PROCEDURA

Projekt

Procedura/Regulamin w zakresie bezpieczeństwa i ochrony informacji

I. Postanowienia ogólne

1. Regulamin określa zasady i sposób ochrony informacji, dokumentów, materiałów i danych oraz infrastruktury informatycznej przed nieuprawnionym ujawnieniem lub dostępem bądź zniszczeniem, jako stanowiących tajemnicę w rozumieniu postanowień niniejszego Regulaminu i podlegających ochronie, a także obejmuje regulację obowiązków zatrudnionych w zakresie:

- używania sprzętu i oprogramowania komputerowego,

- łączenia się z siecią Internet lub innymi sieciami bądź obcymi urządzeniami komputerowymi (informatycznymi) i pocztą elektroniczną,

- używania zewnętrznych nośników, dyskietek i dysków w sprzęcie Spółki oraz zabezpieczenia mienia w tym zakresie.

2. W rozumieniu niniejszego Regulaminu:

- „informacją" objętą tajemnicą jest każda informacja jeżeli jest niejawna, chroniona w tym poufna lub objęta tajemnicą przedsiębiorcy, prywatnością na podstawie RODO lub ustaw szczególnych bądź została zaklasyfikowana / uznana jako wymagająca ochrony przed nieuprawnionym ujawnieniem na mocy postanowień niniejszego Regulaminu, w tym również dane przedsiębiorców – pracowników, kontrahentów i konsumentów (informacje chronione);

- „dokumentem" jest każda utrwalona informacja, stanowiąca tajemnicę w rozumieniu Regulaminu, zwłaszcza na piśmie, mikrofilmach, negatywach i fotografiach, nośnikach do zapisów informacji (nośnikach danych) w postaci cyfrowej i na taśmach elektromagnetycznych, także w formie mapy, wykresu, rysunku, obrazu, grafiki, fotografii, broszury, książki, kopii, odpisu, wypisu, wyciągu i tłumaczenia dokumentu, zbędnego lub wadliwego wydruku, odbitki, kliszy, matrycy i dysku optycznego, kalki, taśmy atramentowej, jak również każda informacja utrwalona na elektronicznych nośnikach danych;

- „materiałem" jest dokument w rozumieniu przedmiotowym oraz przedmiot lub dowolna jego część, w szczególności urządzenie lub wyposażenie, jeżeli zostały objęte ochroną jako stanowiące informacje będące tajemnicą (np. modele, prototypy, itp.);

- „zatrudnionym" jest pracownik, zleceniobiorca, wykonawca lub usługodawca bądź osoby przez nich zatrudnione, świadczące pracę lub usługi w siedzibie i innych lokalach Przedsiębiorcy, spółkach zależnych lub powiązanych;

- „infrastrukturą techniczną/system informatyczny" – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych

zastosowanych w przedsiębiorstwie w celu przetwarzania i ochrony informacji/danych, spełniających wymogi obowiązujących aktów prawnych regulujących zasady gromadzenia i przetwarzania informacji/danych”,

- „nośnikiem informacji / danych” - materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej (płyta Cd, odtwarzacz płyt Cd, pamięć USB, interfejs USB w komputerze, karta micro SD, urządzenia elektroniczne z wbudowaną pamięcią;

- „zabezpieczeniem systemu informatycznego” – wdrożenie właściwych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem informacji/danych, a także ich utratą, w tym stosowanie szyfrowannia i silnego hasła;

- „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 wdrażająca” - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;

- „szyfrowanie” - proces przekształcania tekstu lub informacji w innej postaci (np. zarejestrowanego materiału dźwiękowego lub filmowego) na niezrozumiały ciąg znaków w celu jego utajnienia – przechowywania w takiej postaci lub przekazywania niezabezpieczonymi kanałami;

- „silne hasło” - oznaczenie kodu zabezpieczającego o większej komplikacji (złożoności), który tworzy się z reguły np. do kont bankowych, komputerów firmowych przetwarzających np. dane osobowe lub tajemnice przedsiębiorstwa, systemów operacyjnych, baz czy zbiorów danych;

- „program MDM” - rozwiązanie z zakresu bezpieczeństwa, które dokonują szyfrowania na urządzeniach mobilnych, umożliwia dysponentom urządzenia i działom IT monitorowanie, zarządzanie i zabezpieczanie mobilnego sprzętu wykorzystywanego przez pracowników.

3. Zasadą jest jawność informacji i prawa jej udostępniania, chyba że w trybie tego Regulaminu lub na podstawie ustaw informacja jest niejawna lub objęta tajemnicą z innego tytułu.

4. Spółka zapewnia i realizuje bezpieczeństwo informacji w systemach IT przedsiębiorstwa poprzez zapewnienie:

− poufności informacji/danych – pod którą rozumie się uniemożliwienie dostępu do danych osobom trzecim,

− integralności informacji/danych – pod którą rozumie się zapewnienie dokładności i kompletności informacji/danych i metod ich przetwarzania oraz uniknięcie nieautoryzowanych zmian danych,

− dostępności informacji/danych – pod którą rozumie się zapewnienie dostępu do informacji/danych osobom uprawnionym zawsze wtedy, gdy jest wymagane,

− rozliczalności działań – pod którą rozumie się zapewnienie, że jakiekolwiek działania na danych (przetwarzanie) jest rejestrowane w systemie informatycznym wraz z możliwością identyfikacji tego, kto uzyskał dostęp i/lub dokonał działania.

II. Przedmiot ochrony

Na warunkach tego regulaminu ochroną obejmuje się następujące zakresy i przedmiot:

1.
Chronione w ramach obowiązków publiczno-prawnych

1.1. Sfera prywatności i dobra osobiste (art. 47 Konstytucji, art. 23 Kodeksu cywilnego)

Obowiązek ochrony informacji obejmuje:

- ochronę prawną życia prywatnego, w tym również rodzinnego, czci i dobrego imienia oraz informacje o majątku co pokrywa się z ochroną danych osobowych osób fizycznych regulowaną przez RODO i ustawę wdrażającą (wyciąg z przepisów stanowi załącznik do niniejszego Regulaminu).

Obowiązek ochrony obejmuje:

1) każdą informację, na podstawie której można określić tożsamość danej osoby powiązaną z danymi chronionymi;

2) każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie czyli zbiór danych,

3) przetwarzanie danych w rozumieniu zbierania, utrwalania, przechowywania, opracowywania, zmieniania, udostępniania i usuwania danych, jak również każdej innej operacji przetwarzania wykonywanej w systemach informatycznych, jest możliwe tylko w trybie przewidzianym ustawą o tyle, o ile nie naruszają dobra publicznego, dobra osoby, której dotyczą lub dóbr osób trzecich**,** zgodnie z definicjami RODO.

(wyciąg z przepisów stanowi załącznik do niniejszego Regulaminu).

1.3. Tajemnice według Prawa pracy

Obowiązek ochrony obejmuje:

dokumentację w sprawach związanych ze stosunkiem pracy (wyciąg z przepisów stanowi załącznik do niniejszego Regulaminu).

1) dokumenty urzędowe lub osób prywatnych (rekomendacje, opinie) albo wytworzone przez Spółkę (wyciąg z przepisów stanowi załącznik do niniejszego Regulaminu). dokumenty zgromadzone w związku z ubieganiem się o zatrudnienie,

- dokumenty dotyczące nawiązania stosunku pracy oraz przebiegu zatrudnienia pracownika (karta ewidencyjna czasu pracy, imienna karta/lista wypłacanego wynagrodzenia za pracę i innych świadczeń związanych z pracą),

- dokumenty związane z ustaniem zatrudnienia,

- dokumenty dotyczące karania pracownika i wykroczeń dyscyplinarnych.

2) Oceny pracy, opinie i inne dokumenty, których ujawnienie może naruszyć dobra osobiste pracownika, w tym dane o wynagrodzeniu za pracę, podatkach, w tym PIT-y.

Pokrywa się to z zakresem ochrony z RODO.

1.4. Tajemnica skarbowa (Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa)

Obowiązek ochrony obejmuje w szczególności:

1) dane mieszczące się w składanych przez podatników, płatników i inkasentów deklaracjach i innych dokumentach oraz wszelkie informacje podatkowe przepisane prawem

2) akta spraw prowadzonych przez organy podatkowe i organy kontroli skarbowej

3) informacje przekazane organom podatkowym przez Spółkę o zdarzeniach wynikających ze stosunków cywilno-prawnych albo Prawa pracy w zakresie wymaganym przepisami prawa(wyciąg z przepisów stanowi załącznik do niniejszego Regulaminu).

1.5. Tajemnica bankowa (Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe)

Obowiązek ochrony obejmuje:

1) wszystkie wiadomości dotyczące czynności bankowych i osób będących stroną umowy, uzyskane w czasie negocjacji oraz związane z zawarciem umowy z bankiem i jej realizacją, z wyjątkiem wiadomości, bez ujawnienia których nie jest możliwe należyte wykonanie zawartej przez bank umowy;

2) wszystkie wiadomości dotyczące osób, które nie będąc stroną umowy, o której mowa w pkt. 1, dokonały czynności pozostających w związku z zawarciem takiej umowy, z wyjątkiem przypadków, gdy ustawa przewiduje ujawnienie takich czynności (art. 104 ust. 1 ustawy Prawo bankowe).

2. Chronione w ramach obowiązków prywatno-prawnych.

II.1. Tajemnica przedsiębiorstwa

Obowiązek ochrony obejmuje nie ujawniane do wiadomości publicznej (niepublikowane) informacje techniczne, technologiczne, handlowe lub organizacyjne przedsiębiorstwa (korporacyjne), które u przedsiębiorcy w trybie tego Regulaminu uznano za chronione i objęto tajemnicą przedsiębiorcy.

2.1.1. Rodzaje informacji objętych tajemnicą przedsiębiorstwa:

2.1.2. Informacje techniczne i technologiczne (przemysłowe)

1) **technologie** _____*****

2) dokumentacje _____

3) projekty wzorów użytkowych lub zdobniczych, znaków towarowych, nazw produktów, projektów graficznych do czasu skierowania do produkcji lub rejestracji praw ochronnych lub patentowych,

4) architektura, język i kody źródłowe programów opracowanych i stosowanych w przedsiębiorstwie wraz z hasłami i kodami dostepu,

5) **receptury** _____**.***

2.1.3. Informacje handlowe (tajemnica handlowa)

1) W zakresie zamówień i produkcji wyrobów: _____*,

- ilości zamówionych przez oznaczonych klientów wyrobów,

- wzory użytkowe lub zdobnicze _____

- liczba i adresy oraz dane osobowe klientów,

- zbiory danych dostawców i odbiorców oraz dotyczące reklamacji,

2) W zakresie handlu hurtowego i detalicznego : (jeżeli nie występuje wykreślić)*

- wielkości produkcji i sprzedaży wyrobów poszczególnym klientom,

- treść ofert przeznaczonych dla indywidualnych klientów lub grup klientów,

- treść ofert indywidualnie kierowanych do lub otrzymanych od kontrahentów,

- cen, upustów, bonifikat, rabatów indywidualnie kierowanych do lub otrzymanych od kontrahentów,

- treści negocjacji umów (kontraktów) dostaw surowców i materiałów do Spółki świadczenia usług oraz sprzedaży produktów Spółki oraz wszelka korespondencja handlowa w tym zakresie,

- treść kontraktów podpisanych, w okresie realizacji, o ile Zarząd za zgodą kontrahenta nie zdecydował o upublicznienia,

- wykazy wraz z danymi dotyczące szczegółowej struktury sprzedaży produktów lub zakupu surowców i materiałów,

- _____

1) W zakresie wynajmu, dzierżawy i leasingu maszyn i sprzętu:

- ilość, wartość i ceny,

- treść kontraktów w części zastrzeżonej poufności.

2) W zakresie działalności związanej z prowadzeniem interesów:

- umowy, opinie, ekspertyzy, dokumentacja, wyniki badań i projekty w sprawach doradztwa technicznego w zakresie technologii, inżynierii,

- umowy, opinie, ekspertyzy, dokumentacja, wyniki badań i projekty w zakresie projektowania _____ ,

- umowy, opinie, ekspertyzy, dokumentacja, wyniki badań i projekty w zakresie analiz technicznych, ochrony środowiska, bhp, prawa wodnego, odpadów, przepisów przeciwpożarowych,

- dane związane z własną lub zleconą działalnością w zakresie inwigilacji i ochrony,

- umowy kredytowe,

- dane związane z zakresem ubezpieczeń osobowych i majątkowych.

W umowach zawieranych z kontrahentami/podmiotami zewnętrznymi Spółka zapewnia stosowanie właściwych klauzul/postanowień zobowiązujących do ochrony danych udostępnionych przez Spółkę podlegających zastrzeżeniu jako tajemnice przedsiębiorstwa w

rozumieniu niniejszego Regulaminu. Z podmiotami będącymi Partnerami Zaufanymi w rozumieniu Polityki Bezpieczeństwa, zawierane są odpowiednie Umowy w zakresie stałej współpracy lub świadczenia usług na warunkach RODO.

2.1.4. Informacje organizacyjne:

- szczegółowa struktura organizacyjna przedsiębiorstwa, ujawniająca zakres instytucjonalny i funkcjonalny kontroli i nadzoru, komórek organizacyjnych i stanowisk,

- struktura sprzedaży w rozbiciu na klientów,

- reklamacje i spory związane z jakością wyrobów, opinie i badania w tym zakresie oraz spory związane z zapłatą lub wykonaniem świadczeń z umów.

2.2.Tajemnice korporacyjne:

1) Decyzje Przedsiębiorcy (Zarządu) w przedmiocie :

- określenia znaków towarowych – logo, nazwy własnej firmy, jego zmiany do czasu rejestracji, udzielenie licencji i pozwolenia na używanie przez osoby trzecie w ramach umów franchisingowych lub innych do czasu realizacji,

- wynagrodzenia członków **Kierownictwa/ dyrektorów/ menedżerów*** do czasu zawarcia umów i upublicznienia,

- regulaminu zarządzania lub zarządu w części dotyczącej warunków wykonywania funkcji Dyrektora lub przez członka Zarządu do czasu upublicznienia,

- sposobu prowadzenia oddziałów, zakładów i przedstawicielstw w zakresie wyodrębnienia rachunkowego i majątkowego.

2) Decyzje Przedsiębiorcy i Zarządu dotyczące:

- struktury organizacyjnej przedsiębiorstwa do czasu jej wejścia w życie,

- zaciągania kredytów,

- zbywania i nabywania majątku trwałego o wartości przekraczającej równowartość _____- euro,

- bilansów, rachunków zysków i strat do czasu ich przedłożenia na Walne Zgromadzenie lub zatrudnienia przez Przedsiębiorcę,

- sprawozdań z działalności przedsiębiorstwa do czasu ich publikacji,

- planu kont i zasad rachunkowości.

3) Projektów Umów o wykonywanie funkcji i kontrakty menedżerskie kadry kierowniczej oraz Partnerami Zaufanymi:

4) Projektów Decyzji (postanowień, zarządzeń) w przedmiocie:

- projektów dopłat, nabycia lub umorzeń udziałów, akcji, podwyższania kapitału (do czasu uchwalenia przez Zarząd i upublicznienia),

- zasad utworzenia i wykorzystania funduszów celowych i darowizn oraz sponsoringu,

- projektów rocznych planów finansowych, marketingu, inwestycji do czasu uchwalenia i upublicznienia,

- planów i projektów co do wyborów i odwoływania oraz wynagradzania członków organów spółki lub zespołów doradczych.

5) Dane dostępowe do systemów IT (loginy, hasa, kody).

III. Zakres podmiotowy zobowiązanych do ochrony

1.
Osobami zobowiązanymi do ochrony, organizacji i nadzoru nad zabezpieczeniem informacji chronionych i bezpieczeństwem informatycznym w rozumieniu niniejszego Regulaminu są:

1) **Dyrektor Naczelny/ Zarząd** *- od chwili jego powołania,

2) Rada Nadzorcza - od chwili jej powołania przez Zgromadzenie,

3) Dyrektorzy (kierownicy) terenowych jednostek organizacyjnych (oddziały, zakłady itp.) powołani na podstawie uchwały Zarządu,

4) Pełnomocnik lub pracownik ds. ochrony informacji i bezpieczeństwa informatycznego.

1.

Osoby zobowiązane mają obowiązek zapewnienia ochrony informacji chronionych, w tym dokumentów, materiałów i danych na zasadach i w oparciu o postanowienia niniejszego Regulaminu.

2.

Zatrudnionymi zobowiązanymi do stosowania się do obowiązków wynikających z Regulaminu są osoby fizyczne zatrudnione także na podstawie Umów: agencyjnej, o dzieło, pośrednictwa, akwizycji lub innej umowy mieszanej i nienazwanej z której wynika obowiązek wykonywania dla Spółki lub w jej imieniu czynności prawnych lub faktycznych lub prawo przebywania na terenie obiektów Spółki lub dostęp do sieci teleinformatycznej Spółki.

3.
Kontrahentem zobowiązanym do stosowania się do obowiązków wynikających z Regulaminu są Partnerzy Zaufani i podmioty gospodarcze lub inne osoby prawne lub jednostki organizacyjne (spółki osobowe), które przyjmują do wykonywania prace na terenie przedsiębiorstwa (zakładów, oddziałów) Spółki lub uzyskują dostęp do ksiąg lub dokumentów Spółki bądź do sieci teleinformatycznej Spółki.

IV. Klasyfikacja i oznaczenia informacji chronionej

1.

Podział i oznaczenia:

2.

Dobra osobiste, prywatność, akta pracownicze, dane osobowe – Zastrzeżone Z

3.

Tajemnica skarbowa i bankowa – Zastrzeżone TS

4.

Tajemnica Przedsiębiorcy (handlowa, przemysłowa, organizacyjna) – Zastrzeżone TP

5.
Tajemnica korporacyjna (władz Spółki) – Zastrzeżone TK.

2. Wyznaczone osoby zobowiązane mają obowiązek w zakresie pozostającym w ich kompetencji wprowadzić i przestrzegać oznaczenia akt, danych i dokumentów oznaczeniami informacji chronionej (zastrzeżonej) i odpowiednio zabezpieczać te dokumenty, bazy danych, nośniki informacji jak i dostęp do systemów teleinformatycznych. W szczególności stosować Politykę Bezpieczeństwa Informacji.

3. Dokumenty, akta, dane objęte klauzulą informacji chronionej mogą być udostępnione, prowadzone, przekazywane tylko osobom posiadającym dostęp do danego typu informacji chronionej. Dotyczy to informacji, zbiorów i dokumentów bez względu na formę zapisu i nośnik informacji.

4. Osoby prowadzące akta, dokumentację, sprawy i czynności podlegające ochronie, sporządzają rejestr tych akt, dokumentów, spraw w formie pisemnej niezależnie od baz danych w systemach teleinformatycznych.

5. Do obowiązków osoby odpowiedzialnej za ochronę informacji wyznaczonej przez Prezesa Zarządu należy:

1) przedkładanie otrzymywanej korespondencji i przekazywanie jej upoważnionym pracownikom zgodnie z dekretacją oraz jej przechowywanie,

2) sprawowanie nadzoru nad pracą osób upoważnionych do sporządzania, powielania, fotografowania, skanowania dokumentów zawierających informacje chronione itp.

3) nadzorowanie pracy osób wyznaczonych do doręczania przesyłek zawierających informacje chronione oraz ich przechowywanie,

4) nadzorowanie, aby pracownicy po zakończeniu pracy zwracali dokumenty i materiały zawierające informacje chronione, wyłączali sprzęt informatyczny i wylogowali się po zakończeniu lub przerwaniu pracy.

6. **Przedsiębiorca/ Dyrektor Naczelny** * może na wniosek pracownika zdjąć lub zmienić klauzulę ochrony bądź wyrazić zgodę na udostępnianie danej informacji lub dokumentu konkretnie oznaczonej osobie.

V. Dostęp do informacji chronionej, bezpieczeństwo informatyczne.

1. Każdy pracownik lub osoba zatrudniona na podstawie innego stosunku umownego przez przystąpieniem do wykonywania obowiązku podpisuje Oświadczenie stanowiące Załącznik nr.1. Przedsiębiorca / Zarząd / Dyrektor zapewnia okresowe szkolenia pracowników w zakresie bezpieczeństwa informatycznego.

2. Osoby, które uzyskują dostęp do informacji chronionej otrzymują upoważnienie o treści stanowiącej Załącznik nr 2 oraz podpisują Deklarację stanowiącą Załącznik nr 3.

Otrzymany poziom dostępu do informacji chronionych może być w każdym czasie zmieniony i nie stanowi zmiany warunków pracy w rozumieniu prawa pracy.

3. Decyzje o zakresie dostępu do informacji chronionej podejmuje **Przedsiębiorca/ Dyrektor Naczelny.***

Zakres dostępu do informacji chronionej pracowników stanowi tajemnicę organizacyjną.

4. Zatrudnieni w przedsiębiorstwie mogą posługiwać się na terenie jej przedsiębiorstw **(i spółek zależnych lub powiązanych)*** w sprawach przedsiębiorstwa wyłącznie sprzętem i oprogramowaniem zakupionym przez Przedsiębiorcę, chyba że właściwy członek Zarządu Spółki udzieli indywidualnej zgody na korzystanie z konkretnego obcego sprzętu lub oprogramowania, w innych sprawach w określonym przypadku i czasie. Każdy zatrudniony zobowiązany jest do ochrony swoich danych dostępowych do systemu informatycznego przedsiębiorstwa, w tym hasła dostępu poprzez jego nieprzekazywanie nieuprawnionym osobom trzecim, ochronę przed nieuprawnionym dostępem czy kradzieżą przez osoby trzecie.Zatrudnieni, którzy uzyskują dostęp do sprzętu teleinformatycznego, którym powierza się sprzęt komputerowy lub obsługę poczty elektronicznej, podpisują umowy według wzoru stanowiącego załącznik nr 4 do niniejszego Regulaminu. Wszystkie osoby, które upoważnione są do udostępniania informacji/danych są zobowiązane do stosowania Instrukcji udostępniania/przekazywania informacji/danych.

5.Stacje robocze podlegają zabezpieczeniu przed nieautoryzowanym dostępem osób trzecich. Własny sprzęt komputerowy (informatyczny), oprogramowania, dyski i dyskietki oraz inne urządzenia peryferyjne Zatrudnionego lub osób trzecich mogą być wnoszone na teren przedsiębiorstwa Spółki lub łączone bądź wykorzystywane do/w sprzęcie Spółki wyłącznie za zgodą właściwego członka Zarządu wydaną indywidualnie, odrębnie dla każdego przypadku jednorazowo. Ten sam tryb obowiązuje w przypadku przenoszenia niezabezpieczonych danych poza teren przedsiębiorstwa na nośnikach elektronicznych (pendrive, nośniki CD, etc.).

6.Łączenie się z siedziby przedsiębiorstwa Spółki lub innych jej lokali przy użyciu sprzętu, łączy, sieci Spółki z siecią Internet, pocztą elektroniczną, innymi sieciami lub użytkownikami jest dozwolone wyłącznie w zakresie, w miejscach i przy użyciu sprzętu zintegrowanego Spółki na który jest stała autoryzacja lub wydał na to zgodę właściwy członek Zarządu Spółki. Korzystanie z systemu informatycznego przedsiębiorstwa w celach prywatnych jest niedozwolone.

7.Każdorazowe zalogowanie się, wejście do sieci wewnętrznej Spółki, wyjście z niej na zewnątrz, instalowanie programów, wprowadzanie danych z dysków lub dyskietek musi być poprzedzone sprawdzeniem i zapewnieniem, że jest zainstalowany i działa odpowiedni program antywirusowy zabezpieczający urządzenia i sieci Spółki oraz dane przed utratą lub uszkodzeniem. Każdy przypadek wykrycia lub podejrzenia obecności „wirusa" należy zgłaszać odpowiednim służbom informatycznym (tu : _____).

8. W przedsiębiorstwie stosuje się następujące kategorie środków zabezpieczeń danych:

- zabezpieczenia fizyczne, w tym sposób i miejsce przechowywania elektronicznych nośników informacji/danych, kopii zapasowych,

- zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej,

- zabezpieczenia informatyczne, które szczegółowo określa odrębny dokument w postaci Regulaminu/procedury/polityki bezpieczeństwa informatycznego w Spółce,

- zabezpieczenia organizacyjne, w tym wykonywanie okresowych przeglądów i konserwacji systemu informatycznego oraz nośników informacji/danych (w tym tradycyjnych), jak również ich likwidacji.

9. W ramach zabezpieczenia danych ochronie w przedsiębiorstwie podlegają:

- infrastruktura informatyczna, w tym sprzęt komputerowy, serwery, komputery osobiste (laptopy), drukarki i inne urządzenia zewnętrzne,

- oprogramowanie, w tym kody źródłowe, programy, systemy operacyjne, narzędzia programowe,

- dane zapisane na dyskach i dane podlegające przetwarzaniu w systemie informatycznym,

- hasła użytkowników, które powinny być okresowo zmieniane i przechowywane w formie zaszyfrowanej,

- pliki dziennych operacji systemowych i baz danych, kopie zapasowe i archiwa,

- użytkownicy i administratorzy obsługujący i używający system,

- dokumentacja – zawierająca dane systemu, techniczna,

- wydruki,

- związana z przetwarzaniem danych dokumentacja papierowa, z której dane są wprowadzane do systemu informatycznego albo funkcjonują niezależnie od niego.

10. W systemie informatycznym przedsiębiorstwa obowiązują zabezpieczenia na poziomie wysokim z uwzględnieniem przepisów Rozporządzenia MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004 Nr 100, poz. 1024), Rozporządzenia Ministra administracji i cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. z 2015 r. poz. 745) i Rozporządzenia Ministra administracji i cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U. z 2015 r. poz. 719).

11. Podstawowymi stosowanymi środkami zabezpieczania danych w systemie informatycznym przedsiębiorstwa są:

- hasła dostępu do systemu,

- hasła dostępu do aplikacji,

- wygaszacze ekranu,

- stopniowanie uprawnień,

- stosowanie kilku technik/narzędzi ochrony antywirusowej, w tym oprogramowania antywirusowego, systemu typu firewall, odpowiedniej konfiguracji i aktualizacji używanych programów,

- okresowe archiwizowanie danych na wypadek awarii (kopie zapasowe) wraz z cyklicznym audytem co do możliwości odtworzenia danych.

VI. Organizowanie posiedzeń Zarządu, Rady Nadzorczej oraz Zgromadzenia Wspólników (dotyczy spółek prawa handlowego).

1. Członek Zarządu odpowiedzialny w Spółce za ochronę informacji chronionych oznacza jakie sprawy rozpatrywane przez Zarząd zawierają informacje chronione i jakie dokumenty, uchwały, protokoły zostaną uznane za objęte ochroną ze względu na objęcie tajemnicą w Spółce.

1.1.Materiały na posiedzenie Zarządu, Rady Nadzorczej lub Zgromadzenia Wspólników stanowiące informacje chronione do czasu publikacji są sporządzane, oznaczane i przechowywane oddzielnie w trybie właściwym dla takich informacji.

1.2.W porządku obrad oznacza się, które z punktów porządku obrad zawierają informacje chronione i obrady będą się odbywać z wyłączeniem jawności.

1.3.Właściwe części protokołu, o ile zawierają informacje chronione, są obejmowane poufnością i ogólnie dostępny może być jedynie wyciąg z protokołu obejmujący całość obrad z pominięciem zagadnień i treści objętych poufnością z zaznaczeniem tego faktu.

1.4.Akta Zarządu obejmujące protokoły z posiedzeń Zarządu są w całości uznane za informacje chronione i mogą być udostępniane wyłącznie Radzie Nadzorczej i państwowym organom kontroli chyba, że Zarząd podejmie decyzję o upublicznieniu.

2. W posiedzeniach Zarządu, Rady Nadzorczej, zwanych dalej posiedzeniami, na których mają być omawiane zagadnienia stanowiące informacje chronione mogą brać udział wyłącznie osoby upoważnione do dostępu do informacji, które będą przedmiotem obrad.

2.1. Za ochronę informacji w zakresie organizacyjnego przygotowania posiedzeń oraz w zakresie ich dokumentowania odpowiedzialny jest Pełnomocnik Zarządu ds. ochrony informacji i bezpieczeństwa informatycznego.

2.2. Uczestnikom posiedzenia przekazuje się wyłącznie informacje niezbędne, a przewodniczący posiedzenia w porozumieniu z _____ zastrzega sprawy, których nie wolno utrwalać.

2.3. Uczestnikom posiedzenia _____ zapewnia możliwość przechowywania dokumentów zawierających informacje chronione w przerwach obrad i po ich zakończeniu.

2.4. Po zakończeniu posiedzenia uczestnicy zobowiązani są przekazywać dokumenty zawierające informacje chronione _____.

1.
Taśma magnetofonowa, magnetowidowa itp., z zarejestrowanym zapisem z przebiegu posiedzenia, powinna być opieczętowana i przechowywana jako objęta ochroną na podstawie postanowień Regulaminu w zakresie ochrony informacji.

3.1._____ wyraża pisemną zgodę w przypadku konieczności odtworzenia zapisu z przebiegu posiedzenia.

3.2.Skasowania zapisu lub zniszczenia taśmy dokonuje się na podstawie decyzji _____.

VII. Kontrola i nadzór

Jakiekolwiek podejrzenie naruszenia bezpieczeństwa informatycznego w przedsiębiorstwie podlega niezwłocznemu zgłoszeniu (powiadomieniu) ustnie lub za pośrednictwem poczty elektronicznej do Zarządu Spółki.

1.Kontrola instytucjonalna

1.1. Kontrolę instytucjonalną sprawują członkowie Kierownictwa według kompetencji w zakresie spraw, które są im powierzane do prowadzenia i odpowiedzialności oraz wyznaczeni pracownicy, o których mowa w pkt.4.5. cz. IV Regulaminu.

1.2. _____- (lub osoba przez niego wyznaczona) zobowiązany jest dokonywać bieżącej kontroli stanu zabezpieczenia informacji chronionych, a zwłaszcza obiegu, przechowywania dokumentów i materiałów zawierających informacje niejawne.

1.3. _____ zobowiązany jest co najmniej raz w roku, nie później niż do 31 stycznia, powołać komisje spośród pracowników upoważnionych do dostępu do chronionych informacji - celem przeprowadzenia kontroli stanu ochrony, w tym głównie w zakresie prawidłowego stosowania i przestrzegania postanowień Regulaminu.

1.4. Kontrole doraźne w zakresie ochrony może przeprowadzić każdy członek Kierownictwa.

1.5. Komisja po przeprowadzeniu szczegółowej kontroli zobowiązana jest w terminie nie później niż do 31 marca sporządzić protokół, który przedstawia do zatwierdzenia **Przedsiębiorcy/ Dyrektorowi Naczelnemu Zarządowi*.**

1.6. W przypadku stwierdzenia jakichkolwiek uchybień podlegają one usunięciu w terminie wyznaczonym przez _____.

1.7. Przeprowadzenie kontroli stanu ochrony informacji (audyt bezpieczeństwa informatycznego) może nastąpić w każdym czasie z inicjatywy Zarządu.

1.8. Kontrole stanu ochrony informacji, o których mowa wyżej, nie uchybiają uprawnieniom Przedsiębiorcy lub organów nadzoru w tym względzie.

2. Kontrola funkcjonalna

2.1. Kontrolę funkcjonalną sprawują wszyscy kierownicy jednostek organizacyjnych zgodnie ze swoimi zakresami obowiązków w ramach bieżącego nadzoru.

2.2. Niezależnie od obowiązków w nadzorze, o których mowa wyżej, kontrolę funkcjonalną sprawują:

- w zakresie spraw pracowniczych, ochrony dóbr osobistych, prywatności i danych osobowych _____;

- w zakresie tajemnicy skarbowej, statystycznej i bankowej _____;

- w zakresie tajemnicy przedsiębiorstwa (przemysłowej, handlowej, organizacyjnej) i korporacyjnej _____ .

2.3. Fakt przeprowadzenia kontroli powinien być stwierdzony co najmniej wzmianką i podpisem na dokumencie, a w przypadku koniecznym sporządzony protokół.

2.4. W ramach kontroli funkcjonalnej może być dokonywana zmiana kwalifikacji ochrony, o czym należy powiadomić właściwego Kierownika/ Dyrektora/ Przedsiębiorcę, który może wyrazić sprzeciw w tym zakresie.

3. Odpowiedzialność i kary

3.1. Naruszenie obowiązków wynikających z niniejszego Regulaminu oraz umowy zawartej z pracownikiem, stanowi rażące naruszenie obowiązków pracowniczych i będzie upoważniać Przedsiębiorcę do dochodzenia naprawienia szkody majątkowej albo zapłaty kary pieniężnej zgodnie z Regulaminem pracy lub kary umownej w przypadku umów cywilno-prawnych w wysokości _____

VIII. Wprowadzenie Regulaminu

1. Regulamin został przyjęty za uchwałą/ zarządzeniem/ postanowieniem* nr _____ z dnia _____**Przedsiębiorcy/ Dyrektora Zarządu*** Spółki i obowiązuje od dnia _____.

2. Do dnia wejścia w życie Regulaminu dyrektorzy, prokurenci i kierownicy komórek organizacyjnych wprowadzą oznaczenia akt, dokumentów, zbiorów danych właściwymi oznaczeniami i powierzą prowadzenie konkretnym pracownikom.

3. Do dnia _____ kierownicy komórek organizacyjnych w zakresie podległych pracowników, a Dyrektorzy i prokurenci w zakresie podległych im kierowników wystąpią do **Przedsiębiorcy/ Dyrektora Naczelnego/ Zarządu** *o przyznanie dostępu imiennie wskazanym osobom do konkretnych informacji i wydanie upoważnień.

4. Wykonanie obowiązków związanych z zastosowaniem Regulaminu i nadzór w tym zakresie powierza się _____ (odpowiedzialny członek Kierownictwa).