- 6.2.22 Wnioskodawca występuje z wnioskiem o modyfikację lub odebranie uprawnień dla Członka Organu Spółki po zmianie zakresu działań realizowanych przez Członka Organu Spółki w tym w sytuacji zakończenia współpracy.
- 6.2.23 Użytkownik nie otrzymuje praw Administratora na użytkowanych Zasobach ICT. Prawa takie przyznawane są jedynie po uzyskaniu zgody pisemnej CIO.
- 6.2.24 Na Użytkowniku zalogowanym na Komputerze Biurowym jako Administrator automatycznie ciążyą wszystkie obowiązki wskazane w *PROG 00039 Procedura Ogólna Bezpieczeństwa Teleinformatycznego*, dotyczące administrowania Zasobami ICT.
- 6.2.25 Konto z uprawnieniami Administratora powinno być wykorzystywane wyłącznie w uzasadnionych przypadkach. Podstawowe codzienne prace należy wykonywać na Koncie Użytkownika bez praw administracyjnych.

### 6.3 UŻYTKOWANIE KOMPUTEROWYCH URZĄDZEŃ BIUROWYCH ORAZ NOŚNIKÓW INFORMACJI

- 6.3.1 Komputery Biurowe wykorzystywane w Spółce mogą być przeznaczone tylko i wyłącznie do realizacji zadań służbowych. Oznacza to zakaz użytkowania sprzętu służbowego do celów prywatnych.
- 6.3.2 Wykorzystywanie Zasobów ICT, będących własnością Spółki, w celach służbowych niezwiązanych z powierzonymi obowiązkami wymaga uzyskania zgody bezpośredniego Przełożonego i jeżeli zachodzi taka potrzeba z Menadżerem Dostępu. W Spółkach zagadnienie to powinno zostać doprecyzowane w rozwiązaniach szczegółowych.
- 6.3.3 Instalacji oraz aktualizacji oprogramowania systemowego i aplikacji dokonuje wyłącznie Administrator Techniczny.
- 6.3.4 W przypadku zakończenia pracy lub odejścia od stanowiska pracy każdorazowo należy stosować zasadę czystego biurka i ekranu.
- 6.3.5 Zasada czystego biurka polega na zabezpieczeniu wszelkich dokumentów oraz Nośników podlegających ochronie, znajdujących się na stanowisku pracy, nawet w sytuacji kiedy na krótki okres czasu tracimy nad nimi kontrolę. Niepotrzebne w danej chwili dokumenty oraz Nośniki należy zabezpieczać.
- 6.3.6 Zasada czystego ekranu odnosi się do Komputerów Biurowych, urządzeń przenośnych oraz serwerów. Polega na zastosowaniu zabezpieczenia przed nieupoważnionym użyciem urządzenia komputerowego pozostawionego bez opieki.
- 6.3.7 Udostępnienie Użytkownikowi Komputera Biurowego, Urządzenia Mobilnego, Nośnika informacji oraz innych akcesoriów komputerowych następuje wraz z podpisaniem przez niego protokołu przekazania (przykładowy protokół przedstawia [Załącznik 2](#)).
- 6.3.8 Zwrot Komputera Biurowego, Urządzenia Mobilnego, Nośnika informacji oraz innych akcesoriów komputerowych poświadczany jest protokołem zwrotu (przykładowy protokół przedstawia [Załącznik 3](#)).
- 6.3.9 Użytkownik posługujący się przenośnym Komputerem Biurowym i Urządzeniem Mobilnym ma możliwość korzystania z Sieci korporacyjnej przez dostęp bezprzewodowy.
- 6.3.10 Użytkownik posługujący się Komputerem Biurowym zobowiązany jest nie rzadziej niż raz na 30 dni podłączyć je do Sieci korporacyjnej poprzez lokalną sieć komputerową lub Zdalny Dostęp, w celu aktualizacji komponentów bezpieczeństwa. Niezastosowanie się do powyższego skutkuje wyrejestrowaniem Komputera Biurowego z domeny, co oznacza, że dla Użytkownika część usług z GK PGE będzie niedostępna. Ponowna rejestracja Komputera Biurowego dokonywana jest po jego podłączeniu do Sieci korporacyjnej i wykonaniu czynności technicznych przez Administratora.
- 6.3.11 Użytkownik ma obowiązek dbać z należytą starannością o powierzone Komputery Biurowe, Urządzenia Mobilne oraz Nośniki, a w przypadku zauważonych usterek niezwłocznie zgłaszać je do Service Desk.
- 6.3.12 Sprzętu nie należy pozostawiać bez opieki, bez zabezpieczenia przed kradzieżą lub dostępem osób niepowołanych. W przypadku komputerów przenośnych (laptopów), w celu zabezpieczenia przed kradzieżą zaleca się stosowanie linek zabezpieczających.
- 6.3.13 Użytkownik może zostać wezwany do bezzwłocznego zwrotu udostępnionego Komputera Biurowego, Urządzenia Mobilnego, Nośnika oraz innych akcesoriów komputerowych w przypadkach planowanej nieobecności trwającej dłużej niż 30 dni kalendarzowych (np. zwolnienie lekarskie, szkolenie, urlop wychowawczy itp.). Wnioskującym zwrot może być:
  - a. Przełożony,
  - b. upoważniony przedstawiciel komórki właściwej ds. ICT w Spółce/ oddziale,
  - c. Kierujący komórką właściwą ds. bezpieczeństwa w Spółce/ oddziale.
- 6.3.14 W GK PGE wprowadzono standardy Komputerów Biurowych, Urządzeń Mobilnych oraz oprogramowania instalowanego na urządzeniu komputerowym. Standardy są utrzymywane w CUW-ICT.

- 6.3.15 Witryna <https://ipk.gkpge.pl> jest obligatoryjną stroną startową w przeglądarce internetowej zainstalowanej na Komputerach Biurowych w domenie gkpge.pl.
- 6.3.16 Przydział lub wymiana Komputerów Biurowych i Urządzeń Mobilnych dla Użytkowników realizowana jest w oparciu o możliwości techniczne i osobowe CUW ICT w możliwie najkrótszym czasie.
- 6.3.17 Przydział lub wymiana Urządzeń Mobilnych, usług GSM oraz telefonii stacjonarnej określają odrębne regulacje w Spółce.
- 6.3.18 Przekazanie Komputerów Biurowych w użytkowanie następuje zgodnie z odrębną regulacją Spółki, dotyczącą kwalifikacji i gospodarowania rzeczowymi składnikami majątku.
- 6.3.19 Informację o Komputerach Biurowych i Urządzeniach Mobilnych, które Komórka organizacyjna zaprzestała użytkować (stały się zbędne), należy bez zbędnej zwłoki zgłosić do Service Desk.
- 6.3.20 Administrator Techniczny przeprowadza analizę użyteczności zgłoszonych Zasobów ICT pod kątem możliwości dalszej eksploatacji w Spółce. W zależności od analizy i zgłoszonych potrzeb przekazuje je do użytkowania innym Użytkownikom lub zgłasza informację o ich zbyciu/ likwidacji zgodnie z odrębną regulacją Spółki, dotyczącą zbycia zbędnych składników majątku.
- 6.3.21 Działania dotyczące zbycia/ likwidacji rzeczowych składników majątku oraz wartości niematerialnych są określane indywidualnie przez każdą ze Spółek, przy czym wymaga się aby Nośniki informacji przeznaczone do zniszczenia zostały zutylizowane w ciągu 12 miesięcy od momentu ich wycofania.
- 6.3.22 Nośniki przeznaczone do zniszczenia, Administrator Techniczny przekazuje za pokwitowaniem do komórki właściwej ds. bezpieczeństwa w Spółce lub w CUW ICT (o ile istnieją umowy w tym zakresie). Komórki te zapewniają komisyjne zniszczenie Nośników, z których każdorazowo sporządzany jest protokół. Do czasu zniszczenia Nośników komórka ta odpowiada za ich zabezpieczenie przed nieautoryzowanym dostępem.

## 6.4 UŻYTKOWANIE URZĄDZEŃ MOBILNYCH

- 6.4.1 Dostęp do usług z Urządzeń Mobilnych jest nadawany i odbierany na podstawie Wniosków w SOZ.
- 6.4.2 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 mobilnych Systemów operacyjnych i udostępnia te wykazy wg potrzeb Użytkownikom.
- 6.4.3 CUW ICT na stronie [sd.gkpge.pl](https://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.
- 6.4.4 Na Urządzeniach Mobilnych mogą zostać zainstalowane dodatkowe aplikacje lub uruchomione funkcjonalności, niezbędne do korzystania z tych Usług.
- 6.4.5 Użytkownik zobowiązany jest udostępnić Urządzenie Mobilne na żądanie CUW ICT.
- 6.4.6 Użytkownik nie ma prawa ingerować w System operacyjny Urządzenia Mobilnego (w szczególności obchodząc jego wbudowanych zabezpieczeń), jak również stosować innych Systemów operacyjnych, niż są zatwierdzone i dopuszczone do użytku przez Kierującego komórką odpowiedzialną za cyberbezpieczeństwo w CUW ICT.
- 6.4.7 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 (w tym m.in. poprzez ustawienie kodu PIN),
  - 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 oryginalne Urządzenia.
- 6.4.8 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 (w tym instalowania prywatnej skrzynki elektronicznej, używania aplikacji social media powiązanych z prywatnymi kontami, korzystania z aplikacji streamingowych),
  - 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 służbowych posiadających technologię typu DUAL-SIM,
- h. włączania przekierowania rozmów na numery prywatne.

## 6.5 OPROGRAMOWANIE DO ZASTOSOWAŃ BIUROWYCH

- 6.5.1 Podstawowym oprogramowaniem (pakiet standardowy) udostępnianym Użytkownikowi wraz z Komputerem Biurowym, jest:
  - a. System operacyjny – standardowo System z rodziny Microsoft Windows,
  - b. pakiet biurowy – z rodziny Microsoft Office,
  - c. aplikacja do odczytu dokumentów w formacie PDF,
  - d. program do archiwizacji i kompresji plików,
  - e. komunikator,
  - f. System antywirusowy.
- 6.5.2 Oprogramowanie dodatkowe i specjalistyczne wymagane na stanowisku pracy Użytkownika instalowane jest zgodnie ze zgłoszonymi przez Kierującego Komórką organizacyjną potrzebami zachowując wymogi licencjonowania oraz dostępu dla danego Systemu.
- 6.5.3 Instalacja oprogramowania biurowego realizowana jest jedynie przez wskazanych Administratorów, w tym Service Desk, po uprzednim uzyskaniu stosownych akceptacji osób odpowiedzialnych za weryfikację licencyjną.
- 6.5.4 Zabronione jest przekazywanie przez Użytkownika osobom nieuprawnionym numerów seryjnych, kodów aktywacyjnych, kluczy zabezpieczających i innych kodów mogących posłużyć do nieuprawnionego zainstalowania bądź uruchomienia programu na innym komputerze.
- 6.5.5 Użytkownicy mają prawo do eksploataowania wyłącznie programów dopuszczonych do stosowania w Grupie Kapitałowej PGE (w tym programów bezpłatnych). Lista oprogramowania dopuszczonego do stosowania w GK publikowana jest na stronie [sd.gkpge.pl](http://sd.gkpge.pl).
- 6.5.6 Potrzebę wykorzystywania oprogramowania niezbędnego do realizacji zadań służbowych, a nie znajdującego się na liście oprogramowania dopuszczonego do stosowania w GK należy zgłosić do Service Desk w celu przeprowadzenia przez CUW ICT jego weryfikacji pod kątem zasad licencjonowania i bezpieczeństwa. Zweryfikowane pozytywnie oprogramowanie umieszczane jest na liście oprogramowania dopuszczonego.
- 6.5.7 Użytkownik jest zobowiązany do stosowania się do wszelkich zaleceń przekazywanych przez CUW ICT związanych z użytkowaniem przez niego oprogramowaniem.
- 6.5.8 Administrator Techniczny, zgodnie ze swoim zakresem obowiązków lub na polecenie osoby odpowiedzialnej za obszar ICT w Jednostce organizacyjnej lub Kierującego Komórką organizacyjną ds. bezpieczeństwa w CUW ICT, ma prawo prowadzenia przeglądów oprogramowania zainstalowanego na Komputerach Biurowych oraz Urządzeniach Mobilnych wykorzystywanych przez Spółkę oraz przechowywanych plików, pod kątem zgodności z przepisami prawa.

## 6.6 OCHRONA DANYCH

- 6.6.1 W celu zabezpieczenia Danych przed nieautoryzowanym dostępem, utratą, kradzieżą, uszkodzeniem lub modyfikacją należy postępować zgodnie z ogólnymi zasadami dotyczącymi Bezpieczeństwa informacji, w tym zasadą czystego biurka i ekranu. Użytkownik posługujący się przenośnymi komputerami biurowymi i/ lub przenośnymi Nośnikami zobowiązany jest do ich zabezpieczenia przed kradzieżą, zniszczeniem lub dostępem osób nieuprawnionych.
- 6.6.2 Użytkownicy zarządzają Danymi na swoich Komputerach Biurowych, skrzynkach poczty elektronicznej, zasobach sieciowych, Nośnikach przenośnych i wydrukach zgodnie z nadanymi upoważnieniami do przetwarzania danych i uprawnieniami do systemów IT. O zakresie nadanych upoważnień i uprawnień decyduje Przełożony Użytkownika. Niezależnie od formy Nośnika, Użytkownik jest odpowiedzialny za bezpieczne udostępnianie lub usuwanie przechowywanych w urządzeniu Danych.
- 6.6.3 Do Komputera Biurowego i Urządzenia Mobilnego Użytkownik może podłączać tylko i wyłącznie zaufany oraz zarejestrowany zgodnie z postanowieniami *PROG 00039 Procedura Ogólna Bezpieczeństwa Teleinformatycznego*, przenośny Nośnik informacji. Każdy przenośny Nośnik informacji udostępniony Użytkownikowi przez GK PGE jest zaufany. Korzystanie z Nośnika pochodzącego z innego źródła jest możliwe po jego wcześniejszym zautoryzowaniu. Autoryzacji dokonuje CUW ICT na wniosek Użytkownika (zgłoszenie na Service Desk).

- 6.6.4 Wszystkie Nośniki, przed rozpoczęciem pracy, należy sprawdzić pod kątem ewentualnych zagrożeń za pomocą aktualnego oprogramowania antywirusowego oraz zaszyfrować. W celu wykonania zadań, o których mowa w zdaniu poprzednim, Użytkownik zobowiązany jest do osobistego zgłoszenia się do zespołu CUW ICT obsługującego lokalizację Użytkownika.
- 6.6.5 Przed przekazaniem Nośnika w tym Nośnika Komputera Biurowego lub Urządzenia mobilnego do zbycia, likwidacji lub przydziału innemu Użytkownikowi Administrator Techniczny ma obowiązek trwale usunąć informacje znajdujące się na Nośniku niezwłocznie po 2 tygodniach po przekazaniu.
- 6.6.6 Stosowanie oprogramowania szyfrującego jest obligatoryjne dla Danych przechowywanych na przenośnych Komputerach Biurowych oraz Nośnikach przenośnych w tym Urządzeniach mobilnych. W przypadku, gdy Urządzenie nie jest wykorzystywane do dostępu do Zasobów ICT stosowanie oprogramowania szyfrującego nie jest wymagane ale jest zalecane.
- 6.6.7 Użytkownicy zobowiązani są do wykorzystywania mechanizmów kryptograficznych oferowanych przez oprogramowanie dopuszczone do eksploatacji przez CUW ICT. Lista dopuszczonych mechanizmów kryptograficznych jest dostępna w CUW ICT.
- 6.6.8 Niszczenie Nośników typu płyty CD/ DVD/ BR odbywa się w przeznaczonych do tego niszczarkach, Zasady niszczenia poszczególnych typów Nośników udostępniane są przez CUW-ICT.
- 6.6.9 Informacje przetwarzane elektronicznie na Nośnikach Komputerów Biurowych, istotne z punktu widzenia realizacji poszczególnych Procesów biznesowych, informacje oraz Dane osobowe, których utrata (brak możliwości odtworzenia) może skutkować konsekwencjami prawnymi bądź finansowymi, należy zabezpieczać poprzez tworzenie ich kopii bezpieczeństwa. Klasyfikacja informacji odbywa się zgodnie z *PROG 00037 Procedura Ogólna – Wytyczne w zakresie Klasyfikacji i ochrony informacji w Grupie Kapitałowej PGE*.
- 6.6.10 Kopie należy wykonywać cyklicznie, nie rzadziej niż raz na pół roku.
- 6.6.11 Kopię bezpieczeństwa Użytkownik może wykonać samodzielnie poprzez skopiowanie Danych, np. na służbowy zasób sieciowy lub służbowy, odpowiednio zabezpieczony, zaufany przenośny Nośnik informacji. Niedopuszczalne jest tworzenie kopii bezpieczeństwa na zasobach prywatnych lub niebędących własnością Spółek GK oraz w sieci Internet.
- 6.6.12 W przypadku braku możliwości technicznych Użytkownik ma prawo złożyć do SD wnioski o wykonanie kopii bezpieczeństwa swoich Danych.
- 6.6.13 W przypadku, kiedy kopie wykonywane są przez Użytkownika, ma on obowiązek je zabezpieczyć przed dostępem osób nieuprawnionych.
- 6.6.14 Użytkownik wykonujący wydruki, które zawierają informacje podlegające ochronie jest odpowiedzialny za zachowanie szczególnej ostrożności, a zwłaszcza za zabezpieczenie ich przed dostępem przez osoby nieupoważnione, w tym: wylogowanie się z urządzenia drukującego po zakończeniu pracy oraz sprawdzeniu, czy na urządzeniu drukującym, skanującym lub kopiującym nie pozostawiono zbędnej kopii.
- 6.6.15 Wydruki przeznaczone do usunięcia, należy zniszczyć w sposób trwały, bezwzględnie uniemożliwiający w jakikolwiek sposób ich odtworzenie.
- 6.6.16 Użytkownicy obowiązani są do przestrzegania zakazu prowadzenia rozmów telefonicznych, podczas których może dochodzić do wymiany informacji podlegających ochronie, jeśli rozmowy te odbywają się w miejscach publicznych (np. pociągach, poczekalniach) oraz takich, które nie gwarantują zachowania Poufności rozmów.
- 6.6.17 Użytkownikom zabrania się zapisywania w systemach poczty głosowej informacji zaklasyfikowanych do IV Poziomu ochrony, zgodnie z *PROG 00037 Procedura Ogólna – Wytyczne w zakresie Klasyfikacji i ochrony informacji w Grupie Kapitałowej PGE*.
- 6.6.18 Odczytanie wiadomości z faksów, automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego Hasła. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.
- 6.6.19 Przekazywanie za pomocą urządzeń faksowych dokumentów zawierających informacje sklasyfikowane do IV Poziomu ochrony, zgodnie z *PROG 00037 Procedura Ogólna – Wytyczne w zakresie Klasyfikacji i ochrony informacji w Grupie Kapitałowej PGE*, jest zabronione.

## 6.7 ZGŁASZANIE ZDARZEŃ ORAZ ZAGROŻEŃ

- 6.7.1 Pracownik GK PGE, Kontraktor, Osoba Trzecia bądź Użytkownik Systemów Teleinformatycznych, należących do GK PGE, który podejrzewa zaistnienie Incydentu Cyberbezpieczeństwa, bądź jest w posiadaniu informacji o Incydencie Cyberbezpieczeństwa zobowiązany jest zgłosić zdarzenie i przekazać posiadane informacje do PGE-CERT, poprzez jeden z kanałów:
- e-mail na adres: [cert@gkpge.pl](mailto:cert@gkpge.pl),
  - zgłoszenie na Service Desk,
  - zgłoszenie telefonicznie na dedykowany numer obsługi Incydentów Cyberbezpieczeństwa PGE-CERT dostępny na stronie intranetowej <https://pgesystemy.pl/CERT-PL>.
- 6.7.2 CUW ICT udostępnia Użytkownikom informacje o problemach związanych z eksploatacją usług na stronie [sd.gkpge.pl](https://sd.gkpge.pl). W szczególnych przypadkach informacje te mogą być przekazywane za pośrednictwem poczty korporacyjnej i/ lub SMS.
- 6.7.3 W celu podniesienia poziomu bezpieczeństwa Danych i przeciwdziałania atakom cyberprzestępców wszystkie Komputery Biurowe, Urządzenia Mobilne, skrzynki poczty elektronicznej, Nośniki przenośne, witryny sieciowe i pozostałe Zasoby ICT są monitorowane automatycznymi narzędziami bezpieczeństwa. Narzędzia monitorują w szczególności:
- kondycję Komputerów Biurowych i pozostałych zasobów ICT,
  - znane podatności,
  - wystąpienia złośliwego kodu,
  - nieautoryzowany ruch sieciowy w sieci wewnętrznej i do Internetu,
  - dostęp do niebezpiecznych witryn www,
  - potencjalnie niebezpieczne zawartości dokumentów oraz poczty elektronicznej,
  - niebezpieczne załączniki poczty elektronicznej,
  - niezgodne z regulacjami wewnętrznymi GK PGE zachowania Użytkowników,
  - zarządzanie informacją z wykorzystaniem mechanizmów DLP, w szczególności przekazywaną poza organizację za pomocą poczty elektronicznej, stron internetowych oraz Nośników Informacji.
- 6.7.4 W przypadku, gdy Użytkownik korzystający z Zasobu ICT stwarza zagrożenie dla Bezpieczeństwa Informacji przetwarzanych w danym Systemie, Administrator Techniczny ma prawo, bez wcześniejszego powiadomienia, podjąć działania minimalizujące to zagrożenie np. zablokować Użytkownikowi Konta i odebrać uprawnienia oraz zdalnie wyłączyć Komputer Biurowy lub Urządzenie Mobilne. Ponowne przydzielenie uprawnień do korzystania z Zasobów ICT jest możliwe dopiero po wyjaśnieniu całego zdarzenia i może wymagać ponownego wystąpienia z wnioskiem o nadanie dostępu do Zasobów ICT.
- 6.7.5 W przypadku konieczności dodatkowej analizy zawartości Komputera Biurowego, Użytkownik jest zobowiązany udostępnić wskazane urządzenia na potrzeby CUW-ICT oraz udzielić stosownej pomocy i wyjaśnień.
- 6.7.6 PGE CERT zabezpiecza informacje służbowe jako materiał dowodowy i materiał analityczny dokumentujący Incydent Cyberbezpieczeństwa. Obsługując zdarzenie, PGE CERT bada informacje pod kątem potencjalnego wystąpienia Incydentu Cyberbezpieczeństwa. Działania PGE CERT o których mowa w zdaniu pierwszym nie naruszają prawa Użytkownika do prywatności i tajemnicy korespondencji.
- 6.7.7 PGE CERT może prowadzić kontrolę poczty elektronicznej Pracownika, Kontraktora lub Osoby trzeciej w zakresie niezbędnym do potwierdzenia właściwego wykorzystania udostępnianych narzędzi pracy.

## 6.8 ZASADY KORZYSTANIA ZE SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ

- 6.8.1 Poczta elektroniczna udostępniona przez Pracodawcę jest podstawowym i jedynym kanałem komunikacji e-mail w GK PGE służącym do realizacji zadań służbowych i komunikacji.
- 6.8.2 Użytkownicy w swojej służbowej poczcie elektronicznej mają włączony mechanizm dodawania automatycznej stopki przy wysyłaniu korespondencji na zewnątrz. Stopka zawiera klauzule informacyjne o zasadach przetwarzania Danych Osobowych oraz poufności informacji.
- 6.8.3 Użytkownik służbowej poczty elektronicznej zobowiązany jest do okresowej weryfikacji poprawności danych znajdujących się w stopce. W przypadku stwierdzenia nieprawidłowości w podpisie jest on zobowiązany do niezwłocznego zgłoszenia zmiany:
- dla Pracowników do komórki właściwej ds. zarządzania kapitałem ludzkim w Spółce,
  - dla pozostałych Użytkowników na Service Desk.
- 6.8.4 Użytkownik przesyłając informację służbową pocztą elektroniczną ponosi odpowiedzialność za prawidłowe zaadresowanie wiadomości elektronicznej i przesłanie jej do uprawnionego odbiorcy. Użytkownik



odpowiedzialny jest również za niewłaściwe zaadresowanie wiadomości wysyłanej do adresatów poprzez użycie niewłaściwego pola adresowego, co doprowadzić może do nieuprawnionego ujawnienia ich Danych osobowych oraz Informacji.

- 6.8.5 W przypadku otrzymania wiadomości, przez osobę, która nie jest uprawniona do jej otrzymania, Użytkownik:
- jest zobowiązany do kontaktu z nadawcą w celu potwierdzenia braku uprawnień do jej otrzymania,
  - fizyczne usunięcie wiadomości z poczty elektronicznej,
  - przesłanie nadawcy potwierdzenia usunięcia wiadomości.
- 6.8.6 Zabrania się przesyłania służbową pocztą elektroniczną treści niezgodnych z obowiązującymi przepisami prawa, naruszających zasady współżycia społecznego oraz naruszających prawa własności intelektualnej innych osób.
- 6.8.7 Zabrania się osobom korzystającym ze służbowej poczty elektronicznej przesyłania do Pracowników Spółki, wiadomości o treści niezwiązanej z działalnością Spółki, a w szczególności informacji o charakterze komercyjnym oraz masowego przesyłania korespondencji do Użytkowników, którzy korespondencji tej nie zamawiali. Wyjątkiem jest przesyłanie korespondencji przez Pracowników komórek właściwych ds. komunikacji w Spółkach oraz innych, którym zostało delegowane takie zadanie w ramach obowiązków służbowych.
- 6.8.8 Zabrania się ręcznego lub automatycznego przesyłania wiadomości ze służbowej poczty elektronicznej na prywatną skrzynkę Użytkownika. Wyjątek stanowi przesyłanie własnych dokumentów kadrowo-płacowych otrzymanych od Pracodawcy.
- 6.8.9 Zabrania się wykorzystywania przydzielonej Użytkownikowi służbowej poczty elektronicznej do celów prywatnych (np. wysyłanie korespondencji niezwiązanej z realizacją działań służbowych, wykorzystywania Identyfikatora Konta służbowej poczty elektronicznej (adresu email) do rejestracji i działań w internetowych Systemach Teleinformatycznych, niezwiązanych z realizacją zadań służbowych). Użytkownik naruszający zapis, świadomie narusza niniejszą Procedurę.
- 6.8.10 W przypadku przesyłania w formie elektronicznej informacji, które wymagają zachowania poufności i integralności (III i IV poziom ochrony – zgodnie z *PROG 00037 Procedura Ogólna – Wytyczne w zakresie Klasyfikacji i ochrony informacji w Grupie Kapitałowej PGE*) należy:
- 6.8.10.1 Zaszyfrować wiadomość z wykorzystaniem Infrastruktury klucza publicznego (PKI).
- 6.8.10.2 Lub zaszyfrować załącznik (np. stosując oprogramowanie do kompresji plików) i zabezpieczyć go hasłem, które należy przesłać do odbiorcy innym kanałem komunikacji (np. SMS-em).
- 6.8.11 Korespondencja Użytkownika, prowadzona z wykorzystaniem służbowej poczty elektronicznej, jest własnością Spółki. W uzasadnionych przypadkach, Przełożony lub uprawnione Komórki organizacyjne mogą wnioskować o dostęp do służbowej skrzynki poczty elektronicznej Użytkownika, na zasadach określonych w Procedurze *PROG 00039 Procedura Ogólna Bezpieczeństwa Teleinformatycznego*.
- 6.8.12 System obsługujący służbową pocztę elektroniczną podlega ochronie antywirusowej i wszystkie wiadomości są sprawdzane pod kątem obecności oprogramowania złośliwego. Wiadomości, z których nie można usunąć oprogramowania złośliwego nie będą dostarczane adresatowi.
- 6.8.13 W przypadku otrzymania podejrzanej wiadomości, Użytkownik zobowiązany jest:
- nie otwierać załączników wiadomości,
  - nie otwierać linków załączonych do wiadomości,
  - niezwłocznie przesłać zgłoszenie wraz podejrzaną wiadomością na adres [bezpieczenstwo.pgesystemy@gkpge.pl](mailto:bezpieczenstwo.pgesystemy@gkpge.pl) lub do Service Desk w celu jej weryfikacji,
  - usunąć daną wiadomość (również z folderu zawierającego wiadomości usunięte).
- 6.8.14 Użytkownik służbowej poczty elektronicznej zobowiązany jest do utrzymywania odpowiedniej ilości wolnego miejsca na skrzynce mailowej, w tym celu archiwizuje oraz usuwa zbędną korespondencję, w szczególności nie dotyczącą spraw służbowych (np.: życzeń, ogłoszeń, które straciły aktualność itd.).

## 6.9 LISTY DYSTRYBUCYJNE

- 6.9.1 Liniowe listy (grupy) dystrybucyjne:
- dla każdej Spółki domyślnie tworzone są następujące Liniowe listy dystrybucyjne:
    - nazwa wyświetlana: Zarząd [Spółka - Centrala] – lista adresów mailowych wszystkich Członków Zarządu Spółki; kryterium wyboru do listy: nazwa stanowiska zawiera ciąg znaków „prezes”,
    - nazwa wyświetlana: Rada Nadzorcza [Spółka - Centrala] – lista adresów mailowych wszystkich Członków Rady Nadzorczej Spółki; kryterium wyboru do listy: nazwa Komórki organizacyjnej zawiera ciąg znaków „Rada Nadzorcza”,

- nazwa wyświetlana: Dyrektorzy [Spółka Centrala] – lista adresów mailowych wszystkich osób zatrudnionych w Spółce na stanowisku: Dyrektora; kryterium wyboru do listy: nazwa stanowiska zawiera ciąg znaków „Dyrektor”,
  - nazwa wyświetlana: Dyrektorzy [Spółka - Oddział] – lista adresów mailowych wszystkich osób zatrudnionych w oddziale Spółki na stanowisku: Dyrektora; kryterium wyboru do listy: nazwa stanowiska zawiera ciąg znaków „Dyrektor”,
  - nazwa wyświetlana: Pracownicy [Spółka - Centrala] – lista adresów mailowych wszystkich osób zatrudnionych w Spółce; lista ta nie obejmuje Członków Zarządu i Rady Nadzorczej,
  - nazwa wyświetlana: Pracownicy [Spółka - Oddział] – lista adresów mailowych wszystkich osób zatrudnionych w oddziale Spółki; lista ta nie obejmuje Członków Zarządu i Rady Nadzorczej,
- b. domyślnie każda z Liniowych list dystrybucyjnych ma nałożone restrykcje ograniczające możliwość wysyłania na nie wiadomości; uprawnieniami do wysyłania na Liniową listę dystrybucyjną zarządza właściciel Listy dystrybucyjnej, w szczególności może on zdecydować o zdjęciu nałożonej restrykcji,
- c. na każdą Liniową listę dystrybucyjną domyślnie mają uprawnienia skrzynki funkcyjne w obszarze komunikacji (np. Komunikat PGE S.A.). Jedynie ze skrzynek funkcyjnych obszaru komunikacji może wychodzić wysyłka na listy dystrybucyjne typu Pracownicy (oddziału, Spółki, Grupy PGE) – wyjątek stanowi skrzynka osobowa Prezesa Zarządu PGE S.A. (posiada uprawnienia na wszystkie Listy dystrybucyjne) oraz Prezes Zarządu danej Spółki (posiada uprawnienia do wysyłki na Liniowe listy dystrybucyjne swojej Spółki),
- d. nadawanie uprawnień do wysyłania na Liniową listę dystrybucyjną realizowane jest przez modyfikację dedykowanej dla tej listy grupy zabezpieczeń; modyfikacja polega na dodaniu lub usunięciu Konta Użytkownika lub innej Listy dystrybucyjnej,
- e. zmiana właściciela Liniowej listy dystrybucyjnej może nastąpić tylko na wniosek Kierującego komórką właściwą ds. komunikacji w Spółce lub jego Przełożonego,
- f. informację o osobach występujących w roli właściciela Liniowej listy dystrybucyjnej udostępnia Kierujący komórką właściwą ds. komunikacji wewnętrznej w PGE S.A.
- 6.9.2 Globalne listy dystrybucyjne:
- a. założenie Globalnej listy dystrybucyjnej wymaga złożenia wniosku na Service Desk; wniosek kierowany jest do akceptacji komórki właściwej ds. komunikacji wewnętrznej w PGE S.A.,
  - b. w przypadku, gdy proponowana nazwa Listy dystrybucyjnej nie jest zgodna z przyjętą konwencją nazewnictwa, Administrator Techniczny może tę nazwę zmienić,
  - c. jeżeli w zgłoszeniu nie zaznaczono inaczej właścicielem nowo tworzonej listy zostaje osoba zgłaszająca,
  - d. nie nakłada się restrykcji ograniczających możliwość wysyłania wiadomości na Globalne listy dystrybucyjne,
  - e. zmiana właściciela Globalnej listy dystrybucyjnej może nastąpić na wniosek obecnego właściciela lub jego Przełożonego,
  - f. usunięcie Globalnej listy dystrybucyjnej może zostać zlecone jedynie przez Właściciela Listy dystrybucyjnej lub jego Przełożonego.
- 6.9.3 Lokalne listy dystrybucyjne – są tworzone i zarządzane samodzielnie przez Użytkownika danego Konta pocztowego.

## 6.10 ZASADY KORZYSTANIA Z SIECI KORPORACYJNEJ

- 6.10.1 Zabrania się podłączania do Sieci korporacyjnej jakichkolwiek urządzeń nieposiadających autoryzacji CUW-ICT. Wyjątek stanowi dedykowana sieć dla gości Spółki.
- 6.10.2 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 podgląd operacji), w szczególności:
- a. w ramach korzystania ze służbowej sieci Wi-Fi, Bluetooth:
    - zabrania się Użytkownikom uruchamiania punktów dostępowych na terenie wszystkich Jednostek organizacyjnych z wyjątkiem uzasadnionej konieczności wykorzystania służbowego Urządzenia Mobilnego, jako hotspotu osobistego,
    - każdy Użytkownik zobowiązany jest bezwzględnie wyłączyć porty bezprzewodowe WiFi oraz Bluetooth w urządzeniach podłączonych do Sieci korporacyjnej lub innych urządzeń mobilnych (np. podczas komunikacji pomiędzy telefonem komórkowym i laptopem).
  - b. obsługa połączeń wdzwanianych:
    - zabrania się korzystania z połączeń wdzwanianych (poprzez modemy) Użytkownikom podłączonym do Sieci korporacyjnej,

- zabrania się budowania dostępu wdzwanianych do Systemów Teleinformatycznych udostępniających zasoby Spółki (serwery, urządzenia aktywne, Komputery Biurowe, itp.).
- c. dla łącz internetowych:
  - zabrania się łączenia z Internetem z urządzeń (Komputerów Biurowych, Urządzeń Mobilnych) podłączonych do Sieci korporacyjnej poprzez łącza GPRS, WiFi, Bluetooth, modem, itp.,
  - zabrania się budowania punktów dostępowych do Internetu z wyjątkiem uzasadnionej konieczności wykorzystania służbowego Urządzenia Mobilnego, jako hotspotu osobistego.

W przypadku działań Osób Trzecich, odpowiedzialność za prawidłowość tych działań spoczywa na danym Opiekunie Osoby Trzeciej.

- 6.10.3 Użytkownik ma prawo korzystać z sieci Internet, wyłącznie:
- a. w celach związanych z realizacją zadań służbowych,
  - b. zgodnie z obowiązującymi przepisami prawa,
  - c. w zakresie przyznanych uprawnień.
- 6.10.4 Użytkownikowi zabrania się korzystania z sieci Internet, w celu:
- a. uzyskania nieuprawnionego dostępu do Zasobów ICT będących własnością Spółki lub Systemów Teleinformatycznych podmiotów zewnętrznych,
  - b. pobierania, udostępniania i rozpowszechniania jakichkolwiek materiałów (informacji, Danych, tekstów, programów komputerowych, dźwięków, fotografii, grafik, filmów) naruszających prawa własności intelektualnej,
  - c. pobierania, udostępniania i rozpowszechniania jakichkolwiek materiałów zakazanych przepisami prawa, w tym m.in.: zawierających groźby, treści obraźliwe, zniesławiające, pornograficzne lub naruszające w jakikolwiek inny sposób prawa innych osób.
- 6.10.5 Zabronione jest podejmowanie przez Użytkowników działań powodujących istotne ograniczenia w korzystaniu z sieci Internet przez innych Użytkowników, a w szczególności:
- a. pobieranie dużej ilości Danych, w sytuacji, gdy nie jest to uzasadnione wykonywanymi obowiązkami służbowymi,
  - b. podejmowanie działań skutkujących ograniczeniami w funkcjonowaniu jakichkolwiek usług sieciowych.
- 6.10.6 Wykorzystywanie Internetu przez Użytkownika jest kontrolowane przez Spółkę, ze szczególnym uwzględnieniem monitoringu adresów przeglądanych stron Internetowych.
- 6.10.7 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.
- 6.10.8 Korzystając ze Zdalnego Dostępu należy wykorzystywać zaufane łącza Internetowe. W szczególności zalecane jest korzystanie z sygnału udostępnianego z telefonów służbowych. Zabrania się wykorzystywania łącz niezabezpieczonych, publicznych oraz od nieznanymi dostawców.
- 6.10.9 Podczas pracy ze Zdalnym Dostępem, Użytkownik ma obowiązek zapewnić Poufność przetwarzanych Danych poprzez:
- a. używanie ekranowych filtrów prywatyzacyjnych (służących do zachowania poufności wyświetlanych informacji) w sytuacji, gdy Użytkownik nie może w inny sposób zapewnić poufności informacji danych wyświetlanych na ekranie w inny sposób,
  - b. zweryfikowanie czy otoczenie zapewnia bezpieczeństwo pracy (w tym umiejscowienie osób, luster, szyb, kamer) itp.,
  - c. zabezpieczenia Komputera Biurowego podczas pozostawiania go bez opieki (m.in. poprzez stosowanie zamkniętych pomieszczeń lub linek zabezpieczających),
  - d. chronienie treści rozmów telefonicznych przed osobami niepowołanymi wykonywanych z użyciem zarówno telefonii konwencyjnej, mobilnej oraz systemów telekonferencyjnych (np. Skype, Teams).

## 6.11 ZASADY CZYSTEGO BIURKA

- 6.11.1 Na biurku powinny znajdować się jedynie materiały zawierające Informacje podlegające ochronie aktualnie wykorzystywane przez Pracownika. Wszystkie pozostałe materiały muszą zostać przechowywane w przeznaczonym do tego miejscu (miejsce przechowywania zależy od Poziomu ochrony, którym objęty jest dany materiał).
- 6.11.2 Nie należy pozostawiać materiałów zawierających Informacje podlegające ochronie bez nadzoru.
- 6.11.3 Po zakończeniu wykonywania obowiązków służbowych należy schować wszystkie materiały zawierające Informacje podlegające ochronie – nawet jeśli następnego dnia będziemy z nich korzystać.

- 6.11.4 Należy zamykać pomieszczenie służbowe na klucz, kiedy nie znajduje się w nim żaden uprawniony do tego pracownik.
- 6.11.5 W pomieszczeniu nie mogą przebywać osoby nieuprawnione, bez nadzoru osoby upoważnionej do przebywania w pomieszczeniu.
- 6.11.6 Po spotkaniach, w trakcie których pojawiały się istotne z punktu widzenia organizacji Informacje, należy usunąć je z pomieszczeń gdzie były utrwalone (z tablicy magnetycznej, itd.).
- 6.11.7 Po skorzystaniu z drukarki, kopiarki, skanera lub faksu należy upewnić się, że nie pozostawiono na urządzeniu żadnego materiału zawierającego Informacje podlegające ochronie.
- 6.11.8 Drukując dokumenty należy zweryfikować, czy wydrukowane zostały wszystkie strony. W przypadku nieudanej próby wydrukowania użytkownik powinien skontaktować się z osobą odpowiedzialną za eksploatację urządzenia, jeżeli zachodzi podejrzenie, iż materiał zostanie wydrukowany bez nadzoru.
- 6.11.9 Po użyciu skanera usunąć skanowany dokument z urządzenia.
- 6.11.10 Nie należy wyrzucać materiałów zawierających Informacje podlegające ochronie do kosza. Materiały te, niszczymy w taki sposób, aby ich odczytanie było niemożliwe. Do tego celu najlepiej używać służbowe niszczarki lub pojemniki na dokumenty przeznaczone do zniszczenia, dostarczone przez Pracodawcę.

## 6.12 ZASADY CZYSTEGO EKRANU

- 6.12.1 Komputer, urządzenie mobilne, tablet powinien posiadać „Blokadę ekranu” chronioną hasłem / PIN-em.
- 6.12.2 Powyższe wymaganie nie dotyczy komputerów wykorzystywanych do ciągłego monitoringu (urządzeń technicznych, bezpieczeństwa fizycznego itp.) z zastrzeżeniem, że pomieszczenie nigdy nie pozostaje dostępne bez nadzoru osoby uprawnionej.
- 6.12.3 Każdorazowo opuszczając stanowisko pracy należy bądź uruchomić blokadę ekranu (np. w systemie Windows: naciskając jednocześnie klawisze: [Windows] i [L] albo wcisnąć kombinację klawiszy [Ctrl] [Alt] [Del] i użyć funkcji „Zablokuj komputer”, bądź poprzez wyłączenie komputera.
- 6.12.4 Chroń ekran urządzenia przed nieuprawnionym podglądem osób nieuprawnionych (np. poprzez zastosowanie w filtrów prywatyzujących (folia ograniczająca pole widzenia).
- 6.12.5 Na zakończenie pracy należy zamknąć aktywne sesje oraz wyłączyć komputer.
- 6.12.6 Zabierając komputer przenośny poza siedzibę Spółki (praca zdalna, spotkanie poza siedzibą) należy wyłączyć komputer używając funkcji „Zamknij system”. Należy mieć na uwadze, że uśpienie, hibernacja komputera sprawia, że szyfrowany dysk jest odblokowany, co w przypadku kradzieży bądź zagubienia komputera, pozwala osobom nieuprawnionym na dostęp do Informacji Przetwarzanych na komputerze.
- 6.12.7 Zabrania się zapisywania i przechowywania danych logowania (nazwa użytkownika i/lub hasła) na dyskach twardych komputerów w postaci niezaszyfrowanej lub takiego z nimi postępowania, które umożliwi w prosty sposób dostęp do haseł osobom nieuprawnionym, np. zapisanie hasła na karteczce i przyklejenie jej do monitora.
- 6.12.8 Ekrany monitorów komputerowych należy ustawić w sposób uniemożliwiający bezpośredni odczyt treści na nim wyświetlanych przez osoby postronne, np. skierowane tyłem lub bokiem do drzwi wejściowych i okien, ewentualnie wyposażyć ekrany w filtr prywatyzujący.
- 6.12.9 Przetwarzanie materiałów zawierających Informacje objęte IV Poziomem ochrony, zgodnie z *PROG 00037 Procedura Ogólna – Wytyczne w zakresie Klasyfikacji i ochrony informacji w Grupie Kapitałowej PGE*, na przenośnych Nośnikach danych i urządzeniach mobilnych (w tym telefonach, tabletach) jest możliwe tylko w sytuacji, kiedy te urządzenia posiadają uruchomione funkcje szyfrowania danych.

## 6.13 POSTANOWIENIA KOŃCOWE

- 6.13.1 W przypadku korzystania z Zasobów ICT przetwarzających informacje chronione przez Spółkę, niezależnie od postanowień określonych w Procedurze, należy stosować się do przepisów określonych w odrębnych regulacjach obowiązujących w Spółkach.
- 6.13.2 W zakresie nieobjętym niniejszą Procedurą lub innymi regulacjami zawartymi w aktach normatywnych Spółki i dokumentacjach Systemów, Użytkownicy mają obowiązek postępować zgodnie z interesem Spółki, kierując się najlepszą wiedzą, wraz z dochowaniem należytej staranności we wszystkich podejmowanych działaniach.
- 6.13.3 Wszelkie 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.
- 6.13.4 Z dniem wejścia w życie niniejszej Procedury, traci moc obowiązująca *PROG 00103/B Procedura Ogólna korzystania z Zasobów Teleinformatycznych (ICT) w GK PGE*.

6.13.5 Procedura wchodzi w życie po upływie 7 dni od dnia jej publikacji w Banku DSZ.