Spis treści

1. Cel dokumentu

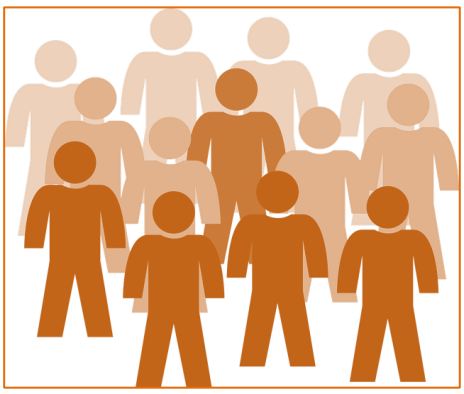
Celem dokumentu jest wskazanie Wykonawcom współpracującym z Polską Spółką Gazownictwa sp. z o.o. zasad, wytycznych i dobrych praktyk w obszarze bezpieczeństwa informacji, których stosowanie jest w interesie obu Stron. Efektem ma być zapewnienie, że wymagania Spółki co do bezpieczeństwa informacji są Wykonawcom znane i przez nich stosowane. Wykonawcy świadczący usługi na rzecz i na terenie Spółki muszą działać zgodnie z mającymi zastosowanie przepisami prawa oraz regulacjami wewnętrznymi Spółki w zakresie ochrony informacji sklasyfikowanych jako ważne, wrażliwe i cenne dla PSG

2. Zakres

Dokument określa zasady, wytyczne i dobre praktyki związane z bezpieczeństwem informacji w codziennej współpracy Wykonawcy ze Spółką PSG.

3. Wykonawcy poruszający się po obiektach PSG.

Zasady



Pracownik Wykonawcy może poruszać się samodzielnie jedynie w **strefie ogólnodostępnej** – we wszystkich ogólnodostępnych miejscach należących do Spółki, ogólnodostępnych parkingach, recepcji oraz holach i innych miejscach, gdzie ruch osobowy i kołowy nie jest ewidencjonowany.

Poruszanie się na terenie obiektu podlega ewidencji i możliwe jest po zarejestrowaniu pracownika Wykonawcy przez Opiekuna i wydaniu mu:

a. osobistej karty identyfikacyjnej dla SERWISU,
b. osobistej karty identyfikacyjnej dla GOŚCIA.

Wykonawca może poruszać się:

a. **w strefie administracyjnej** w obecności pracowników uprawnionych do pracy i przebywania w strefie, z wyjątkiem serwisu sprzątającego i planowanych prac serwisowych wykonywanych pod nadzorem Ochrony Obiektu,
b. **w strefie chronionej** tylko w obecności pracowników uprawnionych do pracy i przebywania w strefie, bez względu na charakter dostępu (sprzątanie, serwis, awaria).

Po zakończeniu prac należy niezwłocznie opuścić obiekt i wyrejestrować się u Opiekuna/Pracownika Ochrony Obiektu.

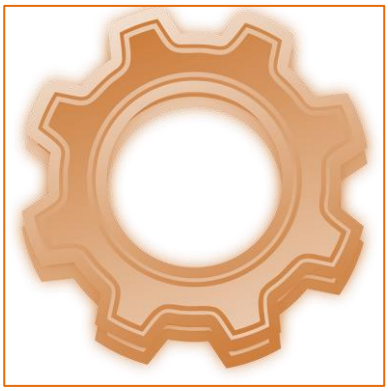
W przypadku utraty, zniszczenia karty identyfikacyjnej Wykonawca musi zgłosić ten fakt bezzwłocznie swojemu Opiekunowi.

Zabrania się:

a. udostępniania osobistej karty identyfikacyjnej innej osobie,
b. poruszania się po pomieszczeniach strefy administracyjnej i chronionej bez nadzoru Opiekuna/ pracownika Ochrony Obiektu,
c. prób wejścia do pomieszczeń niezwiązanych z realizowaną usługą, nawet jeżeli nie byłyby one chronione kontrolą dostępu czy zamknięte na klucz.

4. Przetwarzanie informacji udostępnionych przez Spółkę.

Zasady



Wszystkie przekazane Wykonawcy informacje (w formie papierowej, elektronicznej, ustnej etc.) muszą być przez niego traktowane bezwzględnie jako tajemnica przedsiębiorstwa PSG i podlegać szczególnej ochronie. Wykonawca zobowiązany jest, w trakcie realizacji zlecenia, do stosowania następujących zasad:

a. przy przetwarzaniu udostępnionych lub powierzonych informacji, należy szczególnie zadbać o zachowanie poufności, integralności i dostępności tych informacji,
b. informacje zapisane na nośnikach danych należy przekazywać z zastosowaniem protokołu zdawczo-odbiorczego,
c. na etapie rozpoczęcia współpracy z podmiotem zewnętrznym (np. realizacja umowy) należy ustalić sposób szyfrowania plików elektronicznych, które mają być przesyłane przy wykorzystaniu do tego celu usługi poczty elektronicznej. Dotyczy to także innych przesyłanych w ten sposób informacji, które w ocenie Zamawiającego mogą zawierać informacje poufne,
d. zbędne wydruki, notatki, kserokopie dokumentów itp. zawierające informacje należące do PSG muszą być bezwzględnie niszczone w sposób uniemożliwiający odtworzenie ich

treści. Za skuteczne zniszczenie tych dokumentów odpowiedzialna jest osoba, która do chwili ustania ich użyteczności odpowiedzialna była za jego przechowywanie,

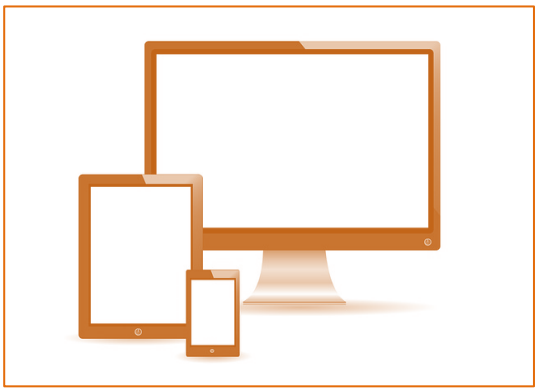
e. wydruki zawierające dane należące do PSG po zakończeniu pracy muszą być przechowywane w zamkniętych szafach, bez dostępu do nich osób nieupoważnionych.

Zabrania się:

a. przekazywania nośników informacji zawierających dane PSG podwykonawcom współpracującym z Wykonawcami bez umowy zachowania poufności,
b. pozostawiania bez dozoru lub udostępniania osobom nieupoważnionym informacji (w formie elektronicznej, papierowej itp.) przekazanych przez Spółkę,
c. przekazywania informacji, należących do Spółki, pozyskanych lub zauważonych podczas realizacji zadań, osobom lub podmiotom, nieuprawnionym do ich pozyskania.

5. Wykonawcy korzystający ze sprzętu komputerowego

Zasady



Wykonawcy korzystający ze sprzętu komputerowego (komputery, urządzenia mobilne, telefony etc.) zobowiązani są do:

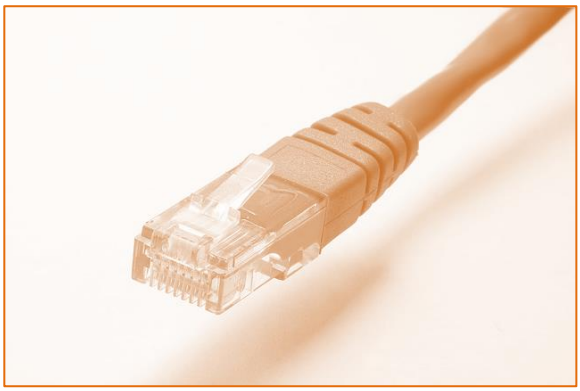
a. używania tylko legalnego oprogramowania,
b. używania oprogramowania antywirusowego z aktualną bazą wirusów,
c. stosowania silnych haseł,
d. natychmiastowej zmiany hasła, jeśli istnieje podejrzenie, że zostało odkryte lub wiadomo, że znajduje się ono w posiadaniu osoby innej niż Wykonawca,
e. ustawienia monitorów stanowisk z dostępem do danych udostępnianych przez PSG (w pomieszczeniach, gdzie przebywają osoby postronne) w taki sposób, żeby uniemożliwić tym osobom wgląd w dane,
f. zabezpieczenia dostępu do systemu informatycznego przed dostępem osób nieuprawnionych (zablokowanie ekranu lub wylogowanie się z systemu), w przypadkach chwilowego opuszczenia stanowiska pracy,
g. wykorzystywania urządzeń mobilnych do transmisji informacji wrażliwych, wyłącznie wtedy, gdy przekaz jest szyfrowany,
h. wykorzystywania sieciowych technologii bezprzewodowych do transmisji informacji wrażliwych, wyłącznie wtedy, gdy przekaz jest szyfrowany,
i. wylogowania się z systemu informatycznego natychmiast po zakończeniu pracy w tym systemie.

Zabrania się:

a. przesyłania danych z systemu informatycznego osobom nieuprawnionym do odbioru takich danych,
b. logowania się z wykorzystaniem identyfikatora i hasła osoby trzeciej,
c. udostępniania identyfikatora i hasła osobom trzecim,
d. informowania o infrastrukturze informatycznej Spółki, stosowanych zabezpieczeniach, wykorzystywanych systemach informatycznych osób trzecich, niezwiązanych z realizacją usługi,
e. stosowania oprogramowania z naruszeniem warunków stosownej licencji,
f. testowania lub podejmowania prób poznania metod zabezpieczenia sieci i systemów informatycznych PSG,
g. podejmowania prób obejścia zabezpieczeń systemów informatycznych.

6. Dostęp Wykonawców do sieci i systemów informatycznych Spółki

Zasady



Dostęp do sieci i systemów informatycznych PSG jest możliwy wyłącznie po autoryzacji Pracownika IT Spółki. Podłączany sprzęt musi mieć zainstalowane aktualne oprogramowanie antywirusowe oraz dostęp do zasobów ograniczony do niezbędnego minimum.

Stosuje się:

a. dostęp z obiektów Spółki po autoryzacji w domenie,
b. dostęp z zewnątrz z wykorzystaniem rozwiązań typu VPN.

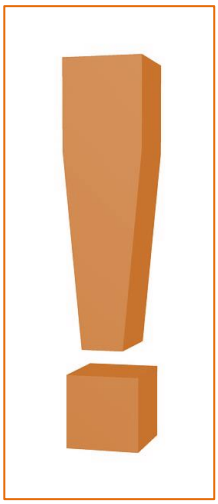
Korzystanie z systemów informatycznych PSG jest możliwe na następujących zasadach:

a. Wykonawca jest jednoznacznie zidentyfikowany przez system jako osoba fizyczna, posiada swój unikalny, nadany przez Pracownika IT identyfikator,
b. w przypadku zdalnego dostępu do systemów informatycznych PSG uwierzytelnianie odbywa się z wykorzystaniem certyfikatu wystawionego przez PSG CA,
c. zdalna obsługa może być prowadzona jedynie z wykorzystaniem urządzeń, które posiadają aktualne zabezpieczenia antywirusowe oraz zainstalowane niezbędne łatki/ aktualizacje bezpieczeństwa,
d. w przypadku zakończenie świadczenia usługi Wykonawca zobowiązany jest bezzwłocznie zaprzestać korzystania z posiadanych dostępów.

Zabrania się:

a. niezgodnych z ustalonymi procedurami, nienadzorowanych prób łączenia z bezprzewodową siecią korporacyjną, o ile nie jest to bezwzględnie wymagane do realizacji umowy
b. samodzielnego wpinania urządzeń do sieci informatycznej,
c. dla urządzeń komputerowych pracujących w sieci LAN zestawiania innych połączeń niż połączenia autoryzowane przez PSG,
d. testowania lub podejmowania prób poznania metod zabezpieczenia sieci i systemów informatycznych PSG,
e. obchodzenia zabezpieczeń systemów informatycznych .
f. skanowania sieci teleinformatycznej PSG

7. Incydenty



Zasady

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie bezpieczeństwa informacji Wykonawca jest zobowiązany bezzwłocznie powiadomić osobę wyznaczoną do współpracy, Opiekuna lub pracownika Ochrony Obiektu o zaistniałej sytuacji.

Jeżeli Wykonawca zauważy:

a. obce osoby bez identyfikatora, poruszające się bez opieki,
b. pozostawione dokumenty, w szczególności z oznaczeniem poufne lub tajne,
c. korzystanie z obcego identyfikatora lub hasła,
d. niezamknięte, pozostawione bez opieki pomieszczenia,
e. niezablokowany komputer z dostępem do systemów informatycznych,
f. wykorzystywanie zdalnego połączenia VPN przez osoby nieupoważnione,
g. inne zdarzenia, które wg własnej oceny stanowią zagrożenie dla bezpieczeństwa, bezpieczeństwa informacji,

bezzwłocznie zgłasza je do osób pod opieką których przebywa w trakcie realizacji zadań dla PSG Sp. z o.o.

Ważne.

Incydenty wynikające z działań pracownika Wykonawcy związane z:

a. nieuprawnionym dostępem do systemu informatycznego PSG,
b. łamaniem haseł,
c. deszyfracją plików,
d. nieautoryzowanymi próbami łamania zabezpieczeń,
e. prób wejścia do pomieszczeń niezwiązanych z realizowaną usługą,
f. udostępniania osobistej karty identyfikacyjnej, identyfikatora i hasła osobie trzeciej

będą uważane za ciężkie naruszenie obowiązującej umowy ze Spółką PSG.

8. Dostarczanie oprogramowania dla PSG

Oprogramowanie (systemy teleinformatyczne) dostarczane dla PSG musi być zgodne z obowiązującymi w Spółce Zasadami Bezpieczeństwa Teleinformatycznego. W szczególności oprogramowanie musi korzystać wyłącznie z szyfrowanych kanałów komunikacji.