

| | |
|---|--|
| Tytuł: Standardy z zakresu bezpieczeństwa współpracy z Dostawcami wspierającymi działanie usługi kluczowej | |
| Klasa ochrony: „c” dane wewnętrzne Spółki | |
| Wydanie: 1.00 | |
| Sporządzono: | Imię i nazwisko: <i>Nadsztygar</i> <i>Urządzeń Elektrycznych p/z</i> Paweł Janowski <i>mgr inż. Paweł Janowski</i> |
| Zweryfikowano | Imię i nazwisko: Krzysztof Chołast – Kierownik Działu Energomaszynowego – Główny Elektryk <i>Główny Elektryk p/z</i> <i>Kierownik Działu</i> <i>Energomechanicznego p/z</i> Data weryfikacji: <i>09.02.2021</i> <i>inż. Krzysztof Chołast</i> Piotr Nowak – Główny Inżynier ds. przeróbki mechanicznej węgla <i>GŁÓWNY INŻYNIER</i> <i>ds. Przeróbki Mechanicznej Węgla</i> <i>Kierownik Działu Utrzymywania Ruchu-Przeróbki</i> Data weryfikacji: <i>16.02.2021</i> <i>mgr inż. Piotr Nowak</i> |
| Zatwierdzono: | Imię i nazwisko Krzysztof Kaźmierczak – Pełnomocnik ds. Ochrony i Bezpieczeństwa IK <i>Główny Specjalista</i> <i>Kierownik Działu ds. Ochrony</i> Data akceptacji: <i>18.02.2021</i> <i>inż. Krzysztof Kaźmierczak</i> |
| Miejsce publikacji: | ZSZ-BMP |
| Kategoria archiwalna | B2 Kategoria archiwalna "B2" (Zgodnie z Ustawą o narodowym zasobie archiwalnym i archiwach, dokumenty kategorii archiwalnej B2 podlegają przechowywaniu: 2 lata w archiwum zakładowym.) |

Spis treści

| | |
|--|----|
| 1. Cel i zakres stosowania dokumentu | 3 |
| 2. Polityka bezpieczeństwa podczas współpracy z Wykonawcą (Dostawcą) | 3 |
| 2.1. Cele bezpieczeństwa | 3 |
| 2.2. Klasyfikacja informacji | 3 |
| 2.3. Bezpieczeństwo informacji | 4 |
| 2.3.1. Wytoczne dotyczące przekazywania informacji | 4 |
| 2.4. Bezpieczeństwo łańcucha dostaw | 6 |
| 2.5. Bezpieczeństwo personelu | 6 |
| 2.6. Bezpieczeństwo wymiennych nośników danych..... | 6 |
| 2.7. Bezpieczeństwo zdalnej pracy | 7 |
| 3. Bezpieczeństwo procesów projektowych Wykonawcy | 7 |
| 3.1. Bezpieczeństwo procesów projektowych Wykonawcy | 7 |
| 3.2. Zarządzanie zmianami | 7 |
| 3.3. Ochrona dokumentacji projektowej i eksploatacyjnej..... | 8 |
| 3.4. Incydenty bezpieczeństwa..... | 8 |
| 4. Ochrona kopii bezpieczeństwa..... | 8 |
| 5. Polityka korzystania z usług w chmurze | 8 |
| 6. Polityka audytów bezpieczeństwa Dostawców | 9 |
| 7. Polityka zakończenia współpracy | 9 |
| Załączniki | 10 |

1. Cel i zakres stosowania dokumentu

Celem niniejszego dokumentu jest określenie standardów bezpieczeństwa dla wdrażanych systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej przez Dostawców, danych jakie znajdują się w tych systemach, a także bezpieczeństwa realizacji zadań na rzecz LW Bogdanka S.A.

Standardy te powinny wspierać proces współpracy z dostawcami zewnętrznymi zgodnie z najlepszymi praktykami i rekomendacjami producentów oprogramowania oraz Polityką Bezpieczeństwa Informacji w systemach teleinformatycznych w spółce Lubelski Węgiel „Bogdanka” S.A.

Przytoczone pojęcia (powinno, należy, zalecane, wskazane, rekomendowane) określające standardy oznaczają zalecenie wykonywania opisanego postępowania.

Niezastosowanie się do standardów dopuszczalne jest tylko w przypadku, gdy w wyniku przeprowadzonej analizy wykazano, że zastosowanie się jest niemożliwe, szkodliwe lub niebezpieczne, zbędne, nieracjonalne lub nieefektywne.

Niezastosowanie się do standardów należy uzasadnić.

2. Polityka bezpieczeństwa podczas współpracy z Wykonawcą (Dostawcą)

2.1. Cele bezpieczeństwa

Dostawca POWINIEN zapewnić, że zadania realizowane na rzecz LW Bogdanka S.A. będą zarządzane zgodnie z standardami zawartymi w Art. 2. Polityki Bezpieczeństwa Informacji w systemach teleinformatycznych w spółce Lubelski Węgiel „Bogdanka” S.A.

W szczególności MUSI zostać zapewnione, aby:

- a. Dostawca zidentyfikował i oszacował ryzyka związane z realizacją przedsięwzięcia z zakresu bezpieczeństwa informacji.
- b. Zdefiniował i zastosował zabezpieczenia adekwatne do zidentyfikowanych ryzyk.

2.2. Klasyfikacja informacji

Dostawca POWINIEN stosować klasyfikację informacji przesyłanej, przechowywanej i przetwarzanej w kontekście realizacji zadań na rzecz LW Bogdanka S.A. zgodnie z zasadami klasyfikacji informacji określonymi w Art. 6 Polityce Bezpieczeństwa Informacji w systemach teleinformatycznych w spółce Lubelski Węgiel „Bogdanka” S.A. lub w inny sposób zgodnie z najlepszymi standardami-praktykami określonymi w rozdz. 8.2 normy PN-ISO/IEC 27002-12.

Zgodnie z zasadami określonymi w Polityce Bezpieczeństwa Informacji w systemach teleinformatycznych wyróżnia się następujące, główne kategorie informacji przetwarzanych w systemach

informatycznych:

a) **Informacje chronione, do których należą poniższe grupy informacji:**

- **informacje niejawne** (opatrzone klauzulą „zastrzeżone”, „poufne”, „tajne” lub „ściśle tajne”),
- **informacje ściśle ewidencjonowane takie jak np.** koncesje, projekt eksploatacji złóż,
- **dane osobowe** (dane pracowników, współpracowników, kontrahentów - osób fizycznych),
- **informacje handlowe Spółki** (obroty z kontrahentami zewnętrznymi),
- **informacje wewnętrzne Spółki** (dokumenty wewnątrzzakładowe, stany magazynowe, plany i wyniki produkcyjne, ewidencje majątkowe firmy, analizy ekonomiczne, rejestry pracy maszyn, ruchy wyposażenia itp.),

b) **Informacje jawne:** informacje, do publikacji których spółka jest zobowiązana przepisami prawa, informacje marketingowe oraz informacje pochodzące z ogólnodostępnych źródeł zewnętrznych.

2.3. Bezpieczeństwo informacji

Dostawca POWINIEN zapewnić bezpieczeństwo informacji przesyłanej w związku z realizacją zadań na rzecz LW „Bogdanka” S.A.

W szczególności Dostawca MUSI:

- a. Zapewnić ochronę poufności oraz integralności informacji przesyłanej publicznymi kanałami transmisyjnymi, odpowiednio do jej klasyfikacji.
- b. Zapewnić, że wszystkie osoby mające dostęp do informacji chronionych lub szczególnie chronionych podpisały klauzule poufności.
- c. Informacje chronione w dowolnej postaci (np. papierowej lub elektronicznej) podlegają ochronie przed: kradzieżą, wyciekiem, nieautoryzowanym dostępem, modyfikacją, utratą (zniszczeniem).

2.3.1. Wytyczne dotyczące przekazywania informacji

- a. Każda Informacja, przekazana podmiotom zewnętrznym podlega ocenie pod kątem jej znaczenia dla LW Bogdanka S.A., co stanowi podstawę do jej klasyfikacji.
- b. Klasyfikacja Informacji ma na celu zapewnienie odpowiedniego poziomu jej zabezpieczenia.
- c. Dokumenty klasyfikowane są do klasy nie niższej niż najwyższa klasa ochrony Informacji w nich zawartych.
- d. Za nadanie klasy ochrony odpowiada Właściciel Informacji.
- e. Klauzulę nadaje autor Dokumentu podczas jego tworzenia na podstawie analizy potencjalnego wpływu, jaki miałoby naruszenie dowolnego Atrybutu bezpieczeństwa.
- f. Kierownik komórki/jednostki organizacyjnej zatrudniającej autora dokumentu staje się Właścicielem Informacji i ma obowiązek weryfikować klasy

nadawane Dokumentom wytwarzanym w podległej sobie komórce/jednostce organizacyjnej.

- g. Każdy Pracownik musi zapoznać się z przyjętymi kryteriami klasyfikacji Informacji i zasadami ich prawidłowego stosowania.
- h. Należy dbać o właściwą klasyfikację informacji. Zarówno zakwalifikowanie Informacji do zbyt niskiej jak i do zbyt wysokiej klasy ochrony może spowodować szkodę dla interesów LW Bogdanka S.A..
- i. W przypadku Dokumentów udostępnianych do podmiotów zewnątrz odpowiednią klasę ochrony nadaje Właściciel Dokumentu.
- j. Jeżeli zachodzi konieczność przekazania poza Spółkę Informacji klasy chronionej (zgodnie z ***Polityką Bezpieczeństwa Informacji w systemach teleinformatycznych w spółce Lubelski Węgiel „Bogdanka” S.A.***) Właściciel Dokumentu musi uzyskać zgodę na jej przekazanie od Dyrektora lub Kierownika komórki podlegającej bezpośrednio pod członka Zarządu Spółki, w której gestii podlega kompetencyjnie dana Informacja.
- k. Jeśli udostępnienie Informacji wewnętrznej Spółki jest wymogiem związanym ze współpracą z zewnętrzną organizacją lub Dostawcą zewnętrznym należy:
 - uzyskać od odbiorcy stosowne oświadczenie o zachowaniu poufności informacji uzyskanych podczas współpracy ze Spółką (np. w formie klauzuli umownej) i stosowania się do zapisów niniejszych ***Zasad*** oraz w ***Polityce Bezpieczeństwa Informacji w systemach teleinformatycznych w spółce Lubelski Węgiel „Bogdanka” S.A.***
 - wyznaczyć jedną lub dwie osoby upoważnione do wymiany Informacji z odbiorcą,
 - wymianę Informacji chronionych z odbiorcami zewnętrznymi prowadzić wyłącznie przez upoważnione osoby w sposób umożliwiający identyfikację, jakie i kiedy Informacje zostały przekazane,
 - przekazywać Informacje chronione wyłącznie w zakresie koniecznym dla realizacji przedmiotu umowy przez Spółkę lub odbiorcę.
- m. Wyznaczenie osób upoważnionych do wymiany Informacji wewnętrznej Spółki z Dostawcą winno zostać utrwalone poprzez:
 - stosowny zapis w umowie z odbiorcą, gdzie osoby upoważnione wymieniane są jako osoby do kontaktów ze strony LW Bogdanka S.A. lub
 - oświadczenie w formie elektronicznej lub
 - oświadczenie w formie pisemnej.
- n. Udostępnianie informacji, zawierających dane osobowe, nie może naruszać zasad zawartych w regulacjach prawnych, zarządzenia wewnętrzne i zalecenia, a w szczególności następujących przepisów:
 - RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

- ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781 z późn. zm.),
- ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 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) (Dz.U. z 2019r., poz. 730),

2.4. Bezpieczeństwo łańcucha dostaw

Dostawca MUSI zidentyfikować i udokumentować łańcuch dostaw związany z realizacją zadania (projektu).

Zaleca się, aby Dostawca zapewnił, że jego podwykonawcy zapewniają taki sam poziom bezpieczeństwa jaki spełnia on sam w odniesieniu do LW Bogdanka S.A. Dostawca odpowiada za zapewnienie bezpieczeństwa w całym łańcuchu dostaw produktów i usług, za który jest odpowiedzialny zgodnie z zawartą umową.

2.5. Bezpieczeństwo personelu

Dostawca POWINIEN zapewnić bezpieczeństwo wykorzystywanego personelu adekwatnie do zadań realizowanych na rzecz LW Bogdanka S.A.

W szczególności Dostawca MUSI posiadać i realizować udokumentowane polityki dotyczące jego personelu, które obejmują:

- a. Przekazanie swojemu personelowi, realizującemu zadania na rzecz LW Bogdanka S.A, informacji o wymaganiach bezpieczeństwa współpracy z LW Bogdanka S.A.
- b. Podpisanie przez pracowników realizujących zadania na rzecz LW Bogdanka S.A oświadczeń o zapoznaniu się z wymaganiami bezpieczeństwa i odpowiednimi politykami ich realizacji. Podpisane oświadczenie winno także zawierać klauzulę o zachowaniu poufności pozyskanych informacji.
- c. Określenie i przedstawienie które zakresy odpowiedzialności i obowiązki w zakresie bezpieczeństwa informacji pozostaną aktualne po zakończeniu lub zmianie zatrudnienia.

2.6. Bezpieczeństwo wymiennych nośników danych

Dostawca POWINIEN zapewnić bezpieczeństwo wymiennych nośników danych wykorzystywanych w związku z realizacją zadań na rzecz LW Bogdanka S.A.

W szczególności Dostawca MUSI:

- a. Posiadać i realizować polityki dotyczące bezpiecznego usuwania danych z nośników zawierających dane związane z realizacją zadań na rzecz LW Bogdanka S.A, zapewniając skuteczne usuwanie.
- b. Posiadać i realizować polityki bezpiecznego przekazywania nośników zawierających dane związane z realizacją zadań na rzecz LW Bogdanka S.A, zapewniając skuteczną ochronę danych.

2.7. Bezpieczeństwo zdalnej pracy

Wymaga się aby zdalny dostęp był realizowany zgodnie Regulaminem zarządzania bezpiecznym dostępem zdalnym dla Kontrahentów do zasobów teleinformatycznych LW „Bogdanka” S.A (załącznik nr 9 Polityki Bezpieczeństwa Informacji w systemach teleinformatycznych w spółce LW Bogdanka S.A.)

3. Bezpieczeństwo procesów projektowych Wykonawcy

3.1. Bezpieczeństwo procesów projektowych Wykonawcy

W szczególności Dostawca POWINIEN:

- zagwarantować, że wykorzystanie produktu możliwe będzie w odpowiednio długim okresie czasowym, a wsparcie administracyjne i autorskie będzie utrzymywane przez dostawcę/producenta przez cały okres planowanej eksploatacji produktu.
- systemy posiadały kompletną dokumentację techniczną zawierającą:
 - i. instrukcje użytkowania, administrowania i utrzymania systemu,
 - ii. instrukcje postępowania w sytuacji występowania błędów i awarii systemu.

3.2. Zarządzanie zmianami

Dostawca POWINIEN zapewnić, że zmiany wprowadzane do projektowanych rozwiązań będą realizowane zgodnie z Art. 42 Polityki Bezpieczeństwa Informacji a w szczególności że:

- a. Zmiany będą rejestrowane.
- b. Zmiany będą zatwierdzane przez upoważnione osoby.
- c. Będą istniały procedury zarządzania zmianami w wytwarzanych aplikacjach i systemach.
- d. Przed przeprowadzeniem aktualizacji lub wprowadzeniem zmiany systemu informacyjnego administrator dostawcy systemu wykonuje kopię bezpieczeństwa systemu.
- e. Administratorzy Dostawcy systemów przeprowadzają testy przed wprowadzeniem każdej zmiany w systemach produkcyjnych.
- f. Testy, o ile to możliwe, są przeprowadzane w wydzielonym środowisku testowym możliwie najbardziej zbliżonym do środowiska produkcyjnego.
- g. Po wprowadzeniu zmian w środowisku produkcyjnym administratorzy dostawcy systemów przeprowadzają ponowne prace kontrolne i sprawdzające poprawność działania z resztą modułów lub systemów współistniejących.

- h. W sytuacji, kiedy wprowadzone lub planowane zmiany mogą mieć lub mają bezpośredni lub pośredni wpływ na zmianę podatności i zagrożeń systemu, Dyrektor ds. Informatyki, Główny Elektryk, Główny Inżynier ds. Przeróbki Mechanicznej Węgla zostają poinformowani każdy w swoim obszarze, o możliwym zakresie i ryzyku w obszarze cyberbezpieczeństwa systemów informacyjnych objętych zmianami.
- i. Wprowadzanie zmian systemowych i aktualizacji odbywa się z zachowaniem istniejących zabezpieczeń aplikacji oraz procedur integralności.

3.3. Ochrona dokumentacji projektowej i eksploatacyjnej

Dostawca POWINIEN zapewnić ochronę dokumentacji projektowej oraz eksploatacyjnej, tworzonej i przetwarzanej na rzecz LW Bogdanka S.A, w szczególności poprzez:

- a. Dokumentacja może być udostępniona wyłącznie osobom mającym upoważnienie do dostępu do takiej informacji w oparciu o umowę z LW Bogdanka S.A.
- b. Dostawca jest ZOBOWIĄZANY do oznaczania dokumentacji projektowej klasą bezpieczeństwa według klasyfikacji LW Bogdanka S.A.

3.4. Incydynty bezpieczeństwa

Dostawca MUSI zapewnić identyfikowanie i obsługę incydentów bezpieczeństwa. W szczególności Dostawca MUSI zgłaszać w formie pisemnej do LW Bogdanka S.A. wszelkie incydynty bezpieczeństwa, które mają związek z zadaniami realizowanymi na rzecz LW Bogdanka S.A lub z produktami wytwarzanymi na rzecz LW Bogdanka S.A. W przypadku zaistnienia incydentu bezpieczeństwa Dostawca wspólnie z LW Bogdanka S.A. podejmuje wszelkie niezbędne środki, aby zminimalizować wpływ incydentu na ciągłość działania LW Bogdanka S.A lub na jego wizerunek publiczny.

4. Ochrona kopii bezpieczeństwa

Dostawca POWINIEN zapewnić ochronę kopii zapasowych informacji przetwarzanej w trakcie realizacji zadań na rzecz LW Bogdanka S.A.

W szczególności Dostawca MUSI zapewnić fizyczne zabezpieczenie kopii bezpieczeństwa, a także gdy jest to właściwe dla wymaganego poziomu ochrony informacji, szyfrowanie kopii bezpieczeństwa.

5. Polityka korzystania z usług w chmurze

- a. Dostawca NIE MOŻE przetwarzać za pomocą usług w chmurze danych osobowych oraz danych sklasyfikowanych jako dane handlowe Spółki i dane wewnętrzne Spółki bez pisemnej zgody LW Bogdanka S.A.

- b. Dostawca korzystając z usług w chmurze do realizacji zadań oraz budowy systemów na potrzeby LW Bogdanka S.A jest ZOBOWIĄZANY do zawarcia formalnej umowy prawnej z Wykonawcą tych usług.
- c. Dostawca JEST ZOBOWIĄZANY do powiadomienia LW Bogdanka S.A o wszelkich incydentach bezpieczeństwa związanych z korzystaniem z usług w chmurze.

6. Polityka audytów bezpieczeństwa Dostawców

- a. W przypadku kiedy Dostawcą będzie realizował prace za pomocą dostępu zdalnego MUSI zapewnić LW Bogdanka S.A możliwość przeprowadzenia audytu bezpieczeństwa w zakresie własnych środowisk wykorzystywanych do współpracy z LW Bogdanka S.A lub przedstawić wyniki audytu bezpieczeństwa informacji wykonanych zgodnie z normą ISO 27001
- b. Zakres audytu bezpieczeństwa POWINIEN być adekwatny do projektu, którego dotyczy.
- c. Termin audytu POWINIEN być uzgodniony z Wykonawcą minimum na 14 dni robocze przed planowanym audytem.
- d. Wyniki audytu WINNY być omówione z przedstawicielami Wykonawcy. Z przeglądu MUSI zostać sporządzony udokumentowany plan działania, w przypadku zidentyfikowania niezgodności.
- e. Wyniki audytu są klasyfikowane jako informacja handlowe (tajemnica przedsiębiorstwa), chronione Spółki LW Bogdanka S.A.

7. Polityka zakończenia współpracy

- a. Dostawca JEST ZOBOWIĄZANY do zwrotu wszystkich aktywów powierzonych przez LW Bogdanka S.A.
- b. Dostawca JEST ZOBOWIĄZANY do zapewnienia bezpieczeństwa wszystkich informacji chronionych w okresie czasu określonego w umowie, po zakończeniu współpracy.
- c. Dostawca JEST ZOBOWIĄZANY do skutecznego zniszczenia informacji, która winna zostać zniszczona po zakończeniu umowy.
- d. Dostawca JEST ZOBOWIĄZANY do przedstawienia protokołu przeprowadzenia zniszczenia ww. informacji.

Załączniki

Załącznik nr 1 Zalecenia dotyczące cyberbezpieczeństwa dla wdrażanych systemów informacyjnych oraz minimalnych wymagań instrukcji eksploatacji systemów wykorzystywanych do świadczenia usługi kluczowej

W dokumencie występują odwołania do:

[1] Polityka Bezpieczeństwa Informacji w systemach teleinformatycznych w spółce Lubelski Węgiel „Bogdanka” S.A.