



Załącznik nr 2

do Polityki Systemu Zarządzania Bezpieczeństwem w Grupie TAURON

Podstawowe wymagania bezpieczeństwa obowiązujące w Grupie TAURON dla Współpracowników

Spis treści

1	Wstęp.....	3
1.2	Cel dokumentu	3
1.3	Zakres stosowania	3
1.4	Definicje.....	3
2	Wymagania dla Współpracowników	4
2.1	Angażowanie podwykonawców.....	4
2.2	Przebywanie i praca na terenie Spółki Grupy TAURON.....	4
2.3	Bezpieczeństwo i przetwarzanie informacji w ramach świadczonych usług.....	6
2.3.1	Dokumentowanie zasad przetwarzania informacji w zapisach umownych	6
2.3.2	Klasyfikacja informacji w Grupie TAURON	6
2.4	Bezpieczeństwo IT w ramach świadczonych usług dla Grupy TAURON.....	8
2.4.2	Dostęp Współpracownika do sieci i systemów informatycznych Spółki Grupy TAURON.....	9
2.4.3	Monitorowanie działań użytkowników systemów IT	10
2.5	Incydenty bezpieczeństwa.....	10

1 Wstęp

1. Niniejsze Podstawowe wymagania bezpieczeństwa obowiązujące w Grupie TAURON dla Współpracowników (zwane dalej: Wymagania) zawierają zbiór podstawowych wymagań wynikających z wewnętrznych i wewnątrzkorporacyjnych regulacji obowiązujących w Grupie TAURON.
2. Wymagania obejmują podstawowe zasady bezpieczeństwa przetwarzania informacji, korzystania z systemów informatycznych oraz zasady bezpieczeństwa fizycznego, których należy przestrzegać w ramach realizowanych umów zawartych ze Spółkami Grupy TAURON. Nie wyczerpują one wszystkich zagadnień, a stanowią uzupełnienie zasad wynikających z przepisów prawa powszechnie obowiązującego oraz zawartych umów ze Spółkami Grupy TAURON, standardów bezpieczeństwa i dobrych praktyk.

1.2 Cel dokumentu

Celem dokumentu jest wskazanie Współpracownikom zasad, wymagań w zakresie bezpieczeństwa przetwarzania informacji, korzystania z systemów informatycznych oraz zasad bezpieczeństwa fizycznego, obowiązujących w Spółkach i obiektach Grupy TAURON.

Celem dokumentu jest zaznajomienie Współpracowników z wymaganiami Grupy TAURON co do bezpieczeństwa oraz ich stosowania.

1.3 Zakres stosowania

Wymagania powinny być wykorzystywane jako załącznik do umów, wszędzie tam, gdzie w ocenie Spółki Grupy TAURON istnieje konieczność przekazania Współpracownikowi tych Wymagań, z uwagi na charakter świadczonej pracy.

1.4 Definicje

1. **Grupa TAURON** - TAURON Polska Energia S.A., jej następcy prawni oraz wszelkie spółki zależne, dominujące lub powiązane z TAURON Polska Energia S.A., w rozumieniu stosowanych przez TAURON przepisów o rachunkowości).

2. **Opiekun umowy** - osoba wskazana przez Spółkę Grupy TAURON do nadzorowania pracy i kontaktów roboczych ze Współpracownikiem.
3. **Spółka Grupy TAURON** - Spółka będąca członkiem Grupy TAURON, zlecniodawca dla Współpracownika,
4. **Współpracownik** - osoba fizyczna lub prawna realizująca prace na rzecz Spółki Grupy TAURON, na podstawie umowy innej niż umowa o pracę, bądź na podstawie innego stosunku prawnego będącego podstawą współpracy Spółki ze Współpracownikiem, z wyłączeniem Członka Zarządu Spółki zatrudnionego niepracowniczo oraz osób zatrudnionych w Spółkach Grupy TAURON, w tym także pracownicy lub współpracownicy kontrahentów Spółki Grupy TAURON będących osobami prawnymi albo jednostkami organizacyjnymi nieposiadającymi osobowości prawnej, realizujący prace bądź usługi na rzecz Spółki Grupy TAURON.
5. **Zasady bezpieczeństwa fizycznego** - reguły postępowania obowiązujące Współpracowników mające na celu zapewnienie bezpieczeństwa zasobów Spółki, wynikające z przepisów prawa powszechnie obowiązującego, w tym także z przepisów BHP i ochrony p.poż., a także przepisów ochrony osób i mienia, regulacji wewnętrznych i wewnątrzkorporacyjnych, a także dobrych praktyk i pragmatyki działania ochrony fizycznej, których przestrzeganie jest wymagane od Współpracowników w trakcie wykonywania zleconych prac

2 Wymagania dla Współpracowników

2.1 Angażowanie podwykonawców

W przypadku zaangażowania podwykonawców, jeżeli zezwala na to umowa ze Spółką Grupy TAURON, Współpracownik działający na rzecz Spółki Grupy TAURON zobowiązany jest zapewnić w umowach w podwykonawcę co najmniej równoważny poziom bezpieczeństwa określony w niniejszych Wymaganiach oraz postanowieniach umownych dotyczących zleconej pracy.

2.2 Przebywanie i praca na terenie Spółki Grupy TAURON

1. Współpracownik jest zobowiązany do przestrzegania zasad dotyczących organizacji ruchu osobowego, ruchu pojazdów i ruchu materiałowego obowiązujących na terenie Spółki, na którym Współpracownik realizuje zadania wynikające z umowy.

2. Współpracownik zobowiązany jest do uzgodnienia z Opiekunem umowy kwestii Zasad bezpieczeństwa fizycznego, obowiązujących na terenie Spółki Grupy TAURON, w której realizowany jest przedmiot umowy.
3. Zasady bezpieczeństwa fizycznego zobowiązują Współpracownika m.in. do:
 - 1) wejścia, wyjścia i przebywania na terenie Spółki Grupy TAURON zgodnie z obowiązującymi w Spółce regulacjami w tym zakresie,
 - 2) poruszania się i przebywania Współpracownika na terenie Spółki Grupy TAURON zgodnie z nadanymi uprawnieniami, a także, jeżeli jest to konieczne – w asyście Opiekuna umowy,
 - 3) pracy wyłącznie w asyście Opiekuna umowy lub innej osoby przez niego wyznaczonej, we wskazanych pomieszczeniach, jeżeli tak zostało ustalone.
4. W przypadku konieczności odstępstwa od przyjętych Zasad bezpieczeństwa fizycznego Współpracownik powinien zwrócić się do Opiekuna umowy, w celu uzyskania formalnej akceptacji.
5. Współpracownikowi zabrania się m.in.:
 - 1) udostępniania poświadczeń (tj. przepustek, kart dostępowych, kodów PIN, itp.) uprawniających do wejścia na teren Spółki Grupy TAURON, do stref ochrony, do obiektów i pomieszczeń innej osobie lub umożliwienia dostępu do tych poświadczeń osobom nieuprawnionym,
 - 2) wejścia do stref ochrony lub pomieszczeń, do których Współpracownik nie posiada uprawnień,
 - 3) wynoszenia, wywożenia mienia z terenu Spółki Grupy TAURON niebędącego własnością Współpracownika, bez stosownego zezwolenia,
 - 4) wnoszenia, wwożenia mienia na teren Spółki Grupy TAURON przez Współpracownika, bez stosownego zezwolenia.
6. W przypadku naruszenia przez Współpracownika Zasad bezpieczeństwa fizycznego Spółka Grupy TAURON może zastosować bezpośrednio w stosunku do naruszającego, następujące sankcje:
 - 1) odebranie uprawnień do wejścia i przebywania na terenie Spółki Grupy TAURON,
 - 2) nadanie statusu „Persona non grata” na czas określony lub bezterminowo,a także obciążyć Współpracownika będącego stroną umowy, karami umownymi, stosownie do zapisów w łączącej strony umowie.

2.3 Bezpieczeństwo i przetwarzanie informacji w ramach świadczonych usług

2.3.1 Dokumentowanie zasad przetwarzania informacji w zapisach umownych

Zapisy niniejszego rozdziału określają podstawowe Wymagania w zakresie przetwarzania informacji w Grupie TAURON, które Współpracownik zobowiązany jest stosować z uwzględnieniem bardziej szczegółowych postanowień umownych, jeżeli takowe zostały w umowie zapisane.

2.3.2 Klasyfikacja informacji w Grupie TAURON

1. Informacje, które Współpracownik przetwarza w związku z realizacją umowy, podlegają klasyfikacji bezpieczeństwa oraz oznaczaniu ze względu na poufność. Jeżeli zapisy umowne nie stanowią inaczej, należy stosować się do poniższych zasad klasyfikacji i oznaczania informacji.
2. Przetwarzana informacja może zostać oznaczona przez Spółkę w sposób przedstawiony w tabeli:

Klasyfikacja w zakresie poufności	Oznaczenie Informacji	Charakterystyka Informacji
	Informacja Ściśle Chroniona <i>lub skrót (IS)</i>	Informacje m.in. operacyjne, strategiczne, organizacyjne, finansowe, itp., które nie powinny być przekazywane osobie lub osobom innym niż wskazane w dokumencie, zidentyfikowane jako odbiorcy danej informacji lub wskazanych w dedykowanej procedurze udostępniania. Ujawnienie spowoduje lub może spowodować bardzo poważne szkody dla Spółki/całej Grupy TAURON, Współpracowników, stron trzecich oraz relacji z nimi.
	Informacja Chroniona <i>lub skrót (IC)</i>	Informacje m.in. operacyjne, strategiczne, organizacyjne, finansowe, itp. jakie powinny być przekazywane wyłącznie za zgodą i wiedzą właściciela informacji. Ujawnienie spowoduje lub może powodować poważne szkody dla Spółki/całej Grupy TAURON, Współpracowników, stron trzecich oraz relacji z nimi.
	Informacja Wewnętrzna	Informacje operacyjne, organizacyjne, finansowe itp. (wewnętrzne), które powinny być chronione jasnymi zasadami przekazywania i udostępniania bez konieczności ścisłego nadzoru nad obiegiem danej informacji. Ujawnienie spowoduje lub może powodować poważne

Załącznik nr 2 do Polityki Systemu Zarządzania Bezpieczeństwem w Grupie TAURON – Podstawowe wymagania bezpieczeństwa obowiązujące w Grupie TAURON dla Współpracowników

<i>lub skrót (IW) lub brak oznaczeń</i>	szkody dla Spółki/całej Grupy TAURON, Współpracowników, stron trzecich oraz relacji z nimi.
Informacja powszechna <i>brak oznaczeń</i>	Informacje publiczne, powszechnie znane lub upublicznione przez Spółkę lub tworzone jako takie, których upublicznienie nie spowoduje żadnej szkody.

3. Wszystkie informacje zaklasyfikowane i oznaczone jako Informacja Chroniona i Informacja Ściśle Chroniona stanowią tajemnicę przedsiębiorstwa Spółki Grupy TAURON (w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji) i podlegają ochronie prawnej.
4. Współpracownik powinien ustalić z Opiekunem umowy praktyczne zasady stosowania klasyfikacji, oznaczania i przetwarzania informacji, które są przedmiotem umowy.
5. W zakresie przetwarzania informacji, jeżeli zapisy umowne nie stanowią inaczej, należy stosować się co najmniej do poniższych zasad:

ZASADY	ZABRANIA SIĘ
<p>Wszystkie przekazane Współpracownikowi informacje (w formie papierowej, elektronicznej, ustnej etc.) muszą być przez niego traktowane bezwzględnie jak tajemnica przedsiębiorstwa Spółki Grupy TAURON i podlegać ochronie. Współpracownik zobowiązany jest w trakcie realizacji zlecenia do stosowania co najmniej następujących zasad:</p> <ul style="list-style-type: none"> a. przy przetwarzaniu udostępnionych lub powierzonych informacji, należy szczególnie zadbać o zachowanie poufności, integralności i dostępności tych informacji, b. rekomenduje się przekazywanie nośników danych z zastosowaniem protokołu zdawczo-odbiorczego, c. stosowanie ustalonych sposobów szyfrowania oraz innych zabezpieczeń plików elektronicznych, które mają być przesyłane pocztą elektroniczną, składowane, przekazywane dalej, 	<ul style="list-style-type: none"> a. przekazywania nośników informacji zawierających dane Spółek Grupy TAURON podwykonawcom zaangażowanym przez Współpracownika bez umowy zachowania poufności (NDA), b. pozostawiania bez dozoru lub udostępniania osobom nieupoważnionym informacji (w formie elektronicznej, papierowej itp.) przekazanych przez Spółkę Grupy TAURON, c. przekazywania w rozmowie ustnej informacji pozyskanych lub zauważonych podczas realizacji zadań, należących do Spółki Grupy TAURON.

Załącznik nr 2 do Polityki Systemu Zarządzania Bezpieczeństwem w Grupie TAURON – Podstawowe wymagania bezpieczeństwa obowiązujące w Grupie TAURON dla Współpracowników

- d. stosowanie ustalonych zabezpieczeń chroniących poufność, dostępność dokumentów papierowych,
- e. zbędne wydruki, notatki, kserokopie dokumentów itp. zawierające informacje należące do Spółek Grupy TAURON muszą być bezwzględnie niszczone w sposób uniemożliwiający odtworzenie ich treści.
- f. wydruki, dokumenty zawierające dane Spółek Grupy TAURON po zakończeniu pracy muszą być przechowywane w zamkniętych szafach uniemożliwiającym dostęp do nich osobom nieupoważnionym.

2.4 Bezpieczeństwo IT w ramach świadczonych usług dla Grupy TAURON

1. Współpracownik korzystający ze sprzętu komputerowego i zasobów informatycznych Grupy TAURON, jeżeli zapisy umowne nie stanowią inaczej, powinien stosować co najmniej poniższe zasady:

ZASADY	ZABRANIA SIĘ
<p>Współpracownik korzystający ze sprzętu komputerowego (komputery, urządzenia mobilne, telefony etc.) zobowiązany jest do:</p> <ul style="list-style-type: none"> a. używania tylko legalnego oprogramowania, b. używania oprogramowania antywirusowego z aktualną bazą wirusów, c. stosowania silnych haseł, zgodnie z dobrymi praktykami oraz politykami haseł stosowanymi w Grupie TAURON, d. natychmiastowej zmiany hasła, jeśli istnieje podejrzenie, że zostało odkryte lub wiadomo, że znajduje się ono w posiadaniu osoby innej niż Współpracownik, e. ustawienia monitorów, stanowisk z dostępem do danych udostępnianych przez 	<ul style="list-style-type: none"> 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 osób trzecich, nie związanych z realizacją usługi, o infrastrukturze informatycznej Spółki Grupy TAURON, stosowanych zabezpieczeniach, wykorzystywanych systemach informatycznych, e. stosowania oprogramowania z naruszeniem warunków stosownej licencji,

Załącznik nr 2 do Polityki Systemu Zarządzania Bezpieczeństwem w Grupie TAURON – Podstawowe wymagania bezpieczeństwa obowiązujące w Grupie TAURON dla Współpracowników

<p>Spółkę Grupy TAURON (w pomieszczeniach, gdzie przebywają osoby postronne) w taki sposób, żeby uniemożliwić tym osobom wgląd w dane,</p> <p>f. zabezpieczenia dostępu do systemu informatycznego przed dostępem osób nieuprawnionych (zablokowanie ekranu lub wylogowanie się z systemu), w przypadkach chwilowego opuszczenia stanowiska pracy,</p> <p>g. wykorzystywania urządzeń mobilnych do przetwarzania informacji, wyłącznie wtedy, gdy urządzenie jest zaszyfrowane,</p> <p>h. wykorzystywania sieciowych technologii bezprzewodowych do transmisji informacji wyłącznie wtedy, gdy przekaz jest szyfrowany,</p> <p>i. wylogowania się z systemu informatycznego po zakończeniu pracy w tym systemie.</p>	<p>f. korzystania z dostępu do sieci Spółki Grupy TAURON w miejscach publicznych i innych miejscach lub w sposób powodujący ryzyko ujawnienia danych uwierzytelniających oraz przetwarzanych informacji.</p>
--	--

2.4.2 Dostęp Współpracownika do sieci i systemów informatycznych Spółki Grupy TAURON

Współpracownik korzystający z własnego sprzętu komputerowego, jeżeli zapisy umowne nie stanowią inaczej, powinien stosować co najmniej poniższe zasady:

ZASADY	ZABRANIA SIĘ
<p>a. dostęp do sieci i systemów informatycznych Grupy TAURON jest możliwy wyłącznie po autoryzacji służb informatycznych Grupy TAURON,</p> <p>b. dostęp i sposób dostępu ustalany i przekazywany jest przez służby informatyczne Grupy TAURON,</p> <p>c. korzystanie z systemów informatycznych Grupy TAURON jest możliwe na następujących zasadach:</p>	<p>a. samodzielnych prób łączenia z bezprzewodową siecią korporacyjną,</p> <p>b. samodzielnego wpinania urządzeń do sieci informatycznej,</p> <p>c. dla urządzeń komputerowych pracujących w sieci LAN zestawiania innych połączeń niż połączenia autoryzowane przez służby informatyczne Grupy TAURON,</p> <p>d. testowania lub podejmowania prób poznania metod zabezpieczenia sieci</p>

Załącznik nr 2 do Polityki Systemu Zarządzania Bezpieczeństwem w Grupie TAURON – Podstawowe wymagania bezpieczeństwa obowiązujące w Grupie TAURON dla Współpracowników

<ul style="list-style-type: none"> • w przypadku zdalnego dostępu do systemów informatycznych Spółek Grupy TAURON uwierzytelnianie odbywa się z wykorzystaniem certyfikatu wystawionego przez TAURON Obsługa Klienta sp. z o.o. (CUWIT), • zdalna obsługa może być prowadzona jedynie z wykorzystaniem urządzeń, które posiadają aktualne zabezpieczenia antywirusowe oraz zainstalowane niezbędne poprawki i aktualizacje bezpieczeństwa, • w przypadku zakończenia świadczenia usługi Współpracownik zobowiązany jest bezzwłocznie zaprzestać korzystania z posiadanych dostępów. 	<p>i systemów informatycznych Grupy TAURON,</p> <p>e. prób obejścia zabezpieczeń systemów informatycznych.</p>
--	--

2.4.3 Monitorowanie działań użytkowników systemów IT

Wszystkie czynności związane z dostępem i użytkowaniem zasobów informatycznych Grupy TAURON, ze względu na bezpieczeństwo Grupy TAURON, są monitorowane w sposób ciągły przez systemy bezpieczeństwa, a dane o tych czynnościach są rejestrowane.

2.5 Incydenty bezpieczeństwa

1. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie bezpieczeństwa, Współpracownik jest zobowiązany bezzwłocznie powiadomić osobę wyznaczoną do współpracy, Opiekuna umowy lub pracownika ochrony obiektu o zaistniałej sytuacji. Takimi okolicznościami lub naruszeniami mogą być:

- 1) obecność osób obcych, których zachowanie w danym miejscu budzi wątpliwości,
- 2) pozostawione bez nadzoru dokumenty, w szczególności z oznaczeniem „Informacja Chroniona” lub „Informacja Ściśle Chroniona”,
- 3) korzystanie z obcego identyfikatora lub hasła,
- 4) niezamknięte, pozostawione bez opieki pomieszczenia,
- 5) niezablokowany komputer z dostępem do systemów informatycznych,

Załącznik nr 2 do Polityki Systemu Zarządzania Bezpieczeństwem w Grupie TAURON – Podstawowe wymagania bezpieczeństwa obowiązujące w Grupie TAURON dla Współpracowników

- 6) wykorzystywanie zdalnego połączenia VPN przez osoby nieupoważnione,
- 7) naruszenie lub wadliwe funkcjonowanie zabezpieczeń budowlanych, jak drzwi, okna w pomieszczeniach oraz mechanicznych, jak np. wyłamane lub zacinające się zamki, naruszone plomby, nie domykające się lub uszkodzone okna,
- 8) utratę nośnika zawierającego informacje należące do Grupy TAURON, w szczególności kradzież lub zaginięcie kopii bezpieczeństwa, wydruku, pendrive czy dysku,
- 9) inne zdarzenia, które wg własnej oceny stanowią zagrożenie dla bezpieczeństwa.

2. Incydenty wynikające z działań Współpracownika związane z:

- 1) nieuprawnionym dostępem do systemu informatycznego Grupy TAURON,
 - 2) niezabezpieczeniem informacji przed dostępem osób nieuprawnionych,
 - 3) udostępnieniem informacji osobom trzecim,
 - 4) pozyskiwaniem oprogramowania z nielegalnych źródeł,
 - 5) instalacją na sprzęcie IT należącym do Grupy TAURON oprogramowania nie pochodzącego i nieautoryzowanego przez służby informatyczne Grupy TAURON,
 - 6) wprowadzeniem do systemu teleinformatycznego treści prawnie zakazanych lub chronionych,
 - 7) łamaniem haseł,
 - 8) deszyfracją plików,
 - 9) nieautoryzowanymi próbami łamania zabezpieczeń,
 - 10) naruszeniem Zasad bezpieczeństwa fizycznego,
- mogą być uważane za rażące naruszenie obowiązującej umowy ze Spółką Grupy TAURON, powodujące skutki określone w umowie.

3. Incydenty związane z naruszeniem bezpieczeństwa w Grupie TAURON powstałe na skutek działań Współpracownika, mogą spowodować natychmiastowe rozwiązanie umowy z winy Współpracownika oraz stanowią podstawę do żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeśli taki obowiązek wynika z zawartej umowy.