

Polityka ochrony tajemnicy przedsiębiorstwa InnoBaltica Sp. z o.o. (sierpień 2018)

SPIS TREŚCI

I.	Definicje.....
II.	Postanowienia ogólne
III.	Zakres stosowania.....
IV.	Postępowanie z Dokumentami zawierającymi informacje stanowiące Tajemnicę przedsiębiorstwa.....
V.	Archiwizacja.....
VI.	Niszczanie.....
VII.	Odpowiedzialność.....
VIII.	Postanowienia końcowe.....
IX.	Akty prawne i dokumenty związane.....
X.	Spis załączników.....
XI.	Wzory załączników.....

I. Definicje

Dokument – każdy dokument lub jego część, w wersji drukowanej lub plik utrwalony na elektronicznym nośniku informacji, zawierający informacje stanowiące Tajemnicę przedsiębiorstwa i oznaczony klauzulą „TAJEMNICA PRZEDSIĘBIORSTWA”;

Polityka ochrony Tajemnicy przedsiębiorstwa (dalej **Polityka**) – zespół reguł oraz dobrych praktyk, mających na celu ochronę informacji stanowiących Tajemnicę przedsiębiorstwa przed ich nieuprawnionym ujawnieniem;

Przetwarzanie informacji – operacja lub zestaw operacji wykonywanych na informacjach lub na zestawach informacji w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

Tajemnica przedsiębiorstwa – nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne Spółki lub inne informacje posiadające dla Spółki wartość gospodarczą, co do których Spółka podjęła niezbędne działania w celu zachowania ich poufności;

Spółka – InnoBaltica Sp. z o.o.

Zasada „need to know” - zasada postępowania, według której użytkownik w trakcie pracy uzyskuje dostęp do informacji przetwarzanych w Spółce w zakresie nie szerszym niż niezbędny do niezakłóconego wykonywania powierzonych obowiązków służbowych na zajmowanym stanowisku, z uwzględnieniem specyfiki struktury organizacyjnej Spółki, wynikającej z potrzeb realizacji jej celów i statutowych zadań;

II. Postanowienia ogólne

1. Wprowadza się do stosowania Politykę ochrony Tajemnicy przedsiębiorstwa InnoBaltica Sp. z o.o.;
2. Polityka jest dokumentem jawnym, z wyjątkiem Załącznika nr 7, i podlega opublikowaniu na stronie internetowej Spółki;
3. Celem Polityki jest zapewnienie prawnej ochrony Informacji przetwarzanych w Spółce:
 - a) posiadających dla Spółki wymierną wartość gospodarczą;
 - b) których ujawnienie osobom nieuprawnionym mogłoby narazić ją na wymierne straty finansowe bądź utratę dobrego imienia.
4. Polityka określa:
 - a) Rodzaje informacji stanowiących Tajemnicę przedsiębiorstwa;
 - b) Tryb i zasady przetwarzania Dokumentów, między innymi w zakresie ich wytwarzania, rejestrowania, modyfikowania, kopiowania, klasyfikowania, gromadzenia, przechowywania, przekazywania, udostępniania niszczenia i archiwizacji;

- c) Wzory dokumentów związanych z ochroną Tajemnicy przedsiębiorstwa;
 - d) Zakres odpowiedzialności za powierzone informacje oraz za ich nieuprawnione ujawnienie.
5. Do określania rodzajów informacji mogących stanowić Tajemnicę przedsiębiorstwa uprawniony jest Zarząd Spółki, w porozumieniu z kierownikami komórek organizacyjnych lub obszarów, w zakresie przysługujących im kompetencji służbowych.
6. Wykaz rodzajów informacji mogących stanowić Tajemnicę przedsiębiorstwa stanowi **Załącznik nr 7** do Polityki.

III. Zakres stosowania

1. Do informacji stanowiących Tajemnicę przedsiębiorstwa w Spółce mogą zostać dopuszczone osoby, które:
- a) zostały zapoznane z niniejszą Polityką oraz
 - b) podpisały zobowiązanie do zachowania poufności informacji, w związku z:
 - i. z zatrudnieniem w Spółce;
 - ii. wykonywaniem obowiązków na rzecz Spółki wynikających z zawartych umów;
 - iii. wykonywaniem innych czynności, niezbędnych do realizacji statutowych zadań Spółki;
 - iv. wykonywaniem czynności urzędowych, wynikających z obowiązujących przepisów prawa;
2. Wzór zobowiązania do zachowania poufności stanowi **Załącznik nr 1** do niniejszej Polityki.
3. Zapoznanie osoby z Polityką oraz odebranie od niej pisemnego zobowiązania do zachowania poufności w stosunku do informacji stanowiących Tajemnicę przedsiębiorstwa leży w gestii Koordynatora-Administratora Bezpieczeństwa Informacji i powinno nastąpić niezwłocznie po nawiązaniu stosunku pracy. Powyższe dotyczy również osób zatrudnionych w Spółce na podstawie umów cywilno-prawnych.
4. Pisemne potwierdzenie zapoznania się z Polityką oraz podpisane zobowiązanie do zachowania poufności informacji włącza się do akt personalnych pracownika Spółki.
5. Zakres dostępu do informacji stanowiących Tajemnicę przedsiębiorstwa określa bezpośredni przełożony pracownika, zgodnie z zasadą „need to know” (wiedzy niezbędnej).

IV. Postępowanie z Dokumentami zawierającymi informacje stanowiące Tajemnicę przedsiębiorstwa

A. Postępowanie z dokumentami w wersji drukowanej

1. Dokument zawierający informacje stanowiące Tajemnicę przedsiębiorstwa podlega zaewidencjonowaniu w odrębnym Rejestrze Dokumentów oznaczonych klauzulą „Tajemnica Przedsiębiorstwa”, prowadzonym przez Koordynatora-Administratora Bezpieczeństwa Informacji;
2. Wzór Dokumentu zawierającego informacje stanowiące Tajemnicę przedsiębiorstwa stanowi **Załącznik nr 2** do Polityki.

3. Rejestr Dokumentów oznaczonych klauzulą „Tajemnica Przedsiębiorstwa” prowadzony jest zarówno w wersji papierowej jak i elektronicznej;
4. Wzór Rejestru, o którym mowa w pkt 1. powyżej, stanowi **Załącznik nr 3** do Polityki;
5. Treść Dokumentu w wersji drukowanej, po jego zeskanowaniu, nadaniu mu formy elektronicznej i wprowadzeniu do bazy danych, może być widoczna wyłącznie dla osób upoważnionych;
6. Oryginał Dokumentu przechowuje w aktach jego dysponent;
7. Na wersji drukowanej Dokumentu nanosi się klauzulę poufności poprzez odcisnięcie, w lewym górnym rogu, na każdej stronie i w sposób nie budzący wątpliwości dla ewentualnego odbiorcy, pieczęci o treści „TAJEMNICA PRZEDSIĘBIORSTWA”. W przypadku wykonania Dokumentu w więcej niż jednym egzemplarzu, klauzulę umieszcza się odpowiednio na każdym egzemplarzu Dokumentu.
8. Wzór pieczęci o treści „TAJEMNICA PRZEDSIĘBIORSTWA” stanowi **Załącznik nr 4** do Polityki.
9. Na dole Dokumentu umieszcza się informację o treści: *„Niniejszy dokument zawiera informacje stanowiące prawnie chronioną tajemnicę przedsiębiorstwa InnoBaltica Sp. z o.o. W związku z tym zobowiązuje się dysponenta dokumentu lub jego adresata do ochrony informacji w nim zawartych przed dostępem osób trzecich. Zabrania się ich powielania, kopiowania, skanowania, publikowania, wykonywania wyciągów lub odpisów bez uprzedniej, pisemnej zgody InnoBaltica Sp. z o. o. z siedzibą w Gdańsku”.*
10. Klauzulę poufności nadaje i nanosi na Dokumentach pracownik uprawniony do jego podpisania lub do oznaczenia klauzulą innego materiału niż Dokument, w porozumieniu z bezpośrednim przełożonym.
11. Do oryginału Dokumentu dołącza się kartę zapoznania/przekazania Dokumentu;
12. W przypadku przekazania Dokumentu do czasowego użytkownika innej osobie, kartę zapoznania/przekazania Dokumentu pozostawia się w aktach pierwotnego dysponenta Dokumentu, jako informację o tym fakcie, umieszczając w karcie adnotację o jego przekazaniu;
13. Trwałe przekazanie Dokumentu innemu pracownikowi Spółki następuje wraz z kartą zapoznania/przekazania Dokumentu, z właściwą adnotacją o przekazaniu i przyjęciu tego Dokumentu;
14. Wzór karty zapoznania/przekazania Dokumentu stanowi **Załącznik nr 5** do niniejszej Polityki.
15. Dopuszcza się możliwość skanowania lub kopiowania zarejestrowanego Dokumentu, celem jego przesłania drogą elektroniczną do innego odbiorcy niż pracownik Spółki, jednak wyłącznie na pisemne polecenie lub za pisemną zgodą przełożonego wytwórcy lub dysponenta oryginału Dokumentu;
16. Fakt wykonania kopii lub skanu Dokumentu należy odnotować w Rejestrze Dokumentów, o którym mowa w pkt. 1 powyżej, papierowym oraz elektronicznym (w kolumnie „UWAGI”), podając:
 - a) datę kopiowania lub skanowania;
 - b) cel kopiowania/skanowania
 - c) rodzaj nośnika (papier/płyta CD/pendrive/pamięć zewnętrzna)
 - d) liczbę wykonanych egzemplarzy (w przypadku kopiowania) oraz ich adresatów;
 - e) adresata lub adresatów poszczególnych kopii Dokumentów lub skanu (w przypadku zamiaru przesłania dokumentu drogą elektroniczną);
 - f) informację, na czyje polecenie lub za czyją zgodą wykonano skan lub kopię;

- g) imię i nazwisko osoby zlecającej wykonanie czynność kopiowania lub skanowania;
 - h) imię i nazwisko osoby wykonującej czynność kopiowania lub skanowania;
17. W uzasadnionych przypadkach dopuszcza się możliwość zapoznania z treścią Dokumentu pracowników Spółki innych niż jego dysponent. Powyższe może nastąpić na wniosek dysponenta po uzyskaniu pisemnej zgody jego przełożonego, lub na pisemne polecenie tego przełożonego;
W takim przypadku zamieszcza się na Dokumencie stosowną dyspozycję, zawierającą imię i nazwisko oraz stanowisko służbowe osoby, która ma być z Dokumentem zapoznana.
18. W uzasadnionych przypadkach dopuszcza się możliwość zapoznania z treścią Dokumentu osób niebędących pracownikami Spółki. Powyższe powinno mieć miejsce w siedzibie Spółki i może nastąpić po uzyskaniu pisemnej zgody lub na pisemne polecenie członka Zarządu Spółki.
W takim przypadku przełożony umieszcza na Dokumencie dyspozycję jak w pkt 17 powyżej.
19. Uprawnienia do dostępu do Dokumentu w siedzibie Spółki, poza dysponentem Dokumentu oraz jego bezpośrednim przełożonym, posiadają:
- a) członkowie Zarządu Spółki oraz przedstawiciele jej organów nadzorczych;
 - b) przedstawiciele organów administracji i instytucji państwowych, w tym sądów, policji i prokuratury – w granicach i na podstawie obowiązujących przepisów prawa, w ramach prowadzonych postępowań oraz na podstawie stosownych prawomocnych i wykonalnych orzeczeń;
 - c) przedstawiciele służb, organów państwa i instytucji kontrolnych – na podstawie obowiązujących przepisów prawa i stosownych upoważnień do kontroli lub w ramach prowadzonych postępowań;
20. Dopuszcza się możliwość zapoznania/przekazania, czasowego wypożyczenia, wykonania kopii, wysłania skanu lub odpisu Dokumentu osobom wymienionym w pkt. 19 powyżej.
Dokumentowanie tych czynności odbywa się w sposób i z zachowaniem zasad określonych w pkt. 17 i 18 powyżej.
21. Dokumenty w wersji drukowanej oraz nośniki elektroniczne, wykorzystywane w bieżącej pracy, należy przechowywać w pomieszczeniu dysponenta Dokumentu lub nośnika, w zamykanych na klucz szafach, szufladach lub w sejfach.
22. W przypadku drukowania Dokumentu na drukarce nieposiadającej funkcjonalności zabezpieczonego wydruku, należy odebrać wydruk Dokumentu niezwłocznie po jego wyjściu z urządzenia.;
23. Zabrania się:
- a) pozostawiania wydrukowanych wersji Dokumentu na drukarkach oraz w pomieszczeniach ogólnodostępnych, umożliwiających dostęp do nich osobom nieupoważnionym;
 - b) pozostawiania Dokumentów oraz nośników elektronicznych, zawierających informacje stanowiące Tajemnicę przedsiębiorstwa, bez dozoru lub w niezamkniętych na klucz pomieszczeniach biurowych;
 - c) pozostawiania stacji roboczych w stanie niezablokowanym lub niewylogowanym w pomieszczeniach biurowych w czasie nieobecności w tych pomieszczeniach ich dysponenta;

Powyższe dotyczy również wszelkich innych Dokumentów zawierających informacje niebędące Tajemnicą przedsiębiorstwa;

24. Nieudane, zbędne wersje lub kopie Dokumentu oraz nieprzydatne nośniki elektroniczne, zawierające informacje stanowiące Tajemnicę przedsiębiorstwa, należy niszczyć trwale, w sposób uniemożliwiający ich odtworzenie, wyłącznie w przeznaczonych i przystosowanych do tego celu niszczarkach;
25. Zabrania się wyrzucania Dokumentów do koszy na śmieci.
Powyższe dotyczy również wszystkich innych dokumentów przetwarzanych w Spółce oraz stosowanych nośników informacji.

B. Postępowanie z Dokumentami w wersji elektronicznej oraz z elektronicznymi nośnikami informacji, zawierającymi pliki Dokumentów oznaczonych klauzulą „Tajemnica przedsiębiorstwa”

1. Elektroniczne nośniki informacji wykorzystywane w Spółce InnoBaltica podlegają ewidencjonowaniu w Rejestrze nośników elektronicznych, prowadzonym w wersji papierowej i elektronicznej przez Administratora ds. ITC;
2. Płyty CD jednokrotnego zapisu, na których utrwalono pliki Dokumentów (kopie), oznacza się trwale, poprzez naniesienie permanentnym markerem na płytę kolejnego numeru Dokumentu w Rejestrze;
3. Elektroniczne nośniki informacji zawierające kopie Dokumentów należy przechowywać w zamykanych na klucz szafach, szufladach lub w sejfach;
4. Informacje oznaczone klauzulą „Tajemnica przedsiębiorstwa”, przetwarzane w systemach teleinformatycznych Spółki, powinny być zabezpieczane przed nieuprawnionym dostępem przy wykorzystaniu informatycznych narzędzi systemowych, takich jak hasła dostępowe, natomiast ich elektroniczne kopie przechowywane na przystosowanych do tego celu nośnikach;
5. Zabrania się przesyłania elektronicznej wersji Dokumentów zwykłą pocztą elektroniczną w niezabezpieczonych plikach. Przesyłanie elektronicznych kopii Dokumentów jest dopuszczalne wyłącznie bezpiecznymi łączami, przy wykorzystaniu informatycznych narzędzi kryptograficznych;
6. Wszelkie nieprawidłowości w działaniu systemu teleinformatycznego, w którym przetwarzane są pliki zawierające Dokumenty, lub nieprawidłowości w działaniu osób przetwarzających te Dokumenty, należy zgłaszać niezwłocznie:
 - a) Koordynatorowi–Administratorowi Bezpieczeństwa Informacji;
 - b) Administratorowi ds. ITC;którzy podejmą niezwłocznie działania, zmierzające do usunięcia nieprawidłowości oraz zminimalizowania ich negatywnych skutków dla Spółki.

V. Archiwizacja

Dokumenty stanowiące Tajemnicę przedsiębiorstwa archiwizuje się na ogólnych zasadach i zgodnie z obowiązującą w Spółce Instrukcją Kancelaryjną .

VI. Niszczenie

1. Do wykonania czynności niszczenia zbędnych kopii Dokumentów powołuje się, w drodze zarządzenia Prezesa Zarządu Spółki, trzyosobową komisję w składzie:
 - a) dysponent dokumentu;
 - b) Koordynator – Administrator Bezpieczeństwa Informacji;
 - c) wskazany imiennie w zarządzeniu pracownik Spółki;
2. W przypadku usuwania plików Dokumentów z elektronicznych nośników informacji, w skład komisji powołuje się pracownika obszaru ITC spółki;
3. Kopie Dokumentów w wersji papierowej oraz elektroniczne nośniki informacji (płyty CD, karty pamięci, pamięci zewnętrzne, pendrivy) zawierające pliki Dokumentów lub Dokumenty, niszczy się fizycznie wyłącznie w przeznaczonych i dostosowanych do tego celu niszczarkach.
4. Przed fizycznym zniszczeniem nośnika elektronicznego należy, o ile istnieją w tym zakresie możliwości techniczne, usunąć zapisane na nim dane w sposób trwały, aby niemożliwe było ich odtworzenie;
5. Dokumenty lub pliki Dokumentów umieszczone na elektronicznych nośnikach informacji usuwa się z tych nośników w sposób trwały i uniemożliwiający ich odtworzenie, wyłącznie z wykorzystaniem przystosowanych do tego celu narzędzi informatycznych (programów komputerowych). Fizycznie procedurę usuwania plików z nośników informacji wykonuje uprawniony pracownik obszaru ITC Spółki na wyznaczonym do tego celu komputerze stacjonarnym.
6. Komisja dokumentuje wykonanie czynności niszczenia kopii Dokumentów/usuwania plików Dokumentów w formie protokołu, który powinien zawierać:
 - a) informację na temat składu komisji;
 - b) datę i miejsce oraz nazwę stacji roboczej, na której wykonano czynności niszczenia kopii Dokumentów/usuwania plików Dokumentów;
 - c) rodzaj narzędzia informatycznego (programu komputerowego) zastosowanego do usuwania plików z nośnika informacji;
 - d) wykaz niszczonych kopii Dokumentów/usuwanych plików Dokumentów z podaniem ich numerów z Rejestru Dokumentów;
 - e) podpisy członków komisji;
7. Protokół z czynności niszczenia kopii Dokumentów/usuwania plików Dokumentów sporządza się w pojedynczym egzemplarzu i przechowuje go w aktach dysponent oryginału Dokumentu, którego kopia podlega niszczeniu.
8. Wzór protokołu z czynności niszczenia kopii Dokumentów/usuwania plików Dokumentów stanowi **Załącznik nr 6** do Polityki.
9. Fakt zniszczenia kopii Dokumentów/usuwania plików Dokumentów z nośników informacji odnotowuje się w kolumnie UWAGI, w odpowiedniej pozycji Rejestru Dokumentów, pod którą Dokument został zaewidencjonowany, z podaniem numeru protokołu zniszczenia.

VII. Odpowiedzialność

1. Obowiązek ochrony informacji stanowiących Tajemnicę przedsiębiorstwa spoczywa na osobach, które weszły w ich posiadanie;

2. Za nadzór nad realizacją Polityki odpowiedzialny jest Koordynator–Administrator Bezpieczeństwa Informacji, który odpowiada w tym zakresie bezpośrednio przed Zarządem Spółki.
3. Koordynator–Administrator Bezpieczeństwa Informacji ma prawo, w ramach wykonywanych obowiązków, do przeprowadzenia kontroli sposobu postępowania z Dokumentami;
4. W kontroli sposobu postępowania z Dokumentami, przetwarzanymi w systemie teleinformatycznym, uczestniczy Administrator ds. ITC lub wyznaczony przez niego pracownik tego obszaru;
5. Z czynności kontrolnych sporządza się notatkę służbową, która powinna zawierać:
 - a) datę i godzinę przeprowadzenia kontroli;
 - b) imiona i nazwiska oraz stanowiska służbowe osób prowadzących kontrolę;
 - c) miejsce, przedmiot i zakres kontroli;
 - d) wyniki kontroli;
 - e) wnioski i zalecenia pokontrolne
6. W przypadku ujawnienia nieprawidłowości w sposobie postępowania z Dokumentami, Koordynator powiadamia Kierownika obszaru, w którym doszło do nieprawidłowości;
7. Naruszenie zasad Polityki grozi odpowiedzialnością porządkową lub dyscyplinarną na podstawie Kodeksu pracy i Regulaminu Pracy, i/lub odpowiedzialność karną, w szczególności w oparciu o przepisy ustawy z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji;

VIII. Postanowienia końcowe

1. Polityka nie obejmuje obszaru informacji niejawnych w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.
2. Wszelkie wątpliwości w zakresie interpretacji zapisów niniejszej Polityki rozstrzygane są przez Koordynatora – Administratora Bezpieczeństwa Informacji, który może w tym zakresie zasięgać opinii prawnych;
3. Polityka wchodzi w życie z dniem jej przyjęcia przez Zarząd Spółki.

IX. Akty prawne i dokumenty związane

1. Ustawa z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji
2. Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych
3. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych
4. Polityka Klasyfikacji Informacji

X. Spis załączników

1. Wzór zobowiązania do zachowania poufności informacji
2. Wzór dokumentu zawierającego informacje stanowiące Tajemnicę przedsiębiorstwa
3. Wzór Rejestru Dokumentów oznaczonych klauzulą „Tajemnica przedsiębiorstwa”
4. Wzór pieczęci o treści „TAJEMNICA PRZEDSIĘBIORSTWA”

5. Wzór karty zapoznania/wypożyczenia Dokumentu
6. Wzór protokołu z czynności niszczenia kopii/usuwania plików Dokumentów oznaczonych klauzulą „Tajemnica przedsiębiorstwa”
7. Wykaz rodzajów informacji mogących stanowić Tajemnicę przedsiębiorstwa InnoBaltica Sp. z o.o.

XI. Wzory załączników

Załącznik nr 1

do Polityki

ochrony tajemnicy przedsiębiorstwa

(Wzór)

ZOBOWIĄZANIE

do zachowania poufności informacji

Ja niżej podpisana/podpisany oświadczam, że zapoznałam/zapoznałem się, ze zrozumieniem, z obowiązującymi w InnoBaltica Sp. z o.o. przepisami oraz regułami w zakresie ochrony Tajemnicy przedsiębiorstwa, w szczególności z Polityką ochrony tajemnicy przedsiębiorstwa InnoBaltica Sp. z o. o.

Jednocześnie zobowiązuję się do:

- stosowania i przestrzegania tych przepisów i reguł;
- ochrony powierzonych mi informacji przed nieuprawnionym dostępem;
- zachowania poufności wszystkich informacji, co do których Spółka podjęła starania zmierzające do ich ochrony, do których dostęp uzyskałam/uzyskałem w trakcie wykonywania obowiązków pracowniczych/wykonywania umowy/wykonywaniem czynności, zarówno w trakcie mojego zatrudnienia/mojej współpracy/wykonywania czynności w InnoBaltica, jak i po jego/jej zakończeniu;¹
- stosowania zabezpieczeń służących ochronie tych informacji oraz zachowania poufności w odniesieniu do tych zabezpieczeń;

Jestem również świadoma/świadomy odpowiedzialności dyscyplinarnej oraz karnej w przypadku naruszenia tych przepisów.

.....
Data i podpis

¹ Niepotrzebne skreślić

Załącznik nr 2
do Polityki
ochrony tajemnicy przedsiębiorstwa
dokument zawierający informacje stanowiące tajemnicę przedsiębiorstwa
(wzór)

L.dz. _____/____

Gdańsk, _____

Egz. Nr _____

TREŚĆ DOKUMENTU

.....
Załączniki: X na X stronach

Załącznik nr 1 - _____ - X stron – tylko adresat

Załącznik nr 2 - _____ - X stron – tylko adresat

Załącznik nr 3 – płyta CD zawierająca – x szt.

Załącznik nr 4 – pendrive zawierający – x szt.

Wykonano w X egzemplarzach

Egz. Nr 1 - _____

Egz. Nr 2 - _____

Wykonał:

„Niniejszy dokument zawiera informacje stanowiące prawnie chronioną tajemnicę przedsiębiorstwa InnoBaltica Sp. z o.o. W związku z tym zobowiązuje się dysponenta dokumentu lub jego adresata do ochrony informacji w nim zawartych przed dostępem osób trzecich. Zabrania się ich powielania, kopiowania, skanowania, publikowania, wykonywania wyciągów lub odpisów bez uprzedniej, pisemnej zgody InnoBaltica Sp. z o. o.”

Załącznik nr 4
do Polityki
ochrony tajemnicy przedsiębiorstwa

Pieczęć o treści „Tajemnica przedsiębiorstwa”
(wzór)

TAJEMNICA PRZEDSIĘBIORSTWA

KARTA ZAPOZNANIA/PRZEKAZANIA DOKUMENTU

(Wzór)

Nazwa i numer dokumentu z rejestru

I.p.	Imię i nazwisko	Data zapoznania/ przekazania	Cel zapoznania/przekazania	Data zapoznania/ zwrotu	Podpis
1.					
2.					
3.					
4.					
5.					
6.					
7.					

L.dz. /

Egzemplarz pojedynczy

PROTOKÓŁ

**Z czynności niszczenia kopii Dokumentów/usuwania plików
Dokumentów oznaczonych klauzulą „Tajemnica przedsiębiorstwa”**

Numer

(Wzór)

W dniu _____ komisja w składzie:

1.
2.
3.

przeprowadziła czynności niszczenia kopii/trwałego usuwania plików następujących Dokumentów stanowiących Tajemnicę przedsiębiorstwa:

1.
2.
3.

Niszczenie kopii elektronicznych wersji Dokumentów przeprowadzono na stacji roboczej.....przy wykorzystaniu oprogramowania.....

Na tym protokół zakończono.

Podpisy członków komisji:

1.
2.
3.

TAJEMNICA PRZEDSIĘBIORSTWA

Wykaz rodzajów informacji mogących stanowić Tajemnicę przedsiębiorstwa
InnoBaltica Sp. z o.o.
(Wzór)

L.p.	Zakres informacji	Rodzaj informacji	Uwagi
1.	Informacje Zarządu Spółki	Zarząd Spółki	
2.	Informacje pracownicze	Np. dokumentacja dot. rekrutacji, dane dot. osób upoważnionych do realizacji transakcji z bankami oraz posiadających służbowe karty płatnicze i kredytowe;	
3.	Informacje organizacyjne	Np. protokoły z posiedzeń Rady Nadzorczej oraz WZ Akcjonariuszy, plany zmian struktury organizacyjnej, plany oraz wyniki audytów oraz kontroli wewnętrznych;	
4.	Informacje finansowe	Np. analizy i ewidencje kosztów, kluczowe umowy oraz ich warunki, plany ekonomiczno-finansowe, strategie rozwoju, dane i wyniki analiz przychodów i wyników finansowych;	
5.	Informacje handlowe	Np. informacje zastrzeżone w dokumentacji przetargowej; informacje zastrzeżone jako poufne przez partnerów w dialogu technicznym plany inwestycyjne, dokumentacja finansowa przeznaczona do wiadomości organów nadzorczych i właścicielskich	
6.	Informacje z zakresu ITC	Np. plany sieci teleinformatycznych, dokumentacja bezpieczeństwa systemów i sieci ITC, dokumenty dotyczące	

		bezpiecznej eksploatacji sieci, kody i hasła dostępowe, procedury dot. tworzenia kopii zapasowych, procedury szczegółowe stanowiące załączniki do Instrukcji Zarządzania Systemem Informatycznym itp.	
7.	Informacje z zakresu systemu ochrony fizycznej i bezpieczeństwa informacji	Np. plany ochrony, dane dot. systemów bezpieczeństwa, alarmowych, procedury szczegółowe reagowania stanowiące załączniki do Polityki Bezpieczeństwa, kody dostępu do systemu alarmowego, itp.	
8.	Inne informacje		