

## PROCEDURA OGÓLNA BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

PROG 00039 / A

Sygn.: PGE/CENT/DSIT/4.07

Data zatwierdzenia: 2015/06/10

Obowiązuje od: 2015/06/10

### I CEL I ZAKRES

- 1.1 Celem Procedury Ogólnej bezpieczeństwa teleinformatycznego jest zapewnienie prawidłowej eksploatacji Systemów Teleinformatycznych i Sieci Korporacyjnej, minimalizacja ryzyka awarii oraz wykrywanie nieautoryzowanych działań związanych z Przetwarzaniem Informacji.
- 1.2 Procedura obejmuje swoim zakresem zasady bezpieczeństwa teleinformatycznego dotyczące wszystkich Zasobów w Spółce przetwarzanych w Systemach Teleinformatycznych.
- 1.3 Stosownie do zapisów Kodeksu Grupy PGE, Dokumenty Systemu Zarządzania Grupy PGE, są wydawane w celu osiągnięcia takich wartości jak:
  - a. spójność działania Spółek,
  - b. przejrzystość działania Spółek i Grupy PGE,
  - c. zwiększenie efektywności i skuteczności kontroli procesów biznesowych, organizacyjnych i prawnych w Grupie PGE,
  - d. ograniczenia ryzyk biznesowych.
- 1.4 Podstawę uchwalenia Procedury stanowi Rozdział 5 Kodeksu Grupy PGE oraz postanowienia statutów (umów) Spółek.

### II ODPOWIEDZIALNOŚĆ

- 2.1 Za stosowanie wymagań niniejszej Procedury odpowiedzialne są Spółki a w szczególności:
  - a. wszyscy Pracownicy Spółki, Członkowie Organów Spółki i Osoby Trzecie realizujące określone zadania na rzecz Spółki,
  - b. Dyrektor Departamentu Strategii IT Grupy PGE w zakresie aktualizacji Procedury.
- 2.1.2 Do Spółek z Grupy PGE Procedura ma bezpośrednie zastosowanie.
- 2.1.3 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. jednostki w Grupie PGE, która ma w swoich podstawowych zadaniach zarządzanie korporacyjne w Grupie PGE – dla pozostałych Spółek.
- 2.2 Wszelkie odstępstwa od niniejszej Procedury muszą być zaakceptowane przez Dyrektora Departamentu Strategii IT w PGE S.A.

### III DOKUMENTY POWIĄZANE

- 3.1 *PROG 00040 Procedura Ogólna zarządzania dostępem do podstawowych zasobów informatycznych Grupy PGE*
- 3.2 *PROG 00041 Procedura Ogólna zarządzania zdalnym dostępem do Sieci Korporacyjnej (VPN)*
- 3.3 *PROG 00042 Procedura Ogólna – udostępnianie komputerowych urządzeń biurowych w Grupie PGE*
- 3.4 *PROG 00043 Procedura Ogólna – zasady zarządzania dostępem do Korporacyjnej Sieci Bezprzewodowej (WiFi)*
- 3.5 *PROG 00044 Procedura Ogólna zarządzania dostępem do sieci Internet*
- 3.6 *PROG 00045 Procedura Ogólna - zasady bezpieczeństwa dla Urządzeń Mobilnych w Grupie PGE*
- 3.7 *PROC 00018\_B Procedura ochrony Tajemnicy Spółki w PGE Polska Grupa Energetyczna SA*
- 3.8 *PROC 00030\_B Procedura ochrony danych osobowych w PGE Polska Grupa Energetyczna SA*
- 3.9 *PROC 55001 A Procedura Zarządzania Incydentami Bezpieczeństwa Teleinformatycznego w PGE Systemy S.A.*

### IV ZAŁĄCZNIKI

Brak

## V SKRÓTY I DEFINICJE

### CUW ICT:

Dokumentacja Systemu Zarządzania; Pracownik; Przełożony; Spółka Grupy PGE, Spółka, Spółki:

### Skróty użyte na potrzeby niniejszego dokumentu:

- ABI** – Administrator Bezpieczeństwa Informacji - osoba wyznaczona przez Administratora danych nadzorująca przestrzeganie zasad ochrony danych osobowych w Spółce (ustawa o ochronie danych osobowych, art. 36 ust.3)
- CUW ICT** – Centrum Usług Wspólnych ICT - podmioty, których celem jest świadczenie usług ICT na rzecz pozostałych spółek Grupy PGE w oparciu o model optymalizujący efektywność ICT w Grupie PGE. Rolę CUW ICT pełnią trzy spółki:
- a. PGE Systemy w zakresie usług informatycznych,
  - b. Exatel w zakresie usług telekomunikacyjnych,
  - c. Energo-Tel w zakresie usług eksploatacji, serwisu sieci i infrastruktury telekomunikacyjnej.
- Exatel nie jest CUW ICT w rozumieniu ustawy Prawo Zamówień Publicznych. W odróżnieniu od PGE Systemy oraz Energo-Tel, Exatel większość swoich usług świadczy poza Grupą PGE
- ICT** – teleinformatyka - 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 automatyzacji, bądź też konieczności wyłączenia fragmentu obszaru z definicji Usługi ICT stosowne decyzje będzie podejmował Komitet ICT
- SLA** – Service Level Agreement – Umowa o gwarantowanym poziomie Usług
- System OW** – System Teleinformatyczny do obsługi Wniosków

### Definicje pojęć użyte na potrzeby niniejszego dokumentu:

- 5.1 **Administrator Danych** - organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych (ustawa o ochronie danych osobowych, art. 7 ust. 4).
- 5.2 **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.
- 5.3 **Bezpieczeństwo Informacji** -zapewnienie Poufności, Integralności i Dostępności informacji przetwarzanych w PGE Systemy S.A., czyli zabezpieczanie jej przed nieautoryzowanym dostępem, zmianą, utratą, uszkodzeniem, zniszczeniem lub zatajeniem.
- 5.4 **Dokumentacja Systemu Zarządzania (DSZ)** – dokument / dokumenty wydawane na podstawie art. 9 Kodeksu Grupy PGE, wykorzystywane przy prowadzeniu działalności Spółki, służące komunikowaniu wymagań i zasad postępowania podczas realizacji procesu, oraz zapewniające ich jednolitość i spójność. W szczególności dokumenty takie:
- a. określają i ustalają zasady organizacji i postępowania w procesie Spółki / Spółek,
  - b. pozwalają nadzorować procesy,
  - c. określają zakres obowiązków i zadań w procesach, Spółce / Spółkach,
  - d. zawierają uzgodnienia wymagań między komórkami / jednostkami organizacyjnymi,
  - e. zawierają 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 Mapy i Karty procesów Grupy PGE.
- 5.5 **Dostępność** - właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu.
- 5.6 **Dziennik Systemu Teleinformatycznego / Dziennik** – 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 Bezpieczeństwa.
- 5.7 **Hasło** - ciąg znaków, który służy do uwierzytelniania w Systemie Teleinformatycznym.
- 5.8 **Identyfikator w Systemie Teleinformatycznym (Identyfikator)** - unikalny ciąg znaków jednoznacznie identyfikujący w Systemie Teleinformatycznym Użytkownika lub inny System Teleinformatyczny.



- 5.9 **Incydenty Bezpieczeństwa** - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z Bezpieczeństwem Informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają Bezpieczeństwu Informacji.
- 5.10 **Integralność** - właściwość zapewnienia dokładności i kompletności. Integralność informacji/danych - oznacza, że dane nie będą w nieautoryzowany lub przypadkowy sposób zmodyfikowane przez nieuprawnione osoby.
- 5.11 **Jednostka organizacyjna** - organizacja powołana do wykonywania określonych części zadań w Spółce, mająca ustalone miejsce w jej strukturze organizacyjnej. Jednostką organizacyjną może być oddział.
- 5.12 **Kierownik Komórki organizacyjnej** - osoba kierująca Komórką organizacyjną w rozumieniu Regulaminu organizacyjnego Spółki.
- 5.13 **Komórka organizacyjna / Komórka** - jedno - lub wieloosobowe ciało powołane do wykonywania określonych części zadań w Jednostce organizacyjnej, mające ustalone miejsce w jej strukturze organizacyjnej. Komórka może być: departament, biuro, zespół, wydział, dział, sekcja lub inna komórka wewnętrzna w Spółce lub oddziale Spółki.
- 5.14 **Konto** - zbiór praw dostępu do Systemu Teleinformatycznego, dedykowany dla Użytkownika lub innego Systemu Teleinformatycznego identyfikowanych przez Identyfikator i środki uwierzytelniania takie, jak Hasła, Hasła jednorazowe, klucze i certyfikaty cyfrowe, tokeny sprzętowe (karty, klucze, transpondery), sygnatury biometryczne lub ich kombinacje.
- 5.15 **Konto Administracyjne** - konto o wyższych uprawnieniach w Systemie używane w celach obsługi technicznej Systemu oraz realizacji działań przez Administratora Systemu.
- 5.16 **Nośnik Informacji / Nośnik** - wszelkiego rodzaju nośniki danych, używane w procesie Przetwarzania informacji, w szczególności dyski twarde, płyty CD/DVD/BR, taśmy DLT/DDS, pamięci przenośne, dyski magneto-optyczne, papier.
- 5.17 **Opiekun Osoby Trzeciej** - Kierownik Komórki organizacyjnej, w ramach której Osoba Trzecia realizuje swoje zadania lub Pracownik tej Komórki organizacyjnej posiadający pisemne upoważnienie wydane przez powyższego Kierownika.
- 5.18 **Organy Spółki** - Organy Spółki w rozumieniu Regulaminu Organizacyjnego Spółki.
- 5.19 **Osoba Trzecia** - pracownik firmy zewnętrznej realizujący określone zadania na rzecz Spółki.
- 5.20 **Poufność** - właściwość, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.
- 5.21 **Pracownik** - osoba, z którą pracodawca nawiązał stosunek pracy w rozumieniu art. 22 K.P., nie obejmuje osób wykonujących pracę na innej podstawie niż stosunek pracy.
- 5.22 **Procedura** – PROG 00039/A Procedura Ogólna bezpieczeństwa teleinformatycznego.
- 5.23 **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.
- 5.24 **Przetwarzanie Informacji** - jakiegokolwiek operacje wykonywane na informacji, w szczególności takie jak ich zbieranie, utrwalanie, przechowywanie, opracowywanie, modyfikowanie, udostępnianie, przesyłanie i usuwanie.
- 5.25 **Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
- 5.26 **Sieć Korporacyjna** - urządzenia komputerowe, oprogramowanie i okablowanie wraz z urządzeniami sieciowymi, umożliwiające gromadzenie, przetwarzanie oraz wymianę informacji.
- 5.27 **Spółka Grupy PGE, Spółka, Spółki** – podmiot / podmioty prawa handlowego wchodzące w skład Grupy PGE.
- 5.28 **System Pomocniczy** - (klasa I) - system przetwarzający dane, których Dostępność oraz Integralność nie powoduje trudności w funkcjonowaniu Procesów biznesowych Spółki.
- 5.29 **System Ważny** - (klasa II) - system przetwarzający dane, których utrata, bądź trwałe uszkodzenie mogą zakłócić przebieg Procesów biznesowych Spółki.
- 5.30 **System Krytyczny** - (klasa III) - system przetwarzający dane, których nawet chwilowa niedostępność może spowodować poważne zakłócenie w przebiegu kluczowych Procesów biznesowych, a w konsekwencji negatywne następstwa dla kondycji ekonomicznej Spółki.
- 5.31 **System Teleinformatyczny (System)** - zespół środków technicznych wraz z oprogramowaniem tworzący logiczną i nierozzerwalną całość wyodrębnioną ze względu na dostarczaną funkcjonalność przy założeniu, że głównym jego celem jest Przetwarzanie Informacji.



- 5.32 **Umowa** - Umowa o pracę lub Umowa cywilno-prawna.
- 5.33 **Użytkownik** - osoba uprawniona do korzystania z Systemu Teleinformatycznego. Użytkownikami mogą być Członkowie Organów Spółki, Pracownicy oraz Osoby Trzecie.
- 5.34 **Właściciel Zasobu** - osoba w strukturze organizacyjnej Spółki sprawująca nadzór nad Zasobem oraz dostępem do Zasobu.
- 5.35 **Wniosek** - formalne wystąpienie o podjęcie określonych działań w zakresie nadania, modyfikacji lub odebrania uprawnień do zasobu lub usługi.
- 5.36 **Zasób** - informacja stanowiąca wartość dla Spółki, w postaci nieutralizowanej lub utrwalonej na dowolnym Nośniku Informacji.

## VI REALIZACJA

### 1.1 POSTANOWIENIA OGÓLNE

- 1.1.1 Procedura Ogólna bezpieczeństwa teleinformatycznego stanowi zbiór zasad niezbędnych do zapewnienia właściwej ochrony Przetwarzanych Informacji w Systemach Teleinformatycznych wykorzystywanych w Spółce, w szczególności są to zasady i procedury opisujące sposób zarządzania Systemami, Siecią Korporacyjną (ochronę przed złośliwym oprogramowaniem, bezpieczeństwo sieci, kopie zapasowe, monitorowanie Systemów i sieci) oraz regulują zasady kontroli dostępu do Zasobów (zarządzanie uprawnieniami, polityka Hasel, zdalny dostęp do Sieci Teleinformatycznej).

### 1.2 NADAWANIE UPRAWNIEŃ. ROZLICZALNOŚĆ

- 1.2.1 Każdy Zasób w Spółce posiada swojego właściciela – Właściciela Zasobu, który sprawuje nadzór nad Zasobem oraz dostępem do Zasobu.
- 1.2.2 Jedną z form dostępu do Zasobów Spółki jest ich udostępnienie poprzez Systemy Teleinformatyczne.
- 1.2.3 Zasoby 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.
- 1.2.4 Właściwy podmiot z CUW ICT odpowiedzialny za utrzymanie danego Systemu wyznacza dla każdego Systemu Teleinformatycznego:
  - a. Administratora Technicznego, który sprawuje opiekę nad powierzonym mu Systemem od strony technicznej,
  - b. zastępcę na wypadek nieobecności Administratora Technicznego.
- 1.2.5 Właściwy podmiot z CUW ICT odpowiedzialny za utrzymanie Systemów Teleinformatycznych zobowiązany jest do utrzymywania aktualnej listy Systemów z przypisanymi Administratorami.
- 1.2.6 W przypadkach szczególnych (np. działania projektowe) można utworzyć tymczasowe Konto administracyjne dla Administratora, który ma przeprowadzić wymagane czynności.
- 1.2.7 Wszyscy Administratorzy oraz Użytkownicy posiadają unikatowy Identyfikator oraz Hasło do Systemu w celu zapewnienia Rozliczalności.
- 1.2.8 Administratorzy korzystają z Kont administracyjnych wyłącznie do zarządzania Systemem. Pozostałe prace wykonują na Koncie zwykłego Użytkownika.
- 1.2.9 W przypadku istnienia Kont współdzielonych oraz braku możliwości rozdzielenia uprawnień należy ściśle zdefiniować grupę Administratorów korzystających z tych Kont.
- 1.2.10 Identyfikator Użytkownika, którego uprawnienia wygasły lub zostały odebrane nie może zostać przydzielony innemu Użytkownikowi.
- 1.2.11 Konto może być używane wyłącznie przez osobę, której zostało przyznane.

### 1.3 OCHRONA PRZED KODEM ZŁOŚLIWYM

- 1.3.1 W Spółce każde urządzenie komputerowe typu stacja robocza oraz serwer objęte są ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego oraz zapory sieciowej.
- 1.3.2 Każdy komputer przenośny powinien być dodatkowo wyposażony w osobistą zaporę sieciową w celu zapewnienia ochrony podczas łączenia się z zewnętrznymi sieciami. Wymagana jest instalacja zapory sieciowej innej niż systemowa, charakteryzującej się wyższą skutecznością działania.
- 1.3.3 Za instalację i właściwe skonfigurowanie oprogramowania antywirusowego oraz zapory sieciowej na stacjach roboczych, serwerach, komputerach przenośnych odpowiada właściwy Administrator.
- 1.3.4 Wszystkie Nośniki wymienne używane poza Spółką, przed rozpoczęciem pracy z tymi Nośnikami w sieci Spółki, należy sprawdzić za pomocą aktualnego oprogramowania antywirusowego.



- 1.3.5 Zarządzanie systemem antywirusowym jest scentralizowane i realizowane przez CUW ICT.
- 1.3.6 Aktualizacja baz wirusów musi się odbywać automatycznie, przynajmniej raz dziennie.
- 1.3.7 Po każdej naprawie i konserwacji urządzenia, a przed ponownym włączeniem do Sieci Korporacyjnej zawartość stałych Nośników komputerowych jest sprawdzana za pomocą aktualnego oprogramowania antywirusowego zawierającego najnowsze bazy antywirusowe.
- 1.3.8 W przypadku, gdy stacje robocze oraz serwery nie są objęte ochroną w czasie rzeczywistym Administrator, co najmniej raz w tygodniu dokonuje rutynowej kontroli pod kątem obecności złośliwego oprogramowania, przy czym kontrola może być realizowana w sposób:
  - a. automatyczny, zgodnie z harmonogramem zdefiniowanym w scentralizowanym systemie antywirusowym,
  - b. ręczny na żądanie.

#### 1.4 AKTUALIZACJA SYSTEMÓW

- 1.4.1 Aktualizacja Systemów odbywa się automatycznie na bieżąco. W przypadku braku możliwości automatycznej aktualizacji – Systemy aktualizowane są pakietami sprawdzonych poprawek. Specjalistyczne Systemy aktualizowane są zgodnie z zapisami znajdującymi się w umowie serwisowej na dany System.
- 1.4.2 Za przeprowadzanie aktualizacji oraz jej udokumentowanie odpowiedzialni są Administratorzy techniczni przypisani do danych Systemów.
- 1.4.3 Administratorzy techniczni zobowiązani są do weryfikowania stabilności wprowadzanych aktualizacji. W przypadku uzasadnionych wątpliwości, co do poprawności aktualizacji Administrator może podjąć decyzję o rezygnacji z instalacji, odnotowując ten fakt w dzienniku Systemu Teleinformatycznego.

#### 1.5 KOPIE ZAPASOWE

- 1.5.1 Dla Systemów krytycznych, Administratorzy są zobowiązani do opracowania, przyjęcia i stosowania określonego planu wykonywania kopii zapasowych Systemu. Plan ten powinien zostać utrwalony w formie pisemnej i przechowywany w bezpiecznym miejscu.
- 1.5.2 Za przestrzeganie planu wykonywania kopii odpowiada Administrator Techniczny Systemu.
- 1.5.3 Zaleca się wykonywanie kopii zapasowych na dwóch różnych Nośnikach przechowywanych w dwóch różnych lokalizacjach.
- 1.5.4 Administrator Techniczny odpowiedzialny za wykonanie kopii zapasowej zobowiązany jest do prowadzenia dokumentacji z wykonywanych kopii, która powinna zawierać co najmniej:
  - a. datę i godzinę rozpoczęcia wykonywania kopii zapasowej,
  - b. datę i godzinę zakończenia wykonywania kopii zapasowej,
  - c. jednoznaczne określenie Nośnika/ów, na którym/ch została wykonana kopia,
  - d. oznaczenie typu kopii będącej odnośnikiem do procedury wykonywania kopii zapasowych (np. kopia pełna, przyrostowa, trzecia w cyklu),
  - e. datę i czytelny podpis osoby wykonującej kopię zapasową lub podpis elektroniczny.
- 1.5.5 Na Administratorach wykonujących kopie zapasowe spoczywa obowiązek weryfikowania poprawności wykonania kopii zapasowej.
- 1.5.6 Administrator Techniczny ma obowiązek okresowo przeprowadzać operację odzyskiwania danych z wykonanych kopii zapasowych w celu weryfikacji procesu wykonania kopii. Podczas odtwarzania kopii zapasowych należy określić zakres przywracanych danych. Częstotliwość wykonywania operacji odzyskiwania danych z kopii należy określić w planie tworzenia kopii zapasowych, o którym mowa w pkt 6.5.1 niniejszego rozdziału.
- 1.5.7 Nośniki Informacji należy przechowywać w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem (np. szafy pancerne, szafy ogniotrwałe).
- 1.5.8 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 Trzecim.
- 1.5.9 Nośniki z kopiami zapasowymi muszą być zabezpieczone w sposób zapewniający Poufność danych.
- 1.5.10 Jeżeli Nośniki kopii zapasowych, które zawierają dane archiwalne, 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 po wyrażeniu pisemnej zgody na niszczenie przedmiotowych Nośników przez Członka Zarządu Spółki (lub Spółek z Grupy PGE), której dane dotyczą.



## 1.6 ZARZĄDZANIE BEZPIECZEŃSTWEM SIECI

- 1.6.1 Pod pojęciem Sieci Teleinformatycznej rozumiana jest infrastruktura umożliwiająca elektroniczną wymianę danych pomiędzy poszczególnymi Komórkami organizacyjnymi Spółki oraz w obrębie tych jednostek, łącząca w jedną całość podsieci poszczególnych Komórek Spółki.
- 1.6.2 Za zarządzanie bezpieczeństwem Sieci Teleinformatycznej na potrzeby Spółki odpowiedzialny jest Administrator Techniczny sieci.
- 1.6.3 Zasoby Sieci Teleinformatycznych udostępniane są zgodnie z zasadą minimum koniecznego oznaczającą udostępnianie minimalnych uprawnień wystarczających do skutecznej realizacji danego zadania.
- 1.6.4 Należy zabezpieczyć miejsce styku sieci z Internetem stosując sprzętową zaporę sieciową.
- 1.6.5 Wykorzystując podsieci i technologię VLAN zaleca się logicznie rozdzielić serwery od stacji roboczych i drukarek.
- 1.6.6 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).
- 1.6.7 Wszystkie serwery usług sieciowych udostępnianych w sieci Internet, muszą być zlokalizowane w wydzielonym segmencie sieci styku – strefie zdemilitaryzowanej (strefie ograniczonego zaufania)

## 1.7 DOKUMENTACJA SYSTEMU

- 1.7.1 Administrator Systemu zobowiązany jest do skompletowania oraz prowadzenia kompletnego Archiwum Systemu.
- 1.7.2 Archiwum Systemu powinno zawierać:
  - a. dokumentację dotyczącą uprawnień do Zasobów udostępnianych przez System: wnioski oraz decyzje o nadaniu, modyfikacji lub odebraniu (cofnięciu) uprawnień,
  - b. Dziennik Systemu Teleinformatycznego,
  - c. plan wykonywania kopii zapasowych,
  - d. politykę logowania zdarzeń,
  - e. dokumenty potwierdzające legalność oprogramowania (nośniki instalacyjne, opakowania itp.),
  - f. plan awaryjny,
  - g. wszelką dodatkową dokumentację wynikającą ze specyfikacji Systemu.
- 1.7.3 Archiwum Systemu prowadzone jest w formie elektronicznej, a w uzasadnionych przypadkach w formie papierowej.

## 1.8 INFORMACJE PUBLICZNE DOSTĘPNE NA STRONIE INTERNETOWEJ

- 1.8.1 Informacje, które mają być dostępne publicznie są każdorazowo autoryzowane przez Kierownika Komórki organizacyjnej lub wyznaczoną przez Zarząd osobę odpowiedzialną za zewnętrzne relacje Spółki przed podaniem informacji do wiadomości publicznej. Zamieszczanie informacji na stronach internetowych Spółki możliwe jest wyłącznie przez osoby, którym przypisano takie zadania w zakresie obowiązków.

## 1.9 MONITOROWANIE I NADZÓR NAD SYSTEMAMI

- 1.9.1 Na Administratorach spoczywa obowiązek monitorowania Podatności Technicznych zarządzanych przez nich Systemów. Monitorowanie uwzględnia pozyskiwanie informacji na temat luk w zarządzanych przez nich Systemach.
- 1.9.2 Dla każdego Systemu krytycznego, Systemu ważnego oraz Systemów pomocniczych (systemy operacyjne, serwery poczty, serwery baz danych, routery brzegowe, zapory sieciowe, systemy tworzenia kopii zapasowych itp.) na potrzeby formalnej rejestracji zdarzeń prowadzony jest Dziennik Systemu Teleinformatycznego. Dziennik może być prowadzony w formie elektronicznej lub papierowej.
- 1.9.3 Za rejestrację zdarzeń odpowiedzialni są Administratorzy przypisani do poszczególnych Systemów.
- 1.9.4 Konfiguracja Systemów powinna uwzględniać rejestrację najważniejszych zdarzeń (błędy, nieudane próby uwierzytelnienia oraz uzyskania dostępu do Zasobów, informacje o możliwej awarii itp.) oraz umożliwiać okresową ich analizę zgodnie z następującą częstotliwością minimalną:

System	Częstotliwość minimalna
Krytyczny	2 razy w tygodniu
Ważny	1 raz w tygodniu
Pomocniczy	1 raz w tygodniu

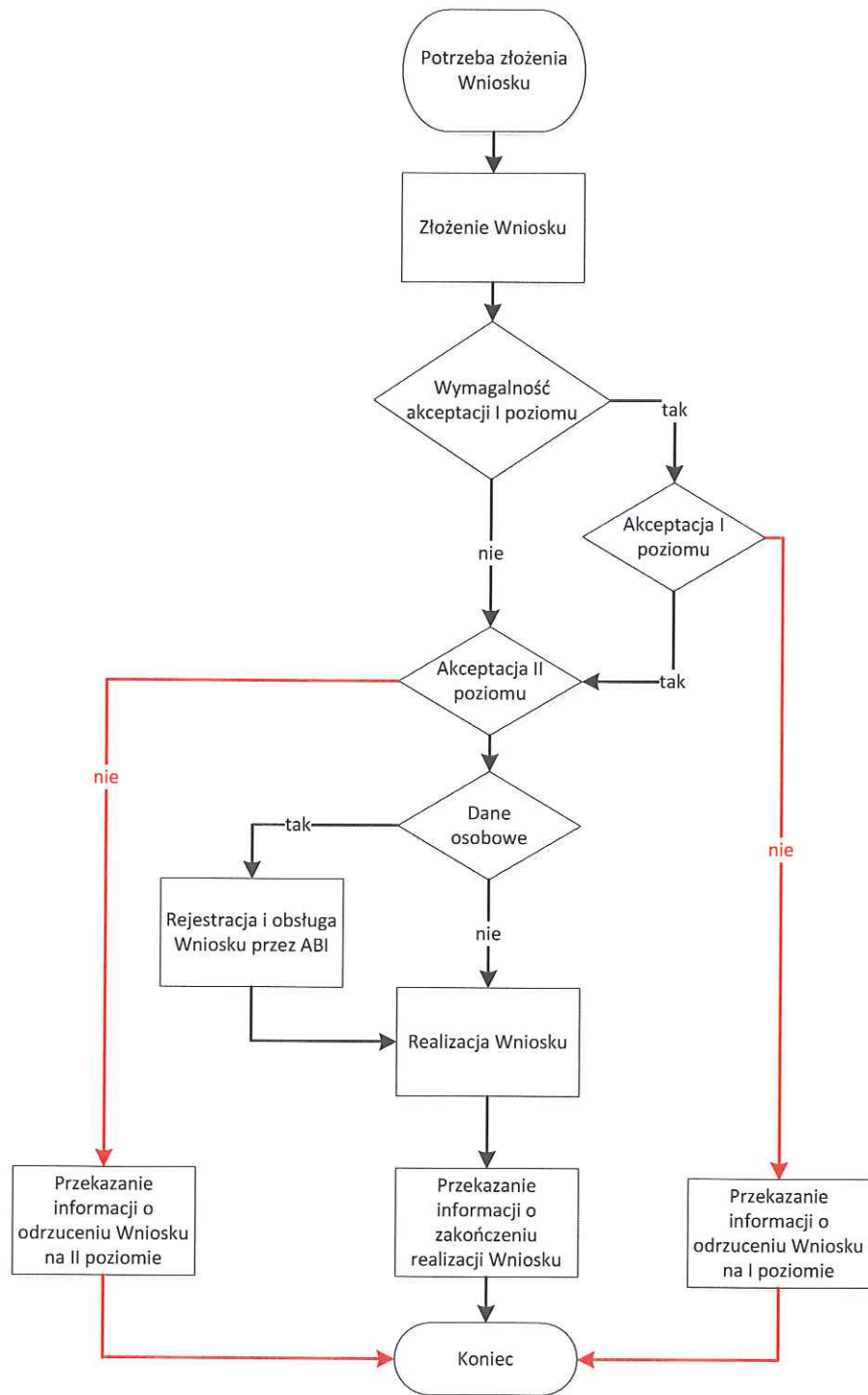
- 1.9.5 Dzienniki dla Systemów Krytycznych, Systemów Ważnych i Systemów Pomocniczych powinny być objęte procesem tworzenia kopii zapasowych oraz archiwizowane przez okres 5 lat na potrzeby analiz lub postępowań. Kopia Dzienników powinna być tworzona zgodnie z harmonogramem tworzenia kopii zapasowych dla danych Systemów.

## 1.10 SYNCHRONIZACJA ZEGARÓW

- 1.10.1 Wymaga się, aby w Sieci Korporacyjnej dostępny był centralny serwer czasu.
- 1.10.2 Administratorzy są zobowiązani do zapewnienia synchronizacji z centralnym serwerem czasu rzeczywistego wszystkich urządzeń aktywnych sieci, serwerów oraz stacji roboczych.

## 1.11 ZASADY DOSTĘPU DO ZASOBÓW SPÓŁKI

- 1.11.1 Uprawnienia do Systemów Teleinformatycznych udostępniających Zasoby Spółki są nadawane, modyfikowane, odbierane na podstawie Wniosków w Systemie OW dostępnych pod adresem <https://sd.gkpge.pl>.
- 1.11.2 W przypadku braku dostępu do Systemu OW dopuszcza się Wnioski papierowe, które po zatwierdzeniu, powinny być zeskanowane i przesłane na adres <https://sd.gkpge.pl>.
- 1.11.3 Wnioskodawca występuje z Wnioskiem o nadanie uprawnień dla Pracownika w następujących sytuacjach:
- a. Pracownik nowoprzyjęty, nadanie uprawnień w Systemach standardowych - dostępnych dla każdego Pracownika,
  - b. uprawnienia przysługują z racji stanowiska i obowiązków służbowych Pracownika.
- 1.11.4 Wnioskodawca występuje z Wnioskiem o nadanie uprawnień dla Osoby Trzeciej gdy rozpoczyna realizację działań na rzecz Spółki.
- 1.11.5 Wnioskodawca występuje z Wnioskiem o nadanie uprawnień dla Członka Organu Spółki po jego powołaniu.
- 1.11.6 Wnioskodawca występuje z Wnioskiem o modyfikację uprawnień dla Pracownika w następujących sytuacjach:
- a. zmiana stanowiska pracy,
  - b. zmiana obowiązków służbowych.
- 1.11.7 Wnioskodawca występuje z Wnioskiem o modyfikację uprawnień dla Osoby Trzeciej po zmianie zakresu działań realizowanych przez Osobę Trzecią na rzecz Spółki.
- 1.11.8 Wnioskodawca występuje z Wnioskiem o modyfikację uprawnień dla Członka Organu Spółki po zmianie zakresu działań realizowanych przez Członka Organu Spółki.
- 1.11.9 Wnioskodawca występuje z Wnioskiem o odebranie uprawnień dla Pracownika w następujących sytuacjach:
- a. rozwiązanie Umowy o pracę,
  - b. zmiana obowiązków służbowych.
- 1.11.10 Wnioskodawca występuje z Wnioskiem o odebranie uprawnień dla Osoby Trzeciej w następujących sytuacjach:
- a. zakończenie realizacji działań na rzecz Spółki,
  - b. zmiana zakresu działań realizowanych przez Osobę Trzecią na rzecz Spółki.
- 1.11.11 Wnioskodawca występuje z Wnioskiem o odebranie uprawnień dla Członka Organu Spółki po jego odwołaniu.
- 1.11.12 Wnioskodawcą może być:
- a. dla Pracownika – Przełożony, Właściciel Zasobu,
  - b. dla Osoby Trzeciej - Opiekun Osoby Trzeciej, Właściciel Zasobu,
  - c. dla Członka Organu Spółki - Kierownik Komórki organizacyjnej właściwej ds. obsługi władz Spółki, Właściciel Zasobu.
- 1.11.13 W szczególności wnioskodawcą może być sam Użytkownik lub inne osoby wyznaczone do wnioskowania o dany Zasób. W takim przypadku wymagana jest akceptacja Wniosku:
- a. dla Pracownika przez Przełożonego,
  - b. dla Osoby Trzeciej przez Opiekuna Osoby Trzeciej,
  - c. dla Członka Organu Spółki - Kierownika Komórki organizacyjnej właściwej ds. obsługi władz Spółki.
- 1.11.14 Wnioskowanie o Zasoby przebiega według następującego schematu:





L.P.	Czynność	Odpowiedzialność za wykonanie czynności	Opis
<b>Potrzeba nadania, modyfikacji lub odebrania uprawnień do Zasobu</b>			
1.	Złożenie Wniosku	Wnioskodawca	Osoba składająca Wniosek przekazuje niezbędne dane dotyczące składanego Wniosku.
2.	Wymagalność akceptacji I poziomu		Akceptacja nie jest wymagana jeśli Wniosek został złożony dla Pracownika przez Przełożonego, dla Osoby Trzeciej przez jej Opiekuna Osoby Trzeciej, dla Członka Organu Spółki przez Kierownika Komórki organizacyjnej właściwej ds. obsługi władz Spółki, Właściciela Zasobu.
3.	Akceptacja I poziomu	Przełożony, Opiekun Osoby Trzeciej, Kierownik Komórki organizacyjnej właściwej ds. obsługi władz	Przełożony, Opiekun Osoby Trzeciej, Kierownik Komórki organizacyjnej właściwej ds. obsługi władz Spółki jest informowany o potrzebie akceptacji Wniosku. Przełożony dla Pracownika, Opiekun Osoby Trzeciej dla Osoby Trzeciej, Kierownik Komórki organizacyjnej właściwej ds. obsługi władz Spółki dla Członka Organu Spółki akceptuje Wniosek lub odrzuca.
4.	Akceptacja II poziomu	Właściciel Zasobu	Właściciel Zasobu jest informowany o potrzebie akceptacji Wniosku, a następnie akceptuje go lub odrzuca.
5.	Dane osobowe	Właściciel Zasobu	Jeśli Wniosek dotyczy dostępu do danych osobowych, Właściciel Zasobu przekazuje Wniosek do ABI.
6.	Rejestracja i obsługa Wniosku przez ABI	ABI	ABI wydaje upoważnienie do przetwarzania danych osobowych. W przypadku rozszerzenia uprawnień wydawane jest kolejne upoważnienie. Każdorazowo przeprowadzane jest szkolenie Użytkownika z bezpieczeństwa danych osobowych. Użytkownik podpisuje oświadczenie o zapoznaniu się z zasadami ochrony danych osobowych. W przypadku odebrania uprawnień ABI rejestruje ten fakt.
7.	Realizacja Wniosku	Administrator	Administrator otrzymuje informację o potrzebie realizacji Wniosku i wykonuje czynności niezbędne do jego realizacji.
8.	Przekazanie informacji o zakończeniu realizacji Wniosku	Administrator	W momencie skutecznego przekazania danych o wnioskowanych uprawnieniach, wnioskodawca oraz akceptujący informowani są o pozytywnym zakończeniu procesu.
9.	Przekazanie informacji o odrzuceniu Wniosku na I poziomie	Przełożony, Opiekun Osoby Trzeciej, Kierownik Komórki organizacyjnej właściwej ds. obsługi władz	Poinformowanie wnioskodawcy o braku akceptacji I poziomu.
10.	Przekazanie informacji o odrzuceniu Wniosku na II poziomie	Właściciel Zasobu	Poinformowanie wnioskodawcy o braku akceptacji II poziomu.

- 1.11.15 Szczegółowe zasady zarządzania dostępem do podstawowych zasobów informatycznych Grupy PGE (rozumianych jako Sieć Korporacyjna oraz poczta elektroniczna) definiuje PROG 00040 Procedura Ogólna zarządzania dostępem do podstawowych zasobów informatycznych Grupy PGE.
- 1.11.16 Przy zarządzaniu uprawnieniami należy kierować się zasadą nadawania minimalnych uprawnień oraz rozdziału obowiązków.
- 1.11.17 Zarządzanie uprawnieniami Użytkowników powinno być oparte o role, jakie pełnią w organizacji, np. stanowisko lub przynależność do Komórki organizacyjnej.
- 1.11.18 Poszczególne Zasoby mogą mieć zdefiniowane szczegółowe zasady zarządzania uprawnieniami, które muszą być zgodne z niniejszymi zasadami.
- 1.11.19 Uprawnienia dla Osób Trzecich mogą być nadawane jedynie na czas określony, nie dłuższy niż okres realizacji działań na rzecz Spółki.

- 1.11.20 Użytkownicy zobowiązani są zgłaszać Właścicielowi Zasobu fakt posiadania szerszych uprawnień do Zasobu, niż wynika to z zakresu zatwierdzonych uprawnień.

### 1.12 ZARZĄDZANIE KONTAMI ADMINISTRACYJNYMI

- 1.12.1 Zarządzanie Kontami Administracyjnymi odbywa się zgodnie z zasadą minimalnych uprawnień.
- 1.12.2 Jedynie Administratorzy są upoważnieni do posiadania Kont Administracyjnych.
- 1.12.3 Konta lokalne z uprawnieniami administracyjnymi na komputerach przenośnych mogą być utworzone wyłącznie na wniosek Kierującego Komórką organizacyjną jeśli wynika to z zakresu obowiązków danego Pracownika.
- 1.12.4 Użytkownik korzystający z Konta lokalnego z uprawnieniami administracyjnymi automatycznie staje się Administratorem ze wszystkimi wynikającymi z tego obowiązkami.
- 1.12.5 Dostęp przydzielany jest przez Właściciela Zasobu. Pozostałym Użytkownikom należy przydzielać Konta z ograniczonymi uprawnieniami.

### 1.13 ZASADY UWIERZYTELNIANIA W SYSTEMACH TELEINFORMATYCZNYCH

- 1.13.1 Wszyscy Pracownicy Spółki, Osoby Trzecie, Członkowie Organów Spółki posiadający dostęp do Zasobów udostępnianych przez System Teleinformatyczny są zobowiązani uwierzytelnić się (logować) do niego przy użyciu Identyfikatora i Hasła.
- 1.13.2 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.
- 1.13.3 Administratorzy zobowiązani są do konfiguracji następujących zasad dla Haseł Użytkowników jeśli Systemy którymi administrują umożliwiają taką konfigurację:
- Hasło Użytkownika składa się z minimum 8 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 zawierać znaków diakrytycznych (np. ą, ę),
  - Hasło nie może być identyczne z nazwą Konta lub jego częścią,
  - Hasło nie może być imieniem, nazwiskiem, datą urodzenia,
  - Hasło wymaga zmiany co 30 dni,
  - minimalny okres pomiędzy kolejnymi zmianami Hasła to 2 dni,
  - nowe Hasło musi być inne, niż co najmniej 5 ostatnio wprowadzonych Haseł,
  - Hasło nie może zawierać nazwy Konta,
  - Hasło musi składać się z co najmniej 5 różnych znaków,
  - Hasło musi różnić się od poprzedniego co najmniej 3 znakami.
- Każde Hasło powinno spełniać wszystkie wymienione wymagania. Jeżeli z powodu ograniczeń technicznych niemożliwe jest przestrzeganie jednej z zasad, wymagane są nadal pozostałe.

### 1.14 ZDALNY DOSTĘP DO SIECI TELEINFORMATYCZNEJ

- 1.14.1 W Spółce dopuszcza się wykorzystywanie zdalnego dostępu w celu udostępniania Administratorom i Użytkownikom dostępu do Systemów Teleinformatycznych udostępniających Zasoby lub umożliwienia firmom zewnętrznym sprawowania opieki serwisowej.
- 1.14.2 Zdalny dostęp może być udzielony do Systemów wszystkich klas na czas określony lub doraźnie.
- 1.14.3 Prawo zdalnego dostępu do Systemu Teleinformatycznego udostępniającego dany Zasób nadaje Właściciel Zasobu.
- 1.14.4 Udzielenie zdalnego dostępu następuje zgodnie z zasadami dostępu do Zasobów Spółki określonymi w pkt 6.11.
- 1.14.5 Udzielenie zdalnego dostępu wymaga technicznego zabezpieczenia w celu sprawowania kontroli dostępu do Sieci Korporacyjnej.
- 1.14.6 System zdalnego dostępu do Systemów w Sieci Korporacyjnej realizowany jest z zachowaniem następujących zasad:



- a. celem zastosowania systemu zdalnego dostępu do Sieci Korporacyjnej jest zapewnienie bezpiecznego dostępu do Systemów Teleinformatycznych, poprzez uwierzytelnianie Użytkowników za pomocą Identyfikatora i Hasła lub innych metod uwierzytelnienia,
  - b. System zdalnego dostępu umożliwia uprawnionym Użytkownikom szybki, łatwy i bezpieczny dostęp do Systemów Teleinformatycznych znajdujących się w Sieci Korporacyjnej oraz umożliwia podjęcie szybkich działań minimalizujących niewłaściwe funkcjonowanie Systemów Teleinformatycznych, z których korzysta Spółka,
  - c. za administrację systemem zdalnego dostępu do Sieci Korporacyjnej odpowiedzialny jest Administrator Techniczny.
- 1.14.7 Podstawowe zasady bezpieczeństwa:
- a. stacje robocze używane do zdalnego łączenia się z Siecią Korporacyjną powinny być objęte ochroną antywirusową,
  - b. Hasło musi być przechowywane w sposób bezpieczny i minimalizujący możliwość dostępu do niego Osób Trzecich,
  - c. Hasło stanowiące element uwierzytelniający Użytkownika powinno być przechowywane i wprowadzane w sposób uniemożliwiający osobom postronnym poznanie jego treści,
  - d. jeśli zachodzi jakiegokolwiek podejrzenie, że Hasło zostało skompromitowane (poznane przez osobę nieuprawnioną), należy bezzwłocznie dokonać jego zmiany,
  - e. jeżeli zdalny dostęp przydzielany jest pracownikowi firmy zewnętrznej w celach serwisowych i umożliwia on uruchomienie zdalnej sesji terminalowej lub innego oprogramowania umożliwiającego penetrację sieci wewnętrznej z serwisowanego serwera, Administrator Techniczny dokonuje odseparowania serwera od sieci wewnętrznej za pomocą dostępnych środków technicznych w celu zatrzymania i rejestracji niepożądanego ruchu sieciowego z danego serwera.

## 1.15 DOSTĘP DO PROGRAMÓW NARZĘDZIOWYCH

- 1.15.1 Administrator odpowiedzialny jest za ograniczenie Użytkownikom dostępu do programów narzędziowych umożliwiających zmianę parametrów użytkowanego Systemu. Użytkownicy nie powinni mieć możliwości samodzielnego modyfikowania ustawień w systemach operacyjnych.
- 1.15.2 W przypadku systemów operacyjnych z rodziny Microsoft Windows, tam gdzie jest to możliwe, należy zablokować możliwość uruchamiania oraz korzystania z następujących narzędzi:
- a. programu msconfig,
  - b. panelu sterowania,
  - c. konfiguratora połączeń sieciowych,
  - d. edytora rejestru systemu operacyjnego.
- 1.15.3 W przypadku pozostałych systemów operacyjnych należy zablokować możliwość wprowadzania zmian do systemu wykorzystując narzędzia analogiczne do wymienionych w pkt 6.15.2 powyżej, oraz okresowo kontrolować dostęp do narzędzi systemowych.

## 1.16 BEZPIECZEŃSTWO SIECI

- 1.16.1 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 uwierzytelić. W przypadku, gdy przerwanie sesji może spowodować utratę przetwarzanych danych w Systemie, dopuszcza się odstępianie od stosowania zapisów niniejszego punktu.
- 1.16.2 Administratorzy zobowiązani są do blokowania dostępu do niebezpiecznych stron WWW. Listę blokowanych adresów zatwierdza Dyrektor Departamentu Strategii IT w PGE.

## 1.17 PRZEGLĄD LEGALNOŚCI OPROGRAMOWANIA

- 1.17.1 Dla wszystkich aplikacji użytkowanych w Spółce właściwy Administrator prowadzi rejestr licencji zawierający:
- a. Nośniki instalacyjne,
  - b. zbiór licencji oraz informacja o okresie ważności,
  - c. dowód zakupu licencjonowanego oprogramowania,
  - d. urządzenie komputerowe, na którym użytkowane jest licencjonowane oprogramowanie,
  - e. informacje o Użytkowniku.

- 1.17.2 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.
- 1.17.3 Użytkownik jest zobowiązany do stosowania się do wszelkich zaleceń przekazywanych przez CUW ICT związanych z użytkowaniem przez niego oprogramowaniem.
- 1.17.4 Okresowo, nie rzadziej niż raz w roku, lokalne urządzenia komputerowe oraz serwery są sprawdzane przez Administratora Technicznego, w szczególności pod kątem obecności nieautoryzowanego oprogramowania.
- 1.17.5 Czynnikiem do podjęcia kontroli na żądanie jest:
  - a. informacja o popełnieniu lub podejrzeniu popełnienia czynu niedozwolonego przez Użytkownika,
  - b. otrzymanie zgłoszenia od Użytkownika o pojawieniu się lub podejrzeniu pojawienia się w Spółce nieautoryzowanego oprogramowania.
- 1.17.6 Do przeprowadzenia kontroli oprogramowania dopuszczane jest stosowanie narzędzi programowych umożliwiających automatyczne sprawdzanie urządzeń komputerowych.
- 1.17.7 Nieautoryzowane oprogramowanie jest niezwłocznie usuwane przez odpowiedniego Administratora Technicznego, który zgłasza wystąpienie Incydentu Bezpieczeństwa zgodnie z PROC 55001/A Procedurą Zarządzania Incydentami Bezpieczeństwa Teleinformatycznego w PGE Systemy S.A. do Konsultanta Service Desk.
- 1.17.8 Użytkownicy mają prawo do eksploatacji programów bezpłatnych (freeware, public domain, open source itp.) dopuszczonych do stosowania w Spółce. Lista oprogramowania utrzymywana jest przez CUW ICT.
- 1.17.9 W celu uzyskania zgody na eksploatację programu bezpłatnego, którego nie ma na liście dozwolonego oprogramowania w Spółce, należy dokonać jego legalizacji kierując do CUW ICT Wniosek o legalizację oprogramowania..

#### **1.18 SZYFROWANIE DANYCH**

- 1.18.1 W celu zapewnienia odpowiedniego poziomu bezpieczeństwa oraz Poufności danych przetwarzanych w Spółce na lokalnych urządzeniach komputerowych Użytkowników wykorzystuje się oprogramowanie szyfrujące.
- 1.18.2 Oprogramowanie szyfrujące umożliwia bezpieczne szyfrowanie całych dysków, pojedynczych partycji lub tworzenia wirtualnych wolumenów. Dostęp do zaszyfrowanych danych (odczyt, zmiana) jest wówczas możliwy jedynie po wprowadzeniu Hasła. Wprowadzenie Hasła, którym zostały zabezpieczone dane, umożliwia normalną pracę na danym dysku lub wolumenie, tak jakby był to każdy inny dysk dostępny w systemie.
- 1.18.3 Przyjmuje się, iż stosowanie niniejszego oprogramowania jest obligatoryjne w przypadku przenośnych urządzeń komputerowych (laptopów). Natomiast w pozostałych przypadkach nie jest obowiązkowe i może zostać zastosowane na Wniosek Właściciela Zasobu.
- 1.18.4 Użytkownicy uprawnieni są do wykorzystywania mechanizmów kryptograficznych oferowanych przez oprogramowanie dopuszczone do eksploatacji przez CUW ICT. Lista dopuszczonych mechanizmów kryptograficznych jest dostępna w CUW ICT.

#### **1.19 TRANSPORT DANYCH NA NOŚNIKACH PRZENOŚNYCH**

- 1.19.1 Zaleca się wykorzystanie Nośników szyfrowanych sprzętowo. Podczas przenoszenia danych na wyżej wymienionych Nośnikach, Pracownik nie musi wykorzystywać oprogramowania szyfrującego.

#### **1.20 AUTORYZACJA I WYKORZYSTANIE ŚRODKÓW PRZETWARZANIA INFORMACJI**

- 1.20.1 Systemy Teleinformatyczne wykorzystywane w Spółce mogą być przeznaczone tylko i wyłącznie do realizacji zadań służbowych.
- 1.20.2 Systemy Teleinformatyczne wykorzystywane w Spółce podlegają inwentaryzacji i autoryzacji (dopuszczenie do pracy w Spółce).
- 1.20.3 Wykorzystywanie środków do Przetwarzania informacji, będących własnością Spółki, w celach służbowych niezwiązanych z powierzonymi obowiązkami wymaga uzgodnienia z bezpośrednim Przełożonym i jeżeli zachodzi taka potrzeba wynikająca z zakresu, ewentualnego wykorzystania urządzeń z Właścicielem Zasobu.
- 1.20.4 Zabrania się podłączania do Sieci Korporacyjnej jakichkolwiek urządzeń nieposiadających autoryzacji. Wyjątek stanowi dedykowana sieć dla gości Spółki.
- 1.20.5 Użytkownicy nie mogą samodzielnie dokonywać jakiejkolwiek zmiany konfiguracji środków Przetwarzania informacji chyba, że Użytkownik jest Administratorem Technicznym.



## 1.21 ZASADY PRACY W SIECI KORPORACYJNEJ

- 1.21.1 Instalacji oraz aktualizacji oprogramowania systemowego i aplikacji dokonuje wyłącznie Administrator Techniczny lub osoby upoważnione przez Właściciela Zasobu.
- 1.21.2 Użytkownikom zabrania się:
- a. podejmować prób wykorzystania obcych Identyfikatorów Użytkownika, i uruchamiania aplikacji deszyfrujących (łamiących) Hasła chyba, że Użytkownik jest Administratorem Technicznym lub osobą upoważnioną przez Właściciela Zasobu, i prowadzi te działania w celu zapewnienia ochrony informacji (np. testowanie zabezpieczeń) przetwarzanych w Spółce,
  - b. prowadzenia działań mających na celu nieautoryzowany dostęp do informacji przetwarzanych w zasobach Spółki lub podsłuchiwanie czy przechwytywanie informacji przepływających w Sieci Korporacyjnej chyba, że Użytkownik jest Administratorem Technicznym lub osobą upoważnioną przez Właściciela Zasobu i prowadzi te działania w celu zapewnienia ochrony informacji (np. testowanie zabezpieczeń) przetwarzanych w zasobach Spółki,
  - c. udostępniać osobom postronnym informacji na temat struktury technicznej Sieci Korporacyjnej (w tym adresacji sieci, struktur aplikacji, baz danych itp.) bez zgody Właściciela Zasobu,
  - d. samodzielnej instalacji oprogramowania systemowego i aplikacji chyba, że Użytkownik jest Administratorem Technicznym lub osobą upoważnioną przez Właściciela Zasobu,
  - e. uruchamiania aplikacji i programów, które mogą zakłócić i destabilizować pracę Sieci Korporacyjnej, bądź naruszyć bezpieczeństwo danych w niej przetwarzanych.
- 1.21.3 W przypadku zakończenia pracy lub odejścia od stanowiska pracy każdorazowo należy stosować zasadę czystego biurka i ekranu. Zasada czystego biurka polega na zabezpieczeniu wszelkich dokumentów oraz Nośników informacji podlegających ochronie znajdujących się na stanowisku pracy, w sytuacji kiedy nawet na krótki okres czasu tracimy nad nimi kontrolę. Niepotrzebne w danej chwili dokumenty oraz Nośniki informacji należy zabezpieczyć.
- 1.21.4 Zasada czystego ekranu odnosi się do stacji roboczych, urządzeń przenośnych oraz serwerów. Polega na zastosowaniu zabezpieczenia przed nieupoważnionym użyciem urządzenia komputerowego pozostawionego bez opieki.
- 1.21.5 W przypadku stacji roboczej przenośnej Użytkownik jest zobowiązany do zabezpieczenia jej przed kradzieżą, np. poprzez stosowanie linek zabezpieczających.
- 1.21.6 Na Użytkowniku spoczywa obowiązek zabezpieczenia danych (plików) opracowywanych bądź tworzonych na lokalnych lub przenośnych urządzeniach komputerowych (komputery typu PC lub laptopy). Również wszelkie dane źródłowe (pliki), na których Użytkownik wykonuje operacje, winny być zabezpieczone przed utratą i nieautoryzowanym użyciem bądź modyfikacją.
- 1.21.7 Użytkownik ma następujące możliwości zabezpieczenia danych (plików):
- a. sporządzenie kopii zapasowej na wymiennym Nośniku,
  - b. umieszczenie danych w zasobach sieciowych (niezgodnie z polityką jest umieszczanie ich na serwerze prywatnych danych).
- 1.21.8 Użytkownik wykonujący wydruki, które zawierają informacje podlegające ochronie (dane osobowe, tajemnica przedsiębiorstwa itp.) jest odpowiedzialny za zachowanie szczególnej ostrożności, a zwłaszcza za zabezpieczenie ich przed dostępem przez osoby nieupoważnione.
- 1.21.9 Wydruki przeznaczone do usunięcia, należy zniszczyć w sposób trwały, bezwzględnie uniemożliwiający w jakikolwiek sposób ich odtworzenie.

## 1.22 ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

- 1.22.1 Użytkownik zobowiązany jest do okresowej weryfikacji poprawności danych znajdujących się w stopce. W przypadku stwierdzenia nieprawidłowości w podpisie jest on zobowiązany do niezwłocznego powiadomienia o tym Administratora Technicznego systemu poczty elektronicznej, który odpowiada za prawidłowość oraz autentyczność danych znajdujących się w stopce wiadomości oraz zobowiązany jest do ich bieżącej aktualizacji.
- 1.22.2 Użytkownik przysyłając informacje za pośrednictwem poczty elektronicznej ponosi odpowiedzialność za prawidłowe zaadresowanie wiadomości elektronicznej i przesłanie jej do uprawnionego odbiorcy.



- 1.22.3 Zabrania się przesyłania za pośrednictwem poczty elektronicznej treści niezgodnych z obowiązującymi przepisami prawa, naruszających zasady współżycia społecznego oraz naruszających prawa własności intelektualnej innych osób.
- 1.22.4 Zabrania się przesyłania do innych 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.
- 1.22.5 Zabrania się rozsyłania za pośrednictwem poczty elektronicznej załączników zawierających pliki zagrażające lub mogące zagrażać bezpieczeństwu Systemu Teleinformatycznego Spółki.
- 1.22.6 Zabrania się wykorzystywania przydzielonego Użytkownikowi Korporacyjnego Konta pocztowego do celów prywatnych (np. prowadzenie korespondencji nie związanej z działalnością służbową, rejestrowania się przy użyciu Konta Korporacyjnego na forach, portalach społecznościowych, itp.).
- 1.22.7 Zabrania się przekierowywania poczty służbowej na prywatną skrzynkę (np. w celu pracy w domu). W tym celu udostępnia się użytkownikom usługę zdalnego logowania się do poczty korporacyjnej lub dostępu zdalnego do Sieci Korporacyjnej.
- 1.22.8 Wiadomości przesyłane pocztą elektroniczną zawierające informacje chronione poza Sieć Korporacyjną należy zabezpieczyć Hasłem o długości zależnej od rodzaju ochrony do którego informacja została zaklasyfikowana.
- 1.22.9 Z zabezpieczania Hasłem, o którym mowa w pkt 6.22.8 są zwolnione wiadomości, jeśli korespondencja jest szyfrowana przy pomocy infrastruktury klucza publicznego PKI.
- 1.22.10 Informacje przesyłane pocztą elektroniczną mogą podlegać kontroli. Udzielenie informacji o treści korespondencji Użytkownika odbywa się na piśmie Wniosek złożony do CUW ICT przez Członka Zarządu Spółki lub przez osobę przez niego upoważnioną.
- 1.22.11 Korespondencja w formie elektronicznej wysyłana ze służbowego adresu jest własnością Spółki.
- 1.22.12 System poczty elektronicznej podlega ochronie antywirusowej i wszystkie wiadomości są sprawdzane pod kątem obecności szkodliwego oprogramowania. Wiadomości, z których nie można usunąć szkodliwego oprogramowania nie będą dostarczane adresatowi.
- 1.22.13 W przypadku otrzymania wiadomości zawierającej podejrzane załączniki Użytkownik zobowiązany jest:
  - a. nie otwierać załączników,
  - b. usunąć daną wiadomość (również z folderu zawierającego wiadomości usunięte).

### 1.23 ZASADY KORZYSTANIA Z SIECI INTERNET

- 1.23.1 Użytkownik ma prawo korzystać z sieci Internet wyłącznie:
  - a. w celach związanych z realizacją zadań służbowych,
  - b. zgodnie z obowiązującymi regulaminami wewnętrznymi Spółki i przepisami prawa,
  - c. w zakresie przyznanych uprawnień.
- 1.23.2 Użytkownikowi zabronione jest korzystanie z sieci Internet w celu:
  - a. uzyskania nieuprawnionego dostępu do Zasobów Spółki będących własnością Spółki lub Zasobów 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 naruszających w jakikolwiek inny sposób prawa innych osób.
- 1.23.3 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.
- 1.23.4 Dozwolone są następujące protokoły dostępu do sieci Internet (przy zachowaniu standardowych portów): http, https. Korzystanie z innych protokołów odbywa się na zasadach zawartych w PROG 00044 Procedura Ogólna zarządzania dostępem do sieci Internet.
- 1.23.5 Wykorzystanie Internetu przez Użytkownika jest kontrolowane, w szczególności adresy stron www przeglądane przez Użytkownika.

### 1.24 ZASADY KORZYSTANIA Z SYSTEMÓW KOMUNIKACJI GŁOSOWEJ I FAKSOWEJ



- 1.24.1 Użytkownicy obowiązani są do przestrzegania zakazu prowadzenia rozmów telefonicznych, podczas których może dochodzić do wymiany informacji chronionych, jeśli rozmowy te odbywają się w miejscach publicznych (np. pociągach, poczekalniach) oraz takich, które nie gwarantują zachowania Poufności rozmów.
- 1.24.2 Użytkownikom zabrania się zapisywania w systemach poczty głosowej informacji wrażliwych (tzn. takich, które są istotne dla Spółki i są w Spółce klasyfikowane jako chronione bądź ściśle chronione).
- 1.24.3 Odczytanie wiadomości z faksów, automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego Hasła.
- 1.24.4 W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.
- 1.24.5 Przekazywanie za pomocą urządzeń faksowych dokumentów zawierających informacje sklasyfikowane jako ściśle chronione lub chronione jest zabronione.

#### **1.25 BEZPIECZEŃSTWO TRANSMISJI DANYCH**

- 1.25.1 Każdy Użytkownik użytkujący komputer służbowy lub inne urządzenie mobilne, zobowiązany jest do przestrzegania następujących wytycznych w przypadku korzystania z:
  - 1.25.1.1 Bezprzewodowych punktów dostępowych (Wi-Fi, Bluetooth):
    - a. zabrania się Użytkownikom uruchamiania punktów dostępowych na terenie wszystkich Jednostek organizacyjnych Spółki,
    - b. 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).
  - 1.25.1.2 Połączeń wdzwanianych:
    - a. zabrania się korzystania z połączeń wdzwanianych (poprzez modemy) Użytkownikom podłączonym do Sieci Korporacyjnej,
    - b. zabrania się budowania dostępow wdzwanianych do Systemów Teleinformatycznych udostępniających Zasoby Spółki (serwery, urządzenia aktywne, stacje robocze, itp.).
  - 1.25.1.3 Łączny internetowych:
    - a. zabrania się łączenia z Internetem z urządzeń (stacji roboczych, komputerów przenośnych) podłączonych do Sieci Korporacyjnej poprzez łącza GPRS, WiFi, Bluetooth, modem, itp.,
    - b. zabrania się budowania punktów dostępowych do Internetu.
- 1.25.2 W przypadku działań Osób Trzecich odpowiedzialność za prawidłowość tych działań spoczywa na danym Opiekunie Osoby Trzeciej.

#### **1.26 STANDARDY STACJI ROBOCZYCH ORAZ OPROGRAMOWANIA**

- 1.26.1 W Spółkach wprowadzono standardy stacji roboczych oraz oprogramowania instalowanego na urządzeniu komputerowym.
- 1.26.2 Parametry techniczne standardów stacji roboczych oraz oprogramowania zainstalowanego na nich określają szczegółowo umowy SLA zawierane na te usługi z CUW ICT.

#### **1.27 POSTANOWIENIA KOŃCOWE**

- 1.27.1 Odstępstwa od procedury w zakresie punktu 6.11 akceptuje Dyrektor Departamentu Strategii IT lub Dyrektor Departamentu Bezpieczeństwa i Ciągłości Biznesowej w PGE Systemy S.A.