ZAKŁADOWY REGULAMIN PRACY

STOWARZYSZENIE "ROZWÓJ BUKOWINY"

84-311 Bukowina 5

20 Sierpień 2018r.

Uchwałą Zarządu Stowarzyszenia z dnia 20.08.2018r. Regulaminowi Pracy wraz z załącznikami nadaje się treść jak w załączeniu.

Egzemplarz nr 2

Spis Treści:

Załączniki do Zakładowego Regulaminu Pracy :

REGULAMIN PRACY

Rozdział I

Postanowienia ogólne

§ 1.

Podstawę prawną ustalania regulaminu pracy stanowią przepisy:
Art. 104, art. 104^1 - 104 Kodeksu Pracy i przepisy wykonawcze wydane na ich podstawie ,
(Dz. U. Nr 24 , póź. 141 z 1974 r. z późniejszymi zmianami – Dz. U. Nr. 213 , poz. 2081 z 2003 r.)

§ 2.

Regulamin pracy jest aktem normatywnym ustalającym organizację i porządek w procesie pracy oraz związane z tym prawa i obowiązki pracodawcy i pracowników w Stowarzyszeniu "Rozwój Bukowiny" w Bukowinie.

§ 3.

Zgodnie z ustawą z 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych (tekst jednolity opracowano na podstawie : DzU. Z 1996 r.: Nr. 70 , poz. 335 , Nr. 118 , poz. 561 , Nr. 139 , poz. 647 , Nr. 147 , poz. 686 ; Dz. U. z 1997 r.: Nr. 82 , poz. 518 , Nr. 121 , poz. 770 ; Dz. U. z 1998 r. Nr. 75 , poz. 486, Nr. 113 , poz. 717 ; Dz. U. z 2002 r.: Nr. 135 , poz 1146 ; Dz. U. z 2003 r. : Nr. 213 , poz. 2081 ; Dz. U. z 2005 r. : Nr. 249 , poz. 2104 oraz późniejszymi zmianami) i ustawą z dnia 26 czerwca 1974 r. (Dz.U. Nr. 24 , poz. 141 z późniejszymi zmianami) zwaną Kodeksem Pracy.

Ponieważ w zakładzie pracownicy nie są objęci układem zbiorowym pracy Pracodawca :

1.Nie będzie tworzył Zakładowego Funduszu Świadczeń Socjalnych.

2.Pracodawca nie wypłaca świadczenia urlopowego.

§ 4.

Siedzibą Zakładu jest miejscowość Bukowina.
Adres: 84-311 Bukowina 5

§ 5.

1.Postanowienia niniejszego regulaminu pracy obejmują wszystkich pracowników zatrudnionych w zakładzie pracy , bez względu na rodzaj wykonywanej pracy i zajmowane stanowisko.
2.Wykaz stanowisk w Zakładzie stanowi załącznik nr.1

§ 6.

Pracodawca zapoznaje z treścią regulaminu pracy każdego przyjmowanego do pracy pracownika przed rozpoczęciem przez niego pracy , a pracownik potwierdza znajomość regulaminu swoim podpisem w treści umowy o pracę.

§ 7.

W sprawach nieuregulowanych w niniejszym regulaminie stosuje się przepisy kodeksu pracy i inne przepisy prawa pracy.

Rozdział II

§ 8.

Obowiązki Pracodawcy

Pracodawca jest obowiązany w szczególności:
1) zaznajamiać pracowników podejmujących pracę z zakresem ich obowiązków, sposobem wykonywania pracy na wyznaczonych stanowiskach oraz ich podstawowymi uprawnieniami,
2) organizować pracę w sposób zapewniający pełne wykorzystanie czasu pracy, jak również osiąganie przez pracowników, przy wykorzystaniu ich uzdolnień i kwalifikacji, wysokiej wydajności i należytej jakości pracy,
3) organizować pracę w sposób zapewniający zmniejszenie uciążliwości pracy, zwłaszcza pracy monotonnej i pracy w ustalonym z góry tempie,
4) przeciwdziałać dyskryminacji w zatrudnieniu, w szczególności ze względu na płeć, wiek, niepełnosprawność, rasę, religię, narodowość, przekonania polityczne, przynależność związkową, pochodzenie etniczne, wyznanie, a także ze względu na zatrudnienie na czas określony lub nieokreślony albo w pełnym lub w niepełnym wymiarze czasu pracy,

5) zapewniać bezpieczne i higieniczne warunki pracy , zapewnić ochronę przeciwpożarową oraz prowadzić systematyczne szkolenie pracowników w zakresie bhp i p.poż.
6) terminowo i prawidłowo wypłacać wynagrodzenie,
7) w miarę możliwości zakładu i bez negatywnego skutku na funkcjonowanie zakładu ułatwiać pracownikom podnoszenie kwalifikacji zawodowych,
8) stwarzać pracownikom podejmującym zatrudnienie po ukończeniu szkoły prowadzącej kształcenie zawodowe lub szkoły wyższej warunki sprzyjające przystosowaniu się do należytego wykonywania pracy,
9) zaspokajać w miarę posiadanych środków socjalne potrzeby pracowników,
10) stosować obiektywne i sprawiedliwe kryteria oceny pracowników oraz wyników ich pracy,
11) prowadzić dokumentację w sprawach związanych ze stosunkiem pracy oraz akta osobowe pracowników,
12) wpływać na kształtowanie w zakładzie pracy zasad współżycia społecznego,
13) przeciwdziałać mobbingowi,
14) udostępnić pracownikom tekst przepisów dotyczących równego traktowania w zatrudnieniu.
15) informować pracowników o możliwości zatrudnienia w pełnym lub w niepełnym wymiarze czasu pracy.

§ 9.

1.Pracodawca nie ponosi odpowiedzialności za przechowywane przez pracownika w zakładzie pracy lub miejscu wykonywania pracy pieniądze i przedmioty wartościowe.
2.Pracodawca ma prawo do rejestracji terenu i pomieszczeń przez system monitorujący (kamery i inne środki zapisu) w obrębie całego zakładu pracy.

§ 10.

Dokumentacja personalna Kandydata do pracy powinna obejmować:
1.Świadectwo ukończenia szkoły , lub dokument potwierdzający kwalifikacje zawodowe
2.Świadectwa pracy z poprzednich miejsc zatrudnienia
3.Kwestionariusz osobowy
4.Dokumenty uprawniające do podjęcia pracy na danym stanowisku w myśl odrębnych przepisów.

§ 11.

1.Przed przystąpieniem do pracy pracownik powinien być zaznajomiony z:
a) przepisami w zakresie bhp i p.poż
b) z warunkami pracy i wynagradzania
c) zakresem przydzielonych obowiązków i odpowiedzialności
d) z regulaminem pracy
2. Ponadto pracownik zatrudniony na stanowisku obsługi przed podjęciem pracy powinien:
a) otrzymać odzież i obuwie robocze
b) posiadać aktualne badania lekarskie (w przypadku kontaktu z żywnością) i brak przeciwwskazań do pracy na danym stanowisku.

§ 12.

1.Pracodawca jest obowiązany prowadzić ewidencję czasu pracy uwzględniającą pracę w porze nocnej i godzinach nadliczbowych.
2.Pracodawca udostępnia tę ewidencję pracownikowi na jego pisemne żądanie

Rozdział III

Obowiązki Pracownika

§ 13.

Podstawowym obowiązkiem pracownika jest stosowanie się do poleceń przełożonych oraz sumienne i staranne wykonywanie swoich obowiązków szczegółowo opisanych w odrębnych umowach, a także w Statucie Zespołu Szkolno - Przedszkolnego.
2. Czas pracy należy wykorzystywać w pełni na pracę zawodową.
3. Czas pracy Pracowników określa i przekazuje do wiadomości Dyrektor Zespołu lub Zarząd Stowarzyszenia
4. Pracownik jest obowiązany w szczególności:
a) rzetelnie i efektywnie wykonywać pracę,
b) przestrzegać porządku w zakładzie pracy, a w szczególności ustalonego czasu pracy,

Keller

c) przestrzegać przepisy oraz zasady bhp i przepisów ppoż.
d) poddawać się wstępnym, okresowym i kontrolnym oraz innym zaleconym badaniom lekarskim i stosować się do wskazań lekarskich,
e) przestrzegać tajemnicy określonej w odrębnych przepisach oraz w zakresie ochrony danych osobowych,
f) dbać o dobro zakładu pracy, chronić mienie pracodawcy oraz zachować w tajemnicy informacje, których ujawnienie mogłoby narazić pracodawcę na szkodę,
g) przestrzegać zasad współżycia społecznego,
h) przestrzegać zakazu palenia wyrobów tytoniowych oraz picia alkoholu w obrębie całego Zakładu Pracy,
i)niekorzystania z telefonów służbowych dla celów prywatnych. Ponadto pracownik ma obowiązek pokryć koszty prywatnych połączeń telefonicznych na podstawie billingów udostępnionych przez pracodawcę.
j)niewysyłania prywatnych e-maili , sms-ów oraz niewykonywania prywatnych rozmów telefonicznych z prywatnego telefonu pracownika.
k) stosować się do wszystkich postanowień Statutu Zespołu Szkolno - Przedszkolnego w Bukowinie

§ 14.

Ciężkim naruszeniem podstawowych obowiązków pracowniczych w rozumieniu art. 52 par. 1 pkt 1 k.p. jest:
1) złe lub niedbałe wykonywanie pracy, które mogłoby narazić pracodawcę na szkodę,
2) rażąca niedbałość o powierzone materiały , sprzęt i wyposażenie,
3) wykonywanie w czasie pracy prac niezwiązanych ze stosunkiem pracy,
4) prowadzenie działań destabilizujących pracę Zespołu i Pracodawcy,
5) nieusprawiedliwione nieprzybycie do pracy, częste spóźnianie się lub samowolne opuszczenie pracy bez usprawiedliwienia,
6) stawienie się do pracy w stanie nietrzeźwości lub po spożyciu innego środka odurzającego lub spożywanie alkoholu lub innego środka odurzającego w miejscu pracy,
7) uporczywe naruszanie przepisów i zasad bhp oraz przepisów ppoż,
8) wykonywanie pracy zarobkowej w okresie orzeczonym w zwolnieniu lekarskim niezdolności do pracy lub zawinione wykorzystywanie zwolnienia lekarskiego od pracy w sposób rażąco niezgodny z jego celem,
9) działania lub zachowania uznane w kodeksie pracy za mobbing.

§ 15

Naruszeniem obowiązków pracowniczych jest w szczególności:
1) niewykonywanie lub niedbałe wykonywanie obowiązków pracowniczych,
2) naruszenie tajemnicy państwowej, służbowej lub tajemnicy zakładu pracy jak również w zakresie ochrony danych osobowych lub niedbalstwo w ochronie tych tajemnic,
3) zakłócenie porządku i spokoju w miejscu pracy,
4) niewłaściwe zachowanie wobec przełożonych, podwładnych, współpracowników pracodawcy,
5) nieprzestrzeganie przepisów i zasad bhp oraz przepisów ppoż.

§ 16

1. W razie podejrzenia lub stwierdzenia naruszenia przez pracownika obowiązku trzeźwości, bezpośredni przełożony pracownika ma obowiązek nie dopuścić go do wykonywania pracy i przebywania na terenie zakładu pracy.
2. Pracownik ma obowiązek poddać się kontroli na zawartość alkoholu na każde żądanie Pracodawcy lub osoby przez niego wyznaczonej.

§ 17

1.Pracownik ma obowiązek niezwłocznie zawiadomić pisemnie pracodawcę o wszelkich zmianach w stanie rodzinnym, warunkujących nabycie lub utratę uprawnień do właściwych świadczeń.
2. Pracownik ma obowiązek niezwłocznie zawiadomić pracodawcę o istotnych zmianach swoich danych osobowych, a w szczególności o zmianie nazwiska, adresu zamieszkania oraz danych osoby, które należy zawiadomić w razie wypadku przy pracy.

§ 18

Pracownik jest zobowiązany do nieprowadzenia działalności destabilizującej wobec pracodawcy oraz stosować się do postanowień Statutu Zespołu Szkolno - Przedszkolnego

Keller

Rozdział IV

Organizacja pracy

§ 19

1. Czasem pracy jest czas , w którym pracownik pozostaje w dyspozycji pracodawcy w zakładzie pracy lub w innym miejscu wyznaczonym przez Pracodawcę.
2. Czas pracy powinien być tak zorganizowany przez pracodawcę aby mógł być w pełni wykorzystany na pracę zawodową pracownika.

§ 20

1. Pracownik może opuścić miejsce pracy wyłącznie za zgodą Pracodawcy.
2. Pracownik może przebywać na terenie zakładu pracy poza godzinami pracy wyłącznie za zgodą Pracodawcy.
3. Samowolna zmiana stanowiska pracy jest niedopuszczalna
4. Po zakończeniu pracy pracownik obowiązany jest zabezpieczyć sprzęt, materiały, dokumenty lub podobne przedmioty wykorzystywane w pracy i pozostawić miejsce pracy w należytym porządku.
5. Wykonywanie jakichkolwiek prac na rachunek prywatny na terenie zakładu pracy także poza godzinami pracy jest dopuszczalne wyłącznie za pisemną zgodą pracodawcy.

§ 21

W zakładzie ustala się system pracy gdzie norma dobowa czasu pracy na jeden wymiar wynosi przeciętnie 8 godzin, tygodniowo – 40 godzin ; w pięciodniowym tygodniu pracy ; w systemie pracy równoważnym – dopuszczającym przedłużenie dobowego wymiaru czasu pracy – gdzie zwiększony czas pracy skutkuje krótszym czasem pracy w trzymiesięcznym okresie rozliczeniowym.

§ 22

Pracodawca może dla wszystkich lub niektórych pracowników:
1.Zmienić ustalony w regulaminie pracy wymiar i rozkład czasu pracy
2.Wprowadzić zmianowy system czasu pracy

§ 23

1.Pracownik potwierdza przybycie do pracy poprzez podpisanie listy obecności
2.Pracownik jest obowiązany do podjęcia pracy w określonym przez Pracodawcę czasie wg. uzyskanej od Pracodawcy informacji wywieszonej w ogólnodostępnym miejscu w siedzibie Pracodawcy.

§ 24

1.Praca w Zakładzie może odbywać się zmianowo przez całą dobę od poniedziałku do niedzieli w pięciodniowym tygodniu pracy w okresie rozliczeniowym trzymiesięcznym.
2. Sobota i niedziela może być normalnym dniem pracy
3. O dniu wolnym na kolejny tydzień Pracodawca informuje pracownika ustnie.

§ 25

1.Praca nocna obejmuje 8 godzin i trwa od 21.00 do 5.00
2.Pracownikowi wykonującemu pracę w porze nocnej przysługuje dodatkowe wynagrodzenie za każdą godzinę pracy w porze nocnej w wysokości 20 % stawki godzinowej wynikającej z minimalnego wynagrodzenia.

§ 26

Przerwa w pracy na spożycie posiłku jest udzielana po przepracowaniu co najmniej 4 godzin , trwa 15 minut . Czas przerwy wg. przepisów K.P. – wlicza się do czasu pracy.

§ 27

Niedziele i święta określone odrębnymi przepisami są dniami wolnymi od pracy.
Za pracę w niedzielę oraz święta uważa się pracę wykonywaną pomiędzy godziną 00.00 w tym dniu ,a godziną 00.00 dnia następnego.

§ 28

Pracownikowi , który na polecenie Pracodawcy wykonywał pracę w dniu dla niego wolnym od pracy , przysługuje w zamian dzień wolny w innym terminie.

Rozdział V

Usprawiedliwianie nieobecności w pracy i zwolnienia od pracy

§ 29

1.Pracownik powinien powiadomić Pracodawcę o przyczynie i przewidywanym okresie nieobecności w pracy, jeżeli przyczyna tej nieobecności jest z góry wiadoma lub możliwa do przewidzenia.
2. W razie zaistnienia przyczyny uniemożliwiającej stawienie się do pracy, pracownik jest obowiązany niezwłocznie usprawiedliwić nieobecność w pracy lub spóźnienie do pracy, przedstawiając Pracodawcy przyczyny nieobecności w pracy lub spóźnienia, a na żądanie Pracodawcy także odpowiednie dowody.
3. Usprawiedliwianie nieobecności w pracy i udzielanie zwolnień od pracy następuje na zasadach określonych w powszechnie obowiązujących przepisach.

Rozdział VI

Udzielanie urlopów

§ 30

1. Urlop wypoczynkowy udzielany jest pracownikowi na zasadach określonych w kodeksie pracy, w terminie ustalonym przez pracodawcę tj. w czasie w którym nie są prowadzone w placówce zajęcia lekcyjne (w tym ferie zimowe i letnie, dni wolne zgodnie z organizacją systemu nauczania w szkole)
2. W celu potwierdzenia rozpoczęcia urlopu, przed terminem jego rozpoczęcia pracownik ma obowiązek złożyć wniosek urlopowy.
3. Przed rozpoczęciem urlopu, pracownik jest zobowiązany do pozostawienia swego miejsca pracy oraz otrzymanych materiałów i wyposażenia zgodnie z wytycznymi Pracodawcy lub przełożonych.
4. Po wykorzystanym urlopie Pracownik obowiązany jest zgłosić swoją gotowość do pracy Dyrektorowi Zespołu;

Rozdział VII

Odpowiedzialność porządkowa pracowników

§ 31

Pracownik, który wskutek niewykonania lub nienależytego wykonania obowiązków pracowniczych ze swej winy wyrządził pracodawcy szkodę materialną lub finansową, ponosi odpowiedzialność materialną na zasadach określonych w deklaracji materialnej.

§ 32

Za nieprzestrzeganie przez pracownika ustalonej organizacji i porządku w procesie pracy zostaje wprowadzona odpowiedzialność materialna na zasadach określonych w powszechnie obowiązujących przepisach.

§ 33

1.Za nieprzestrzeganie przez pracownika:
* ustalonej organizacji i porządku w procesie pracy,
* przepisów bhp,
* przepisów ppoż.,
* przyjętego sposobu potwierdzania przybycia i obecności w pracy
* usprawiedliwiania nieobecności w pracy,

pracodawca może stosować:
a) karę upomnienia,
b) karę nagany.
2. Za nieprzestrzeganie przez pracownika:
* przepisów bhp
* przepisów ppoż.,
* opuszczenie pracy bez usprawiedliwienia,
* stawienie się do pracy w stanie nietrzeźwości
* spożywanie alkoholu w czasie pracy

* rażące i nagminne niedopełnianie obowiązków pracowniczych
pracodawca może stosować karę pieniężną.
3. Pracodawca nie może zastosować jednocześnie kilku kar porządkowych.
4. Wysokość kary pieniężnej, tryb nakładania kar porządkowych oraz zasady zatarcia kary są uregulowane w kodeksie pracy.

Rozdział VIII

Nagrody , premie i wyróżnienia

§ 34

1. Wynagrodzenie szczegółowo jest określane przez indywidualne umowy lub Politykę Zatrudniania
2. Pracownikom, którzy wzorowo wypełniają swoje obowiązki, przejawiają inicjatywę w pracy oraz podnoszą jej wydajność i jakość, mogą być przyznawane wyróżnienia i premie uznaniowe mające charakter nagrody:
a) nagroda pieniężna,
b) nagroda rzeczowa,
c) pochwała pisemna,

3.Wysokość nagrody jest ustalana przez Pracodawcę indywidualnie dla każdego pracownika.
4.Ustalając wysokość nagrody Pracodawca bierze pod uwagę między innymi :
a. - jakość i efekt wykonanej pracy
b. - zaangażowanie i obecność w pracy
c. - inne opisane w Statucie Zespołu oraz w Polityce Zatrudniania
5. O wysokości nagrody pracownik może zostać poinformowany przez Pracodawcę ustnie do 10 dnia następnego miesiąca.
6. Pracodawca ma prawo ustalać wysokość nagrody biorąc pod uwagę między innymi :
a) czy w danym miesiącu pracownik przebywa na zwolnieniu lekarskim lub urlopie wypoczynkowym.
b) przypadki rażącego naruszenia obowiązków pracowniczych, oraz nie wywiązywania się z obowiązków.

Rozdział IX

Termin, miejsce i czas wypłaty wynagrodzenia

§ 35

1. Wynagrodzenie za pracę wypłaca się przelewem, z dołu raz w miesiącu, 10 dnia miesiąca kalendarzowego, następującego po miesiącu, za który wypłacane jest wynagrodzenie,
2. Jeżeli ustalony dzień wypłaty wynagrodzenia za pracę jest dniem wolnym od pracy, wynagrodzenie wypłaca się w dniu roboczym poprzedzającym dzień wypłaty wynagrodzenia
3. Wynagrodzenie wypłaca się wg. pisemnej dyspozycji pracownika na wskazany przez niego rachunek bankowy.

Rozdział X

Bezpieczeństwo i higiena pracy. Ochrona przeciwpożarowa.

§ 36

1.Pracodawca ponosi odpowiedzialność za stan bhp w zakładzie pracy oraz ochrony przeciwpożarowej.
2. Pracodawca jest obowiązany chronić zdrowie i życie pracowników poprzez zapewnienie bezpiecznych i higienicznych warunków pracy . W szczególności pracodawca jest obowiązany:
a) organizować pracę w sposób zapewniający bezpieczne i higieniczne warunki pracy,
b) zapewniać przestrzeganie w zakładzie pracy przepisów oraz zasad bezpieczeństwa i higieny pracy oraz ochrony przeciwpożarowej , wydawać polecenia usunięcia uchybień oraz kontrolować wykonanie tych poleceń,
c) zapewniać wykonanie nakazów, wystąpień, decyzji i zarządzeń wydawanych przez organy nadzoru nad warunkami pracy,

d) zapewniać wykonanie zaleceń inspektora pracy.

3.Pracodawca oraz osoba kierująca pracownikami są obowiązani znać, w zakresie niezbędnym do wykonywania ciążących na nich obowiązków, przepisy o ochronie pracy, w tym przepisy oraz zasady bhp oraz przepisy ochrony przeciwpożarowej.

§ 37

Przestrzeganie przepisów i zasad bhp oraz ochrony przeciwpożarowej jest podstawowym obowiązkiem pracownika. W szczególności pracownik jest obowiązany:
1) znać przepisy i zasady bhp i p. poż. , brać udział w szkoleniu i instruktażu z tego zakresu oraz poddawać się wymaganym egzaminom sprawdzającym,
2) wykonywać pracę w sposób zgodny z przepisami i zasadami bhp i p. poż. oraz stosować się do wydawanych w tym zakresie poleceń i wskazówek przełożonych,
3) dbać o należyty stan wyposażenia, narzędzi i sprzętu oraz o porządek i ład w miejscu pracy,
4) stosować środki ochrony zbiorowej, a także używać przydzielonych środków ochrony indywidualnej oraz odzieży i obuwia roboczego, zgodnie z ich przeznaczeniem,
5) poddawać się wstępnym, okresowym i kontrolnym oraz innym zaleconym badaniom lekarskim i stosować się do wskazań lekarskich,
6) niezwłocznie zawiadomić przełożonego o zauważonym w zakładzie pracy wypadku albo zagrożeniu życia lub zdrowia ludzkiego oraz ostrzec współpracowników, a także inne osoby znajdujące się w rejonie zagrożenia, o grożącym im niebezpieczeństwie,
7) współdziałać z pracodawcą i przełożonymi w wypełnianiu obowiązków dotyczących bhp i p. poż.

§ 38

W razie gdy warunki pracy nie odpowiadają przepisom bhp i p. poż. i stwarzają bezpośrednie zagrożenie dla zdrowia lub życia pracownika lub osób jemu podległym, albo gdy wykonywana przez niego praca grozi takim niebezpieczeństwem innym osobom, pracownik ma prawo powstrzymać się od wykonywania pracy, zawiadamiając o tym niezwłocznie Pracodawcę.

§ 39

1.Szkolenia okresowe pracowników zatrudnionych na stanowiskach, na których występują szczególnie duże zagrożenia dla zdrowia oraz zagrożenia wypadkowe, przeprowadza się raz do roku.
2.Szkolenia okresowe dla pracowników na stanowiskach robotniczych przeprowadza się nie rzadziej niż co 3 lata.
3. Szkolenia okresowe dla pracowników na stanowiskach administracyjnych przeprowadza się nie rzadziej niż co 5 lat.
4.Zapoznanie pracownika z ryzykiem zawodowym ,które wiąże się z wykonywaną pracą zostaje przekazane pracownikowi przez Zakładowego Inspektora BHP podczas szkolenia wstępnego pracownika. Pracownik potwierdza zaznajomienie się z ryzykiem zawodowym pisemnie potwierdzając ten fakt podpisem.
5. Pracownicy wykonywujący pracę w siedzibie Zakładu są zobowiązani do zaznajomienia się z Instrukcją Bezpieczeństwa Pożarowego znajdującej się w ogólnodostępnym miejscu. Potwierdzenie zaznajomienia się z w/w Instrukcją Pracownicy potwierdzają na odrębnym oświadczeniu znajdującym się w aktach osobowych pracownika.

§ 40

Okresowe badania pracowników przeprowadzane są zgodnie z powszechnie obowiązującymi przepisami na koszt pracodawcy.

§ 41

1.Pracownik nie może być dopuszczony do pracy bez środków ochrony indywidualnej oraz odzieży i obuwia roboczego przewidzianych do stosowania na danym stanowisku pracy.
2.Zasady przydziału odzieży i obuwia roboczego oraz środków ochrony indywidualnej określa załącznik do niniejszego regulaminu.

§ 42

W sprawie prania i naprawy odzieży roboczej i ochronnej
1.Zakład zapewnia pracownikom pranie odzieży zakładowej w wyspecjalizowanej pralni na koszt Pracodawcy.

2. Pracownik pozostawia brudne ubrania w miejscu wyznaczonym przez Pracodawcę wraz z ich pisemną listą.
3. Pracodawca zapewnia na czas prania ubranie zmienne.

§ 43

Ochrona pracy kobiet i młodocianych

1.Kobiety nie mogą być zatrudniane przy pracach szczególnie uciążliwych i szkodliwych dla zdrowia, ujętych w wykazie prac wzbronionych kobietom, stanowiącym załącznik nr. 5 do regulaminu.
2.Młodocianego nie wolno zatrudniać w godzinach nadliczbowych ani w porze nocnej. Wykaz prac wzbronionych młodocianym stanowi załącznik do regulaminu.

Rozdział XI

Postanowienia końcowe

§ 44

1.Niniejszy regulamin pracy wchodzi w życie po upływie 2 tygodni od dnia podania go do wiadomości pracowników poprzez odczytanie przez Pracodawcę i wywieszeniu na tablicy ogłoszeń przez okres 30 dni.
2. Nowo przyjmowani pracownicy potwierdzają zapoznanie się z regulaminem pracy i zobowiązują się do jego przestrzegania przed przystąpieniem do pracy.

§ 45

1.Regulamin pracy obowiązuje przez czas nieokreślony
2.Zmiana treści regulaminu może nastąpić w formie pisemnej , w tym samym trybie co jego ustanowienie bądź przez wprowadzenie nowego regulaminu.

§ 46

W sprawach wynikających ze stosunku pracy , nie uregulowanych niniejszym regulaminem zastosowanie mają przepisy kodeksu i prawa pracy.

ZATWIERDZAM:

.....

Stowarzyszenie
"Rozwój Bukowiny"

WYKAZ STANOWISK W ZAKŁADZIE
Stowarzyszenie "Rozwój Bukowiny"

1. dyrektor

2. nauczyciel (w tym może wystąpić funkcja wicedyrektora, pedagoga , bibliotekarza, opiekuna świetlicy, kierowcy)

3. specjalista ds. kontroli dokumentacji

4. sekretarka

5. kierownik sekcji ds. utrzymania porządku i czystości

6. pracownik sekcji ds. utrzymania czystości i porządku (w tym może wystąpić funkcja konserwatora, palacza, kierowcy, opiekuna dzieci, opiekuna boiska)

7. kierowca (w tym może wystąpić funkcja konserwatora, palacza, opiekuna dzieci, opiekuna boiska)

8. opiekun dzieci (w tym może wystąpić funkcja konserwatora, palacza, kierowcy, opiekuna boiska)

TABELA PRZYDZIAŁU ODZIEŻY ROBOCZEJ I OBUWIA W ZAKŁADZIE
Stowarzyszenie "Rozwój Bukowiny"

L. P.	STANOWISKO	RODZAJ ASORTYMENTU	OKRES UŻYTKOWANIA	UWAGI
1.	dyrektor	R - fartuch ochronny	36 msc	
2.	nauczyciel	R - fartuch ochronny	36 msc	
3.	Specjalista ds. kontroli dokumentacji, sekretarka	R - fartuch ochronny	36 msc	
4.	Pracownik sekcji ds. utrzymania porządku i czystości , kierowca, opiekun dzieci	R – fartuch ochronny R – spodnie R – buty robocze R- nakrycie głowy O – rękawice gumowe	12 – 18 msc 12 – 18 msc 12 – 18 msc 18 msc d.z.	

Legenda:
R – odzież robocza ; O – odzież ochronna ; d.z. – do zużycia

Dodatkowa odzież ochronna oraz środki ochrony indywidualnej dla pracowników może być przyznawana na wniosek pracowników po uzyskaniu pozytywnej opinii Inspektora BHP i akceptacji Pracodawcy

PRACODAWCA
.....

WYKAZ ŚRODKÓW CZYSTOŚCI PRZEZNACZONYCH DLA ZARUDNIONYCH PRACOWNIKÓW
w Stowarzyszeniu "Rozwój Bukowiny"

L.P.	STANOWISKO PRACY	MYDŁO TOALETOWE	PASTA BHP	PROSZEK DO PRANIA - PRANIE ODZIEŻY
1.	Pracownicy administracji i nauczyciele	Zakład zapewnia na bieżąco	----------	Zakład przekazuje do wyspecjalizowanej pralni
2.	Pracownicy ds. utrzymania porządku i czystości, kierowca, opiekun dzieci	Zakład zapewnia na bieżąco	Zakład zapewnia na bieżąco	Zakład przekazuje do wyspecjalizowanej pralni

PRACODAWCA

.....

WYKAZ PRAC WZBRONIONYCH MŁODOCIANYM

Na podstawie Art. 204 § 1 i 3 Kodeksu Pracy (Dz. U. z dnia 5 lipca 1974 r. Nr 24 poz. 141) oraz Rozporządzenia Rady Ministrów z dn. 1 grudnia 1990 r. w sprawie wykazu prac wzbronionych młodocianym (Dz. U. Nr 85, poz. 500) ze zmianą z dn. 21 grudnia 1991 r. (Dz. U. Nr 1, poz. 1 z dnia 7 stycznia 1993 r.).

1. Zabronione jest zatrudnianie młodocianych w godzinach nadliczbowych oraz w porze nocnej.
2. Przerwa pracy młodocianego obejmująca porę nocną powinna trwać nie mniej niż 14 godzin.
3. Rodzaje prac, przy których nie wolno zatrudniać młodocianych.

3.1. Obciążenie pracą fizyczną.

3.1.1. Wzbronione jest młodocianym prace polegające wyłącznie na podnoszeniu, przenoszeniu i przewożeniu ciężarów i prace wymagające powtarzania dużej liczby jednakowych ruchów. Czynności te mogą być wykonywane przez młodocianych tylko w zakresie niezbędnym do nauki zawodu, jeżeli czas ich wykonywania nie przekracza 1/3 czasu pracy młodocianego.

3.1.2. Wzbronione jest zatrudnianie młodocianych przy pracach, przy których najwyższe wartości obciążenia pracą fizyczną, mierzone wydatkiem energetycznym netto na wykonanie pracy, przekraczają:

Wiek	Dziewczęta					Chłopcy				
	dorywczo na min.		na 6 godz.		W	dorywczo na min.		na 6 godz.		W
	kJ	kcal	kJ	kcal	-	kJ	kcal	kJ	kcal	-
do ukończenia 16 roku życia	9,2	2,2	1800	430	84	11	2,7	2600	620	120
od 16 do ukończenia 18 roku życia	10,5	2,5	2300	550	107	12,6	3,0	3030	720	140

Uwaga: Wartości wydatku energetycznego na minutę dotyczy wysiłków krótkotrwałych.

3.2 Dźwiganie ciężarów i ich transport.

3.1.1. Wzbronione jest zatrudnianie młodocianych przy pracach załadunkowych i wyładunkowych, przy przetaczaniu beczek, bali, kloców itp. przy przewożeniu ciężarów samojezdnymi środkami transportu.

3.2.2. Wzbronione jest zatrudnianie młodocianych przy ręcznej obsłudze dźwigni, korb i kół sterowniczych, przy której niezbędna jest siła przekraczająca następujące wartości:

Wiek	Przy obciążeniu jednostkowym (w N) przeciętnie do 4 x na godzinę w czasie zmiany roboczej	
	Dziewczęta	Chłopcy
do ukończenia 16 roku życia	60	100
od 16 do ukończenia 18 roku życia	100	150
	Przy powtarzalnym obciążeniu	
do ukończenia 16 roku życia	30	40
od 16 do ukończenia 18 roku życia	40	60

Uwaga: 1 N = ok. 0,1 kg

3.2.3 Wzbronione jest zatrudnianie młodocianych przy ręcznym dźwiganiu i przenoszeniu na odległość powyżej 25 m ciężarów o masie przekraczającej następujące wartości:

Wiek	Przy obciążeniu jednostkowym (w N) przeciętnie do 4 x na godzinę w czasie zmiany roboczej	
	Dziewczęta	Chłopcy
do ukończenia 16 roku życia	10	15
od 16 do ukończenia 18 roku życia	20	25
	Przy powtarzalnym obciążeniu	
do ukończenia 16 roku życia	5	8
od 16 do ukończenia 18 roku życia	8	12

3.2.4 Wzbronione jest zatrudnianie młodocianych przy ręcznym przenoszeniu ciężarów pod górę tj. po pochylniach, schodach, których maksymalny kąt nachylenia przekracza 30° a wysokość tych urządzeń -5m, ciężarów o masie przekraczającej następujące wartości:

Wiek	Przy obciążeniu jednostkowym (w N) przeciętnie do 4 x na godzinę w czasie zmiany roboczej	
	Dziewczęta	Chłopcy
do ukończenia 16 roku życia	5	8
od 16 do ukończenia 18 roku życia	10	15
	Przy powtarzalnym obciążeniu	
do ukończenia 16 roku życia	3	5
od 16 do ukończenia 18 roku życia	5	8

4. Przewożenie ciężarów na taczkach jednokołowych
4.1. Wzbronione jest młodocianym chłopcom ukończenia 16 roku życia oraz dziewczętom do ukończenia 18 roku życia na taczkach jednokołowych,
4.2. Dozwolone jest młodocianym chłopcom po ukończeniu 16 roku życia przewożenia na odległość 50m ładunków o masie do 50kg po powierzchni gładkiej, utwardzonej lub po pomostach z desek trwale zamocowanych, jeżeli pochylenie powierzchni nie przekracza 2%.
5. Przewożenie na wózkach dwukołowych poruszanych ręcznie.
4.3. Wzbronione jest przewożenie ciężarów wyżej wymienionymi wózkami młodocianym chłopcom do ukończenia 16 roku życia oraz dziewczętom do ukończenia 18 roku życia.
4.4. Dozwolone jest młodocianym chłopcom po ukończeniu 16 roku życia przewożenia na odległość 100m po powierzchni gładkiej ładunków o masie do 80kg, jeżeli pochylenie powierzchni nie przekracza 2% a po powierzchni nierównej – ciężarów do 50kg, jeżeli pochylenie powierzchni nie przekracza 1%.
6. Przewożenie na wózkach trzykołowych lub czterokołowych poruszanych ręcznie.
6.1 Wzbronione jest młodocianym chłopcom i dziewczętom do ukończenia 16 roku życia przewożenia ładunków na wymienionych wózkach.
6.2 Dozwolone jest młodocianym po ukończeniu 16 roku życia przewożenia na odległość 150m ładunków o masie: dziewczętom do 50kg oraz chłopcom do 80kg, jeżeli pochylenie powierzchni nie przekracza 2% Uwaga: Wielkość ciężarów wymienionych obejmuje również wagę urządzenia transportowego
7. Prace wzbronione ze względu na możliwość urazów u młodocianych z naprawami i remontem maszyn i urządzeń
6.3 Wzbronione jest zatrudnianie młodocianych przy pracach związanych z naprawami i remontem maszyn i urządzeń.
6.4 Wzbronione jest młodocianym uruchamianie maszyn i innych urządzeń bezpośrednio po ich naprawie.

ZATWIERDZAM

.....

WYKAZ PRAC WZBRONIONYCH KOBIETOM

Na podstawie art. 176 Kodeksu pracy oraz Rozporządzenia Rady Ministrów z dnia 10 września 1996 r. w sprawie wykazu prac wzbronionych kobietom (Dz. U. Nr 114, poz. 545 z 1996 r.) ze zmianą z dnia 11.11.2002 r. (Dz.U. Nr 127, poz. 1092).

I
Prace związane z wysiłkiem fizycznym i transportem ciężarów oraz wymuszoną pozycją ciała.

1. Wszystkie prace, przy których najwyższe wartości obciążenia pracą fizyczną, mierzoną wydatkiem energetycznym netto na wykonanie pracy, przekraczają 5000 kJ na zmianę roboczą, a przy dorywczej - 20 kJ/min. Uwaga: 1 kJ = 0,24 kcl.
2. Ręczne podnoszenie i przenoszenie ciężarów o masie przekraczającej:
   - **2.1.** 12 kg – przy pracy stałej;
   - **2.2.** 20 kg – przy pracy dorywczej (do 4 razy na godzinę w czasie zmiany roboczej)
3. Ręczna obsługa elementów urządzeń (dźwigni, korb, kół sterowniczych itp.), przy której wymagane jest użycie siły przekraczającej,
   - **3.1.** 50 N – przy pracy stałej
   - **3.2.** 100 N – przy pracy dorywczej (do 4 razy na godzinę w czasie zmiany roboczej)
4. Przewożenie ciężarów o masie przekraczającej;
   - **4.1.** 50 kg – przy przewożeniu na taczkach jednokołowych
   - **4.2.** 80 kg – przy przewożeniu na wózkach 2,3 i 4 kołowych.

Wyżej podane dopuszczalne masy ciężarów po powierzchni obejmują również masę urządzenia transportowego i dotyczą przewożenia ciężarów po powierzchni równej twardej i gładkiej o pochyleniu nie przekraczającym 2% przy pracach wymienionych w pkt. 4.1. i 4.2.

W przypadku przewożenia ciężarów po powierzchni nierównej, w sposób określony w pkt. 4 masa ciężaru nie może przekroczyć 60 proc. wielkości podanych w tym punkcie.

5. Kobietom z ciąży i w okresie karmienia:
   - **5.1.** Wszystkie prace, przy których najwyższe wartości obciążenia pracą fizyczną, mierzone wydatkiem energetycznym netto na wykonanie pracy, przekraczają 29000 kJ na zmianę.
   - **5.2.** Prace wymienione w pkt. 2-4 jeżeli występuje przekroczenie ¼ określonych w nich wartości np.: ręczne przenoszenie i podnoszenie ciężarów:

- 3 kg – przy pracy stałej,
- 5 kg – przy pracy dorywczej,

Obsługa elementów urządzeń:

- 12,5 N – przy pracy stałej
- 20 N – przy pracy dorywczej,

   - **5.3.** Praca w pozycji wymuszonej.
   - **5.4.** Praca w pozycji stojącej łącznie ponad 3 godziny w czasie zmiany roboczej.

II
Praca w hałasie i drganiach

1. Praca w środowisku, w którym wartość ważone przyspieszenie drgań oddziałujących na organizm człowieka przez kończyny górne, mierzone zgodnie z Polskimi Normami, dla drgań różnej wartośc współczynnika szczytu k, przy ciągłym 8-godzinnym, oddziaływania na organizm przekraczają wartości podane w tabeli.

Składowe drgań	Wartości ważone przyspieszenia drgań (m/s^2)		
	$k \leq 2$	$2<k\leq3$	$k>3$
X, Y, Z (x, y, z)	0,1	0,15	0,3

2. Praca w środowisku, w którym wartości wazone przyspieszenia drgań o ogólnym oddziaływaniu na organizm człowieka, mierzone zgodnie z Polskimi Normami, dla drgań o różnej wartości współczynnika szczytu k, przy ciągłym 8-godzinnym oddziaływaniu na organizm, przekraczają wartości podane w tabelkach.

Składowe drgań	Wartości ważone przyspieszenia drgań (m/s^2)		
	$k \leq 2$	$2<k\leq3$	$3<k\leq3$
Poziome X, Y, Z (x, y, z)	0,1	0,15	0,3
Pionowe Z (z)	0,13	0,2	0,4

3. Kobietom w ciąży.
   3.1. Prace w środowisku, którym poziom ekspozycji na hałas, odniesiony do 8 godzinnego dnia pracy, mierzony zgodnie z Polskimi Normami, przekracza wartość 65 dB.
   3.2. Prace w środowisku, w którym poziom ciśnienia akustycznego hałasu infradźwiękowego, mierzony zgodnie z Polskimi Normami, przekracza wartości podane w tabeli (dla 8 godzinnej ekspozycji na hałas):

Częstotliwość środkowa pasm oktawowych (Hz.)	Poziom ciśnienia akustycznego (dB)
8;16	85
31,5	80

   3.3. Prace w środowisku, w którym poziom ciśnienia akustycznego hałasu ultradźwiękowego, mierzony zgodnie z Polskimi Normami, przekracza wartości podane w tabeli (dla 8-godzinnej ekspozycji na hałas).

Częstotliwość środkowa pasm tercjowych	Dopuszczalny poziom ciśnienia akustycznego
10; 12,5; 16	77
20	87
25	102
31,5; 40; 50; 63; 80; 100	107

   3.4. Prace w środowisku, którym wartości ważone przyspieszenia drgań oddziałujących na organizm człowieka przez kończyny górne nie przekraczają wartości określonych pkt. 1. – powyżej 4 godzin na dobę.
   3.5. Każda praca w warunkach narażania na drgania o ogólnym oddziaływaniu na organizm człowieka.

III.
Prace narażające na działanie pól elektromagnetycznych, promieniowania jonizującego i nadfioletowego oraz prace przy monitorach ekranowych.

1. Kobietom w ciąży:
   1.2. Praca w zasięgu pól elektromagnetycznych o natężeniach przekraczających wartości dla sfery bezpiecznej.
   1.3. Praca w środowisku, w którym występuje przekroczenie ¼ wartości najwyższych dopuszczalnych natężeń promieniowania nadfioletowego, określonych w przepisach w sprawie najwyższych dopuszczalnych stężeń i natężeń czynników szkodliwych dla zdrowia w środowisku pracy.
   1.4. Prace przy obsłudze monitorów ekranowych – powyżej 4 godzin na dobę.

IV.
Prace grożące urazami fizycznymi i psychicznymi. Kobietom w ciąży i w okresie karmienia.

1. Prace w wymuszonym rytmie pracy (na przykład na taśmie produkcyjnej).
2. Prace stwarzające ryzyko ciężkiego urazu fizycznego lub psychicznego, np.: gaszenie pożarów, udział w akcjach ratownictwa chemicznego, usuwanie skutków awarii.

ZATWIERDZAM

.....

INSTRUKCJA PRZECIWPOŻAROWA

W sprawie ogólnych warunków zabezpieczenia przeciwpożarowego w Stowarzyszeniu "Rozwój Bukowiny" w Bukowinie. Na podstawie Ustawy z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej tekst jednolity [Dz.U. Nr 147, poz. 1591 z 2002 r.].

I
POSTANOWIENIA OGÓLNE.

1. Ochrona przeciwpożarowa polega na realizacji przedsięwzięć mających na celu ochronę życia, zdrowia i mienia przed pożarem, klęską żywiołową lub innym miejscowym zagrożeniem poprzez:
   - **a)** zapewnienia koniecznych warunków ochrony technicznej nieruchomościom i ruchomościom,
   - **b)** Tworzenie warunków organizacyjnych i formalno-prawnych, zapewniających ochronę ludzi i mienia, a także przeciwdziałających powstaniu pożaru, klęski żywiołowej lub innego miejscowego zagrożenia/katastrofy techniczne, chemiczne, ekologiczne/,
   - **c)** zapewnienienie sił i środków do zwalczania pożaru, klęski żywiołowej lub innego miejscowego zagrożenia
   - **d)** prowadzenie działań ratowniczych.
2. Zapobiegania pożarowi klęsce żywiołowej lub innego miejscowemu zagrożeniu

2.1. Osoby fizyczne, prawne organizacje lub instytucje korzystające ze środowiska przyrodniczego, budynku, obiektu lub terenu, obowiązane są zabezpieczyć użytkowane środowisko, budynek, obiekt lub teren przed zagrożeniem pożarowym lub innym miejscowym zagrożeniem.

2.2. Właściciel, zarządca lub użytkownik budynku, obiektu lub terenu, zapewniając jego ochronę przeciwpożarową obowiązany jest w szczególności do:
   - **a)** przestrzegania przeciwpożarowych wymagań budowlanych i technologicznych,
   - **b)** wyposażenia budynku, obiektu w sprzęt pożarniczy i ratowniczy oraz środki gaśnicze,
   - **c)** zapewnienia osobom przebywającym w budynku, obiekcie lub na terenie bezpieczeństwo i możliwość ewakuacji,
   - **d)** przygotowania budynku, obiektu lub terenu do prowadzenia akcji ratowniczej,
   - **e)** ustalenia sposobów postępowania na wypadek powstania pożaru, klęski żywiołowej lub innego miejscowego zagrożenia.

II
W CELU UNIEMOŻLIWIENIA POWSTANIA POŻARU ZABRANIA SIĘ:

1. Palenia tytoniu
2. Używania ognie otwartego/zapałki, zapalniczek, świec itp., do prześwietlania na halach, poddaszach i innych pomieszczeniach oraz na terenie Zakładu.
3. Wykonywania wszelkich prac przy użyciu ognia otwartego jak spawanie, rozpalanie ognisk, używanie lamp lutowniczych w halach produkcyjnych, garażach oraz na terenie fabrycznym bez należytego przygotowania stanowiska pracy.
4. Pozostawianie nawet na krótki okres czasu bez nadzoru wszelkich palników gazowych, koszy koksowych, pieców grzewczych i grzejników elektrycznych. Urządzenia te i im podobne powinny być wygaszone lub wyłączone przed opuszczeniem pracy przez pracowników.
5. Pozostawienie materiałów palnych w suszarkach, komorach na grzejnikach, rurociągach parowych itp. bez nadzoru.
6. Przekraczanie określonych instrukcją norm technologicznych i magazynowych oraz temperaturą, czasu suszenia i hartowania.

III
SPOSÓB ZAPOBIEGANIA POWSTANIA I ROZSZERZENIA SIĘ POŻARÓW.

1. Przed opuszczeniem miejsca pracy – każdy pracownik powinien sprawdzić czy na jego odcinku pracy nie zachodzi możliwość powstania pożaru, a ewentualnie braki czy usterki mogące stworzyć zagrożenie winien usunąć.
2. Urządzenia ogrzewcze i energetyczne powinny być wykonywane zgodnie z obowiązującymi przepisami oraz powinne być zabezpieczone przed uszkodzeniami mechanicznymi.
3. W przestrzeniach zagrożonych pożarem zabrania się:
   - **a)** instalowania transformatorów i kondensatorów energetycznych do kompensacji mocy biernej w wykonaniu normalnym z palnym czynnikiem izolującym lub chłodzącym oraz prostowników rtęciowych
   - **b)** umieszczenia stanowisk ładowania akumulatorów.
4. Wszelkie urządzenia elektryczne jak tablice rozdzielcze, bezpieczniki, wyłączniki itp. powinny być obsługiwane i naprawiane przez personel fachowy upoważniony oraz zabezpieczone przed dostępem pyłów i gazów łatwopalnych.
5. Zaoliwione odpadki i czyściwo należy przechowywać w naczyniach metalowych – zamykanych w miejscach na ten cel wyznaczonych.
6. Obowiązkiem każdego pracownika jest uczęszczanie na szkolenie przeciwpożarowe prowadzone przez Zakładową Służbę Przeciwpożarową.
7. Wszyscy pracownicy obowiązani są czuwać nad przestrzeganiem bezpieczeństwa przeciwpożarowego Zakładu. O wszelkich zauważonych usterkach i niedociągnięciach w pracy maszyn, urządzeń i innych przyczynach, które mogłyby spowodować powstanie pożaru należy bezzwłocznie zgłosić Kierownikowi Działu lub Inspektorowi Ochrony Przeciwpożarowej.

IV
ZWALCZANIE POŻARÓW.

1. W razie zauważenie pożaru należy natychmiast zawiadomić:
   a) straż pożarną
   b) pracodawcę lub bezpośredniego przełożonego
   c) policję.
2. Jednocześnie należy zaalarmować wszystkich pracowników, którzy powinni udać się niezwłocznie na miejsce pożaru i podporządkować poleceniom najstarszego stopniem służbowym.
3. Do tłumienia pożaru należy używać podręcznego sprzętu gaśniczego oraz wszelkich dostępnych środków gaśniczych zgodnie z ich przeznaczeniem, gdyż należy pamiętać, że źle prowadzona akcja gaśnicza może przyczynić się do zaistnienia nieszczczęśliwych wypadków np. porażenia prądem oraz przyczynić się do powstania większych strat materialnych np. odkształcenia części maszyn i urządzeń.
4. Po przybyciu straży pożarnej należy wskazać jej drogę do miejsca pożaru, po czym kierowanie akcją obejmuje dowódcą straży.
5. Dowódcy straży pożarnej należy przekazać dotychczasowy przebieg akcji i wskazać ewentualne zagrożenia oraz podporządkować się kierującemu akcję ratowniczo – gaśniczą, którego zarządzenia obowiązani są wykonywać wszyscy pracownicy.

V
W CELU USPRAWNIENIA AKCJI GAŚNICZO – RATOWNICZEJ NA WYPADEK POŻARU NALEŻY:

1. Oznakować tablicami /znakami/drogi pożarowe, ewakuacyjne sprzętu p. poż. Zgodnie z PN-92/N-01256/01 i 02.
2. Wywiesić w dostępnych miejscach plan rozmieszczania sprzętu gaśniczego, wyłączników prądu elektrycznego i gazu oraz punktów czerpania wody.
3. Wywiesić w dostępnych miejscach instrukcje, ustalające stosowanie odpowiednich środków gaśniczych dla danych pomieszczeń.

VI
W CELU USPRAWNIENIA AKCJI GAŚNICZO – RATOWNICZEJ NA WYPADEK POŻARU ZABRANIA SIĘ:

1. Używania sprzętu przeciwpożarowego do celów nie związanych z ochroną przeciwpożarową.
2. Zastawiania bądź tarasowania przejść, wyjść zapasowych, dróg, dostępu do drabin, dojazdów do zbiorników, niszczenia lub zastawiania orientacyjnych znaków przeciwpożarowych.

VII
PRZEPISY KARNE:

Przestępstwa przeciwko bezpieczeństwu powszechnemu oraz bezpieczeństwu w ruchu lądowym wodnym i powietrznym normuje. Prawo Karne w rozdziale XX. Są to następujące przestępstwa:

1. Sprowadzenie zdarzenia zagrażającego życiu lub zdrowiu ludzi albo mieniu w znacznych rozmiarach /art. 136/; - podlega karze pozbawienia wolności na czas nie krótszy od lat 3.
2. Sprawdzenie bezpośredniego niebezpieczeństwa zdarzenia wymienionego w srt. 136 /art. 136/ § 1. Sprawca takiego czynu podlega karze pozbawienia wolności od 6 miesięcy do 8 lat. Jeżeli sprawca działa nieumyślnie, podlega zgodnie z § 2 karze pozbawienia wolności do lat 3.
3. Sprowadzenia pożaru /art.138/ - podlega karze pozbawienia wolności na czas nie krótszy od lat 3. Jeżeli zaś sprawca działa nie umyślnie, podlega zgodnie z § 2 z tego artykułu jest to wystep, który podlega karze pozbawienia wolności od roku do lat 8.
4. Sprawdzenie bezpośredniego niebezpieczeństwa pożaru /art. 139/ - podlega karze pozbawienia wolności od 6 m-cy do lat 8 (§ 1). Jeżeli sprawca działa nieumyślnie, podlega karze pozbawienia wolności do lat 3 (§ 2).
5. Sprowadzenie niebezpieczeństwa powszechnego (art. 140), podlega karze pozbawienia wolności od lat 2 do lat 10. Jeżeli sprawca działa nieumyślnie, zgodnie z § 2 podlega karze pozbawienia wolności od 6 miesięcy do lat 5.

Zatwierdzam:
.....

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

stanowiąca załącznik do Regulaminu Pracy

w

Stowarzyszeniu "Rozwój Bukowiny" 84-311 Bukowina 5

Bukowina, maj 2016

Regulamin Pracy uchwalony w dniu 20.08.2018r. nie wniósł zmian w niniejszej instrukcji z maja 2016r.

ROZDZIAŁ I
Podstawowe pojęcia oraz zakres przedmiotowy instrukcji

§ 1

Stosownie do postanowień § 3 i § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji 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. Nr 100, poz. 1024), ustala się treść Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Stowarzyszeniu "Rozwój Bukowiny".

§ 2

Ilekroć w instrukcji jest mowa o:

a) **systemie informatycznym** - należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
b) **zabezpieczeniu systemu informatycznego** - należy przez to rozumieć zastosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, mające na celu w szczególności zabezpieczenie danych przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, zmianą, utratą uszkodzeniem lub zniszczeniem.
c) **zbiorze danych osobowych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
d) **przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
e) **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
f) **Administratorze Danych Osobowych** – dalej jako Administrator danych; - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych. Administratorem danych jest Stowarzyszenie "Rozwój Bukowiny"
g) **Administratorze Bezpieczeństwa Informacji** - rozumie się przez to osobę wyznaczoną przez Administratora danych, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
h) **użytkowniku** - rozumie się przez to upoważnionego przez Administratora danych (w przypadku powołania Administratora Bezpieczeństwa Informacji również przez ABI), wyznaczonego do przetwarzania danych osobowych pracownika, który odbył stosowne szkolenie w zakresie ochrony tych danych.
   Każdy użytkownik jest odnotowany w Rejestrze Upoważnień stanowiący załącznik do niniejszej Instrukcji
   Szkolenie dotyczące ochrony danych osobowych jest przeprowadzane przez Administratora lub ABI zgodnie z treścią ustawy o ochronie danych osobowych , polityki bezpieczeństwa oraz niniejszą instrukcją.

§ 3

1. Instrukcja ta określa:
   1) sposób przydziału haseł dla użytkowników i częstotliwości ich zmiany oraz wskazania osób odpowiedzialnych za te czynności;
   2) sposób rejestrowania i wyrejestrowywania użytkowników oraz wskazania osób odpowiedzialnych za te czynności;
   3) procedury rozpoczęcia, zawieszenia i zakończenia pracy;
   4) metody i częstotliwość tworzenia kopii awaryjnych;

5) metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz metodę ich usuwania;
6) sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków;
7) sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych;
8) sposób postępowania w zakresie komunikacji w sieci komputerowej.

2. Działaniem instrukcji objęci są:
1) Administrator Danych;
2) Administrator Bezpieczeństwa Informacji
3) osoby zatrudnione w Stowarzyszeniu "Rozwój Bukowiny" przy przetwarzaniu danych osobowych;
4) osoby, które przetwarzają dane osobowe znajdujące się w posiadaniu Stowarzyszenia "Rozwój Bukowiny"

ROZDZIAŁ II
Administracja i organizacja bezpieczeństwa

§4

1. Instrukcja ma zastosowanie na obszarze wskazanym w Polityce Bezpieczeństwa przetwarzania danych osobowych w Stowarzyszeniu "Rozwój Bukowiny" (dalej Polityka Bezpieczeństwa), w którym przetwarzane są dane osobowe w systemie informatycznym.

2. Przebywanie wewnątrz obszaru, o którym mowa w ust. 1, osób nieuprawnionych do dostępu do danych osobowych jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych osobowych.

§ 5

1. Administrator danych lub ABI sprawuje ogólną kontrolę i nadzór nad przestrzeganiem postanowień instrukcji, a w szczególności:

1) sam lub za pomocą wyznaczonej przez siebie osoby sporządza kopie bezpieczeństwa dla baz sieciowych;
2) pozbawia urządzenia i inne nośniki informacji przeznaczone do likwidacji zapisu danych lub - gdy nie jest to możliwe - uszkadza je trwale w sposób uniemożliwiający odczytanie danych;
3) nadzoruje usuwanie awarii sprzętu komputerowego w sposób zapewniający bezpieczeństwo przetwarzanych danych osobowych;
4) zabezpiecza zbiory danych osobowych wysyłanych poza obszar określony w Polityce Bezpieczeństwa;
5) sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe;
6) sam lub za pomocą wyznaczonej osoby sprawuje nadzór nad czynnościami związanymi z ochroną przeciwwirusową, czynnościami serwisowymi dotyczącymi systemu informatycznego, w którym przetwarzane są dane osobowe;
7) nadzoruje obieg i przetwarzanie wydruków z systemu informatycznego zawierających dane osobowe;
8) podejmuje i nadzoruje wszelkie inne działania zmierzające do zapewnienia bezpieczeństwa przetwarzanych w systemie informatycznym danych osobowych.

ROZDZIAŁ III
Obowiązki osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym

§ 6

1. Dostęp do sytemu informatycznego należącego do Administratora danych posiadają jedynie osoby upoważnione.
2. Indywidualny zakres czynności osoby upoważnionej przy przetwarzaniu danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę tych danych przed:
1) niepowołanym dostępem;
2) nieuzasadnioną modyfikacją lub zniszczeniem;

3) nielegalnym ujawnieniem;
4) pozyskaniem - w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych.

3. Przed dopuszczeniem do przetwarzania danych osobowych, każda osoba powinna być zaznajomiona z przepisami dotyczącymi ochrony danych osobowych.
4. Bezpośredni dostęp do sprzętu i aplikacji służących do przetwarzania danych osobowych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
5. Jeżeli istnieje taka możliwość, ekrany monitorów, na których możliwy jest dostęp do danych osobowych, powinny być automatycznie wyłączane po upływie ustalonego czasu nieaktywności użytkownika.
6. Monitory komputerów powinny być tak ustawione, aby uniemożliwić osobom postronnym wgląd do danych osobowych.

ROZDZIAŁ IV
Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym

§ 7

1. Przed rozpoczęciem pracy w systemie informatycznym użytkownik zobowiązany jest do:
   1) zalogowania się do systemu z wykorzystaniem zastrzeżonych tylko dla siebie: identyfikatora i hasła w sposób uniemożliwiający ich ujawnienie osobom postronnym - hasło nie może zawierać mniej niż 8 znaków, osoba je tworząca obowiązana jest uczynić to w taki sposób, aby utrudnić jego ewentualne odczytanie, poprzez wprowadzenie do hasła: znaków szczególnych, cyfr, dużych liter itd.,
   2) sprawdzenia prawidłowości funkcjonowania sprzętu komputerowego i systemów, na swoim stanowisku pracy,
   3) w razie stwierdzenia nieprawidłowości, do powiadomienia o tym fakcie bezpośredniego przełożonego oraz Administratora Bezpieczeństwa Informacji
   4) w razie stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub stanu wskazującego na istnienie takiej możliwości, do podjęcia odpowiednich kroków stosownie do zasad postępowania w sytuacji naruszenia zabezpieczenia danych osobowych.
2. Przerywając przetwarzanie danych w ciągu godzin pracy, użytkownik powinien co najmniej: aktywować wygaszasz ekranu lub w inny sposób zablokować możliwość korzystania ze swego konta użytkownika przez inne osoby. Niemniej jednak zalecane jest w takich przypadkach:
   1) skorzystanie z mechanizmu czasowej blokady dostępu do komputera poprzez uruchomienie wygaszacza ekranu z hasłem (hasło powinno być zbieżne z hasłem logowania do systemu);
   2) zakończenie pracy w systemie informatycznym - wylogowanie się z systemu.
3. Po zakończeniu przetwarzania danych osobowych w danym dniu, osoba upoważniona zobowiązana jest do:
   1) zakończenia pracy w systemie informatycznym;
   2) wylogowania się z systemu informatycznego;
   3) wyłączenia sprzętu komputerowego oraz zamknięcia szaf, w których przechowuje się nośniki, na których utrwalone są dane osobowe;
   4) zamknięcia i opuszczenia pomieszczeń biurowych;
4. Korzystanie z pomieszczeń biurowych oraz ich wyposażenia w celach niezwiązanych z przetwarzaniem danych osobowych wynikających z uzyskanego upoważnienia może następować tylko za zgodą Administratora danych lub Administratora Bezpieczeństwa Informacji i nie może być związane z przetwarzaniem danych znajdujących się w zbiorach danych Administratora danych.
5. Nośniki informacji oraz wydruki z danymi osobowymi, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.

ROZDZIAŁ V
Procedury rejestracji użytkowników

§ 8

1. Użytkownikiem systemu informatycznego może być jedynie osoba posiadająca odpowiednie upoważnienie i zarejestrowana w rejestrze użytkowników.
2. Rejestr użytkowników systemu prowadzi Administrator Danych bądź Administrator Bezpieczeństwa Informacji.

3. Każdy zarejestrowany użytkownik korzysta z przydzielonego mu konta użytkownika, opatrzonego identyfikatorem i hasłem dostępu.
4. Nadawanie identyfikatorów i przydzielanie haseł;
   1) w celu jednoznacznego określenia użytkowników przyjmuje się następującą metodologię nadawania nazw kont:
   2) pierwsza litera imienia + nazwisko (nie używając polskich znaków i wielkich liter);
   3) hasło składa się z co najmniej 8 znaków; zalecane jest, aby zawierało małe i wielkie litery oraz cyfry i znaki specjalne;
   4) zmiana hasła powinna być wykonywana **najlepiej co 30 dni.** W systemie informatycznym zapewnia się automatyczne wymuszanie zmiany hasła,
   5) identyfikator użytkownika powinien być inny dla każdego użytkownika, a po jego wyrejestrowaniu z systemu informatycznego, nie powinien być przydzielany innej osobie;
   6) identyfikatory użytkowników ujawnione są w wykazie osób upoważnionych do przetwarzaniu danych osobowych;
   7) hasła pozostają tajne, każdy użytkownik jest zobowiązany do zachowania w tajemnicy swego hasła, także po jego zmianie;
   8) obowiązek ten rozciąga się także na okres po upływie ważności hasła;
   9) hasło, co do którego zaistniało choćby podejrzenie ujawnienia powinno być niezwłocznie zmienione przez użytkownika;
   10) utrata upoważnienia do przetwarzania danych osobowych, powoduje natychmiastowe usunięcie z grona użytkowników systemu informatycznego.

ROZDZIAŁ VI
Kopie bezpieczeństwa

§ 9

Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, powinny być zabezpieczone przed utratą tych danych wskutek awarii zasilania lub zakłóceń w sieci zasilającej. Zabezpieczenie to powinno być tak skonstruowane, by umożliwiało zapisanie danych we wszystkich uruchomionych aplikacjach i wykonanie kopii bezpieczeństwa.

§ 10

1. Kopie bezpieczeństwa powinny być wykonywane codziennie (od poniedziałku do piątku).
2. W Stowarzyszeniu "Rozwój Bukowiny" do tworzenia kopii bezpieczeństwa wykorzystuje się **rejestratory** lub inne dostępne na rynku urządzenia przeznaczone do tworzenia kopii zapasowych.
3. Tworzenie kopii bezpieczeństwa odbywa się poprzez poprzez codzienne, automatyczne zgranie danych do dysku zewnętrznego.
4. Osobą odpowiedzialną za tworzenie kopii zapasowych oraz weryfikację zgodnie z pkt 9 jest Administrator Danych
5. Tworzone kopie bezpieczeństwa powinny być opisane w sposób pozwalający na określenie ich zawartości.
6. Kopie bezpieczeństwa nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.
7. Ewentualne dodatkowe kopie bezpieczeństwa należy przechowywać w innym miejscu niż kopie pierwotne.
8. Kopie bezpieczeństwa powinny być przechowywane w sejfie lub w przypadku braku takiej możliwości w zamkniętych szafach, znajdujących się w pomieszczeniach, które również są zamykane na klucz.
9. Kopie bezpieczeństwa należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu oraz bezzwłocznie usuwać po ustaniu ich użyteczności.
10. Kopie bezpieczeństwa, które uległy uszkodzeniu lub stały się niepotrzebne pozbawia się zapisu danych w sposób uniemożliwiający ich odtworzenie.
11. Jeżeli pozbawienie zapisu nie jest możliwe, kopie są niszczone w sposób uniemożliwiający odczytanie bądź odtworzenie danych zawartych na nośniku kopii.

ROZDZIAŁ VII

Sposób i czas przechowywania oraz zasady likwidacji nośników informacji

§ 11

1. Wydruki komputerowe z systemu, zawierające dane osobowe są sporządzane jedynie dla celów operacyjnych.
2. Wydruk komputerowy z systemu, zawierający dane osobowe, po odpowiednim opisaniu i oznaczeniu, podlega zasadom ochrony danych osobowych przetwarzanych metodami tradycyjnymi.
3. Wydruki ze zbiorów danych osobowych tworzone i używane do celów roboczych, (operacyjnych) przechowywane są w zamykanych szafach.
4. Nośniki magnetyczne, optyczne i inne nośniki informatyczne, zawierające dane osobowe, przechowywane są w odpowiednich, przeznaczonych do tego zamykanych szafach na terenie siedziby Stowarzyszenia "Rozwój Bukowiny" oraz poza siedzibą u osób wyznaczonych do reprezentacji Stowarzyszenia "Rozwój Bukowiny"
5. Likwidacja wydruków z systemu, zawierających dane osobowe odbywa się za pomocą niszczarki do dokumentów lub w inny sposób, trwale uniemożliwiający odczytanie danych.
6. Z urządzeń, dysków lub innych nośników informatycznych, które zostały przeznaczone do przekazania innemu podmiotowi, usuwa się zapisane na nich dane

ROZDZIAŁ VIII

Ochrona antywirusowa

§ 12

1. Ochrona antywirusowa jest realizowana poprzez zainstalowanie odpowiedniego oprogramowania antywirusowego.
2. W przypadku wykrycia wirusa komputerowego, użytkownik systemu zobowiązany jest do natychmiastowego poinformowania o tym fakcie Administratora Danych lub Administratora Bezpieczeństwa Informacji
3. System informatyczny podlega regularnej, (co najmniej raz w tygodniu) kontroli pod kątem obecności wirusów komputerowych.
4. Wykryte zagrożenia usuwa się niezwłocznie z systemu informatycznego.
5. Przed przystąpieniem do unieszkodliwienia wirusa, należy zabezpieczyć dane zawarte w systemie przed ich utratą.
6. Osobą odpowiedzialną za powyższe działania jest osoba upoważniona przez Administratora Danych do tych czynności.

ROZDZIAŁ IX

Konserwacja i naprawa systemu przetwarzającego dane osobowe

§ 13

1. Prace bieżące w dziedzinie konserwacji i naprawy systemu przetwarzającego dane osobowe prowadzi osoba odpowiedzialna za te czynności lub w wypadku konieczności zaangażowania do w/w czynności przedsiębiorcy zajmującego się zawodowo ich wykonywaniem, są one wykonywane pod bezpośrednim nadzorem Administratora danych lub Administratora Bezpieczeństwa Informacji.
2. Administrator danych lub Administrator Bezpieczeństwa Informacji mogą upoważniać pracowników Biura do nadzorowania bieżących napraw w dziedzinie konserwacji i napraw.
3. Urządzenia komputerowe, dyski twarde, lub inne informatyczne nośniki danych przeznaczone do naprawy, pozbawia się przed tymi czynnościami zapisu zgromadzonych na nich danych osobowych.
4. Czynności serwisowe mogą być wykonywane jedynie pod nadzorem Administratora Bezpieczeństwa Informacji lub osoby wyznaczonej.

ROZDZIAŁ X
Sposoby postępowania w zakresie komunikacji w sieci komputerowej

§ 14

1. Wszelkie pliki zawierające kopie danych osobowych zawartych w systemie, wysyłanych poza system, muszą być zabezpieczone hasłem.
2. W miarę możliwości, dane osobowe zawarte na serwerze sieciowym nie mogą być przechowywane na stacjach roboczych. Należy dane te umieszczać na dysku sieciowym.
3. Nieuzasadnione kopiowanie danych z serwera na stacje robocze bądź na nośniki informatyczne jest zabronione.

ROZDZIAŁ XI
Zasady korzystania z komputerów przenośnych

§ 15

1. Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem, przeznaczonym do przetwarzania danych osobowych wskazanym w Polityce Bezpieczeństwa.
2. W celu zapobieżenia dostępowi do tych danych osobie niepowołanej, należy:
   1) zabezpieczyć dostęp do komputera hasłem (w przypadku systemu operacyjnego Windows - w sposób który umożliwia to oprogramowanie);
   2) nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych;
   3) zabezpieczyć aplikacje przetwarzające dane osobowe hasłem.

ROZDZIAŁ XII
Postępowanie w sytuacji stwierdzenia naruszenia ochrony danych osobowych

§16

Naruszeniem zabezpieczeń systemu informatycznego są w szczególności:

1) naruszenie lub próby naruszenia integralności systemu przeznaczonego do przetwarzania danych osobowych - przez osoby nieuprawnione do dostępu do sieci lub aplikacji ze zbiorem danych osobowych;
2) naruszenie lub próba naruszenia integralności danych osobowych w systemie przetwarzania (wszelkie dokonane lub usiłowane modyfikacje, zniszczenia, usunięcia danych osobowych przez nieuprawnioną do tego osobę);
3) celowe lub nieświadome przekazanie zbioru danych osobowych osobie nieuprawnionej do ich otrzymania;
4) nieautoryzowane logowanie do systemu;
5) nieuprawnione prace na koncie użytkownika dopuszczonego do przetwarzania danych osobowych przez osobę do tego nieuprawnioną;
6) istnienie nieautoryzowanych kont dostępu do danych osobowych;
7) włamanie lub jego usiłowanie z zewnątrz sieci;
8) nieautoryzowane zmiany danych w systemie;
9) nie zablokowanie dostępu do systemu przez osobę uprawnioną do przetwarzania danych osobowych w czasie jej nieobecności;
10) ujawnienie indywidualnych haseł dostępu użytkowników do systemu;
11) brak nadzoru nad serwisantami lub innymi pracownikami przebywającymi w pomieszczeniach, w których odbywa się przetwarzanie danych osobowych;
12) nieuprawniony dostęp lub próba dostępu do pomieszczeń, w których odbywa się przetwarzanie danych osobowych;
13) kradzież nośników, na których zapisane są dane osobowe;
14) nieautoryzowana zmiana lub usunięcie danych zapisanych na kopiach bezpieczeństwa lub kopiach archiwalnych;
15) niewykonanie kopii bezpieczeństwa w odpowiednim terminie;
16) niewłaściwe bądź nieuprawnione uszkadzanie, niszczenie nośników zawierających dane osobowe.

§ 17

Osoba zatrudniona przy przetwarzaniu danych osobowych, która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych w systemie informatycznym, zobowiązana jest niezwłocznie powiadomić o tym Administratora danych Administratora Bezpieczeństwa Informacji

§ 18

W przypadkach, o których mowa w § 16 i § 17, należy podjąć czynności zmierzające do zabezpieczenia miejsca zdarzenia, zabezpieczenia ewentualnych dowodów przestępstwa i minimalizacji zaistniałych szkód, w tym w szczególności:

1) zapisać wszelkie informacje związane z danym zdarzeniem, a w szczególności:
   a. dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu,
   b. dane osoby zgłaszającej,
   c. opis miejsca zdarzenia,
   d. opis przedstawiający stan techniczny sprzętu służącego do przetwarzania lub przechowywania danych osobowych,
   e. wszelkie ustalone okoliczności zdarzenia;
2) na bieżąco wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem;
3) dokonać identyfikacji zaistniałego zdarzenia, poprzez ustalenie w szczególności:
   a) rozmiaru zniszczeń,
   b) sposobu, w jaki osoba niepowołana uzyskała dostęp do danych osobowych,
   c) rodzaju danych, których dotyczyło naruszenie;
4) wyeliminować czynniki bezpośredniego zagrożenia utraty danych osobowych;
5) sporządzić protokół z wyżej wymienionych czynności;
6) poinformować właściwe organy ścigania w przypadku podejrzenia popełnienia przestępstwa.

§ 19

Administrator danych lub osoba przez niego upoważniona, przy udziale osoby, o której mowa w § 17, obowiązani są do niezwłocznego podjęcia działań mających na celu powstrzymanie lub ograniczenie osobom niepowołanym dostępu do danych osobowych w szczególności przez:

a) zmianę hasła dla administratora i użytkowników;

b) fizyczne odłączenie urządzeń i tych segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie niepowołanej;

c) wylogowanie użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych.

§ 20

Po przeanalizowaniu przyczyn i skutków zdarzenia powodującego naruszenie bezpieczeństwa przetwarzanych danych osobowych, osoby odpowiedzialne za bezpieczeństwo danych osobowych obowiązane są podjąć wszelkie inne działania mające na celu wyeliminowanie podobnych naruszeń w przyszłości oraz zmniejszenie ryzyka występowania ich negatywnych skutków. W szczególności, jeżeli przyczyną naruszenia są:

1) błąd osoby upoważnionej do przetwarzania danych osobowych związany z przetwarzaniem danych osobowych - należy przeprowadzić dodatkowe szkolenie, indywidualne lub grupowe;
2) uaktywnienie wirusa komputerowego - należy ustalić źródło jego pochodzenia oraz wykonać test zabezpieczenia antywirusowego;
3) zaniedbanie ze strony osoby upoważnionej do przetwarzania danych osobowych - należy wyciągnąć konsekwencje zgodnie z przepisami z zakresu prawa pracy o odpowiedzialności pracowników;
4) włamanie - należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających;
5) zły stan urządzenia lub sposób działania programu lub inne niedoskonałości informatycznego systemu przetwarzania danych osobowych - należy niezwłocznie przeprowadzić kontrolne czynności serwisowo - programowe.

§ 21

1. Wykonanie czynności, o których mowa w § 19 i 20, ma na celu przywrócenie prawidłowego działania systemu.
2. W przypadku uszkodzenia urządzeń służących do przetwarzania danych, utraty danych, lub ich zniekształcenia, odtwarza się bazy danych osobowych z ostatniej kopii bezpieczeństwa.

§ 22

1. Administrator danych obowiązany jest sporządzić raport ze zdarzenia naruszającego zabezpieczenia systemu informatycznego, obejmujący wnioski dotyczące całokształtu procesu teleinformatycznego przetwarzania danych osobowych, a w szczególności:
   1) stanu urządzeń wykorzystywanych do przetwarzania danych osobowych;
   2) zawartości zbioru danych osobowych;
   3) prawidłowości działania systemu informatycznego i teleinformatycznego, w którym przetwarzane są dane osobowe z uwzględnieniem skuteczności stosowanych do chwili wystąpienia naruszenia, środków zabezpieczających przed dostępem osób niepowołanych;
   4) jakości działania sieci informatycznej;
   5) wykluczenia obecności wirusów komputerowych;
   6) ustalenia przyczyny i przebiegu zdarzenia;
   7) wyciągnięcia wniosków co do uniknięcia podobnych naruszeń w przyszłości.
2. Raport, o którym mowa w ust. 1, jest przekazywany Administratorowi danych w terminie 30 dni od dnia potwierdzenia zdarzenia naruszenia zabezpieczenia systemu informatycznego.

ROZDZIAŁ XIII
Postanowienia końcowe

§ 23

1. Instrukcja niniejsza nie narusza postanowień powszechnie obowiązującego prawa.
2. W sprawach nieunormowanych stosuje się przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 poz. 1182) oraz przepisy rozporządzenia Ministra Spraw Wewnętrznych i Administracji 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. Nr 100, poz. 1024).

Zatwierdzam

.....

Keller

Rejestr Upoważnień

załącznik do Instrukcji Zarządzania Systemem Informatycznym

L. P.	Data udzielenia upoważnienia	Imię i nazwisko osoby upoważnionej	Numer i seria dokumentu tożsamości	Data przeprowadzenia szkolenia	Podpis osoby upoważnionej	Podpis Administratora

Zatwierdzam:

.....

Polityka bezpieczeństwa przetwarzania danych osobowych

stanowiąca załącznik do Regulaminu Pracy

w

Stowarzyszeniu "Rozwój Bukowiny"

84-311 Bukowina 5

Bukowina, maj 2016

Regulamin Pracy uchwalony w dniu 20.08.2018r. nie wniósł zmian w niniejszej polityce z maja 2016r.

I. Wstęp

§ 1

Celem Polityki Bezpieczeństwa przetwarzania danych osobowych w Stowarzyszeniu "Rozwój Bukowiny", zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania w Stowarzyszeniu "Rozwój Bukowiny" informacji zawierających dane osobowe, a przede wszystkim zapewnienie ochrony danych osobowych przetwarzanych w Stowarzyszeniu "Rozwój Bukowiny" przed wszelkiego rodzaju zagrożeniami, tak zewnętrznymi jak i wewnętrznymi.

§ 2

Polityka Bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz rozporządzeniu Ministra Spraw Wewnętrznych i Administracji 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. Opracowany dokument jest zgodny również z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osób oraz ochrony prywatności w sektorze komunikacji elektronicznej.

§ 3

Obszarem przetwarzania danych osobowych w Stowarzyszeniu "Rozwój Bukowiny" jest teren siedziby Stowarzyszenia "Rozwój Bukowiny" pod adresem Bukowina 5 oraz teren na którym pracują osoby wyznaczone do sprawowania nadzoru oraz reprezentacji Stowarzyszenia "Rozwój Bukowiny".

§ 4

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników.

§ 5

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Stowarzyszeniu "Rozwój Bukowiny" rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   1) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
   2) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
   4) integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
   5) dostępność informacji - rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
   6) zarządzanie ryzykiem - rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§ 6

Administratorem Danych Osobowych przetwarzanych w Stowarzyszeniu Rozwój Bukowiny jest Stowarzyszenie "Rozwój Bukowiny"

§ 7

Jeżeli na Administratora Bezpieczeństwa Informacji w Stowarzyszeniu "Rozwój Bukowiny" zostanie mianowana osoba lub podmiot to będzie on odnotowany w odrębnym aneksie to niniejszej polityki.

II. Definicje

§ 8

Przez użyte w Polityce Bezpieczeństwa określenia należy rozumieć:

1) **Polityka Bezpieczeństwa** – rozumie się przez to Politykę Bezpieczeństwa Ochrony Danych Osobowych w Stowarzyszeniu "Rozwój Bukowiny";

2) **Administrator Danych Osobowych** – dalej jako Administrator danych; rozumie się przez to Stowarzyszenie "Rozwój Bukowiny"
3) **Administrator Bezpieczeństwa Informacji (także ABI)** - rozumie się przez to osobę wyznaczoną przez Administratora Danych Osobowych, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

4) **Biuro** – Sekretariat Zespołu Szkolno Przedszkolnego w Bukowinie
5) **Ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r. poz.1182);
6) **Rozporządzenie** – rozporządzenie Ministra Spraw Wewnętrznych i Administracji 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. z 2004 r. Nr 100, poz. 1024);
7) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
8) **Zbiór danych osobowych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
9) **Baza danych osobowych** – zbiór uporządkowanych powiązanych ze sobą tematycznie zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane osobowe;
10) **Usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dotyczą.
11) **Przetwarzane danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
12) **System informatyczny** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
13) **System tradycyjny** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
14) **Zabezpieczenie danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
15) **Administrator systemu informatycznego** – rozumie się przez to osobę lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi w Stowarzyszeniu "Rozwój Bukowiny"
16) **Użytkownik** - rozumie się przez to upoważnionego przez Administratora danych lub Administratora Bezpieczeństwa Informacji , wyznaczonego do przetwarzania danych osobowych bez możliwości usuwania danych i ingerencji w oryginał zapisów. Osoba ta może być pracownikiem lub członkiem zarządu Stowarzyszenia "Rozwój Bukowiny", który odbył stosowne szkolenie w zakresie ochrony tych danych.

III. Zakres stosowania

§ 9

W Stowarzyszeniu "Rozwój Bukowiny" przetwarzane są przede wszystkim informacje służące do
- zwiększania bezpieczeństwa społeczności szkolnej oraz osób przebywających na terenie zespołu szkolno-przedszkolnego w Bukowinie
- ograniczania zachowań niepożądanych, destrukcyjnych zagrażających zdrowiu, bezpieczeństwu uczniów,
- wyjaśniania sytuacji konfliktowych,
- ustalania sprawców czynów nagannych (bójki, zniszczenia mienia, kradzieże itp.) na terenie całej placówki,
- ograniczania dostępu do terenu ZSP osób nieuprawnionych i niepożądanych,
- zmniejszania ilości zniszczeń na terenie ZSP
- zapewniania bezpiecznych warunków nauki, wychowania i opieki,

-sprawowania nadzoru pedagogicznego

1. Przetwarzany jest wizerunek osób fizycznych w celu wykonywania czynności wymienionych w §9
2. Informacje te są przetwarzane i składowane zarówno w postaci dokumentacji tradycyjnej jak i elektronicznej.
3. Polityka Bezpieczeństwa zawiera dokumenty dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

§ 10

Politykę Bezpieczeństwa stosuje się przede wszystkim do:

1) Danych wizerunkowych i osobowych przetwarzanych w systemach Symfonia, Enova, Płatnik, Microsoft Office , Windows , itp.
2) Wszystkich informacji dotyczących danych pracowników Stowarzyszenia "Rozwój Bukowiny" oraz uczniów ZSP w Bukowinie , w tym danych osobowych pracowników i treści zawieranych umów o pracę.
3) Informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych.
4) Rejestru osób dopuszczonych do przetwarzania danych osobowych.
5) Innych dokumentów zawierających dane osobowe.

§ 11

1. Zakresy ochrony danych osobowych określone przez dokumenty Polityki Bezpieczeństwa mają zastosowanie do systemów informatycznych Izby, w których są przetwarzane dane osobowe, a w szczególności do:
    1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie;
    2) wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
    3) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, stażystów i innych osób mających dostęp do informacji podlegających ochronie, w tym do członków zarządu Stowarzyszenia "Rozwój Bukowiny"
2. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie, w tym członkowie zarządu Stowarzyszenia "Rozwój Bukowiny"

§ 12

Informacje niejawne nie są objęte zakresem niniejszej Polityki Bezpieczeństwa.

IV. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe oraz sposobów ich zabezpieczeń

§ 13

1. Polityka obowiązuje w Stowarzyszeniu "Rozwój Bukowiny", w pomieszczeniach lub częściach pomieszczeń, w których przetwarzane są dane osobowe, a których wykaz został zamieszczony poniżej.
2. Stowarzyszenie "Rozwój Bukowiny" mieści się pod adresem: 4-311 Bukowina 5

1.	Wykaz pomieszczeń, w których przetwarzane są dane osobowe	Wszystkie pomieszczenia oraz teren usytuowany na działce 84-311 Bukowina 5 z wyłączeniem toalet oraz przedsionków toalet.
2.	Wykaz pomieszczeń, w których znajdują się komputery stanowiące element systemu informatycznego	Wszystkie komputery stacjonarne i rejestratory znajdujące się pod adresem 84-311 Bukowina 5 oraz inne komputery przenośne znajdujące się pod adresem osób upoważnionych
3.	Wykaz pomieszczeń, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe	Gabinety i miejsca pracy Członków Zarządu Stowarzyszenia "Rozwój Bukowiny" , Pomieszczenie serwerowni.

4.	Wykaz pomieszczeń, w których składowane są uszkodzone komputerowe nośniki danych (taśmy, dyski, płyty CD, dyski przenośne, uszkodzone komputery)	Pomieszczenie serwerowni.
5.	Wykaz pomieszczeń archiwum	Pomieszczenie serwerowni.
6.	Wykaz programów, w których przetwarzane są dane osobowe	Programy zainstalowane na komputerach Stowarzyszenia "Rozwój Bukowiny" oraz członków Zarządu
7.	Wykaz podmiotów zewnętrznych, które mają dostęp do danych osobowych lub je przetwarzają	Podmioty wykonujące usługi informatyczne posiadające aktualne upoważnienie wpisane w rejestr
8.	Inne	Szafy zamykane na klucz, pokoje zamykane na klucz, budynki chronione, komputery z indywidualnymi hasłami – systemowo wymuszona zmiana co 30 dni

V. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

§ 14

Stowarzyszenie "Rozwój Bukowiny"

Lp	Zbiór Danych	Dział/ jednostka organizacyjna	Program	Lokalizacja bazy danych	Miejsce przetwarzania danych
1.	Np.Dane wizerunkowe osób fizycznych znajdujących się na terenie ZSP	Zarząd Stowarzyszenia "Rozwój Bukowiny"	Programy zainstalowane na komputerach Stowarzyszenia "Rozwój Bukowiny" oraz członków Zarządu	Rejestrator i jednostki komputerowe służące do przekazywania danych	84-311 Bukowina 5
2.	Dane kadrowe, ubezpieczenia , płace , księgowość	Pracownik wyznaczony do pełnienia w/w funkcji	j.w.	j.w.	j.w.

VI. Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych

§ 15

Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych dla programów i systemów stosowanych w Stowarzyszenie "Rozwój Bukowiny" przedstawiają programy zainstalowane na jednostkach komputerowych należących do Stowarzyszenia "Rozwój Bukowiny"

VII. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych

§ 16

1. Zabezpieczenia organizacyjne
   1) sporządzono i wdrożono Politykę Bezpieczeństwa;
   2) sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Krajowej Izbie Doradców Podatkowych;
   3) wyznaczono ABI

4) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora danych bądź osobę przez niego upoważnioną;
5) stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych;
6) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
7) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
8) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
9) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;
10) dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób.

2. Zabezpieczenia techniczne
   1. wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą bramy DNS, FireWall itp.,
   2. stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową,
   3. komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła,
3. Środki ochrony fizycznej:
   1. obszar, na którym przetwarzane są dane osobowe, poza godzinami pracy, chroniony jest alarmem,
   2. obszar, na którym przetwarzane są dane osobowe objęty jest całodobowym monitoringiem,
   3. urządzenia służące do przetwarzania danych osobowych umieszcza się w zamykanych pomieszczeniach.

VIII. Instrukcja postępowania w przypadku zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych

§ 17

1. Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

2. Każdy pracownik bądź członek zarządu Stowarzyszenia "Rozwój Bukowiny" w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować Administratora danych lub ABI
3. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   2) niewłaściwe zabezpieczenie sprzętu, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników.
4. Do typowych incydentów bezpieczeństwa danych osobowych należą:
   1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych),
   3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
5. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator danych lub ABI prowadzi postępowanie wyjaśniające w toku, którego:
   1) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,

2) inicjuje ewentualne działania dyscyplinarne,
3) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,
4) dokumentuje prowadzone postępowania.

6. W przypadku stwierdzenia incydentu (naruszenia), Administratora danych lub ABI prowadzi postępowanie wyjaśniające w toku, którego:
   1) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
   2) zabezpiecza ewentualne dowody,
   3) ustala osoby odpowiedzialne za naruszenie,
   4) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
   5) inicjuje działania dyscyplinarne,
   6) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
   7) dokumentuje prowadzone postępowania.

IX. Zadania Administratora Danych lub Administratora Bezpieczeństwa Informacji

§ 18

Do najważniejszych obowiązków Administratora Danych lub Administratora Bezpieczeństwa Informacji należy:

1. organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,
2. zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki,
3. **wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,**
4. **prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,**
5. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych, prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
6. nadzór nad bezpieczeństwem danych osobowych,
7. kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
8. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych

§ 19

Administrator Bezpieczeństwa Informacji ma prawo:

1) wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w Stowarzyszeniu "Rozwój Bukowiny";
2) wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą;
3) żądania złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego;
4) żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli;
5) żądania udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

X. Zadania Administratora Systemu Informatycznego

§ 20

1. Administrator Systemu Informatycznego odpowiedzialny jest za:
   1) Bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych.
   2) Optymalizację wydajności systemu informatycznego, baz danych, instalacje i konfiguracje sprzętu sieciowego i serwerowego.
   3) Instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego.

4) Konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem.
5) Nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych.
6) Współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych.
7) Zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego.
8) Zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie.
9) Przeciwdziałanie próbom naruszenia bezpieczeństwa informacji.
10) Przyznawanie na wniosek Administratora danych lub Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do informacji w danym systemie.
11) Wnioskowanie do Administratora danych lub Administratora Bezpieczeństwa Informacji w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń.
12) Zarządzanie licencjami, procedurami ich dotyczącymi.
13) Prowadzenie profilaktyki antywirusowej.

2. Praca Administratora Systemu Informatycznego jest nadzorowana pod względem przestrzegania ustawy o ochronie danych osobowych, Rozporządzenia Ministra Spraw Wewnętrznych i Administracji 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 oraz Polityki Bezpieczeństwa przez Administratora danych lub Administratora Bezpieczeństwa Informacji.

XI. Sprawozdanie roczne stanu systemu ochrony danych osobowych

§ 21

1. Corocznie do dnia 15 marca ABI lub wyznaczony przez Administratora danych pracownik **przygotowuje sprawozdanie roczne stanu funkcjonowania systemu ochrony danych osobowych,**
2. W spotkaniu sprawozdawczym uczestniczą: Administrator danych oraz ABI. Na wniosek co najmniej jednego z uczestników w spotkaniu mogą wziąć udział: członkowie zarządu, informatyk, kierownicy działów/jednostek.
3. Sprawozdanie przygotowywane jest w formie pisemnej.

XII. Szkolenia użytkowników

§ 22

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada Administrator danych lub ABI
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora danych, a także o zobowiązaniu się do ich przestrzegania.
4. Szkolenie zostaje **zakończone podpisaniem przez słuchacza oświadczenia** o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.
5. Dokument ten jest **przechowywany w aktach osobowych** użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

XIII. Postanowienia końcowe

§ 23

1. Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.

Keller

Załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

- Stanowi Załącznik do Polityki Bezpieczeństwa Przetwarzania danych osobowych

A. Środki bezpieczeństwa na poziomie podstawowym

I

Obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

Przebywanie osób nieuprawnionych w obszarze, o którym mowa w § 4 pkt 1 rozporządzenia, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

II

1. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.
2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:
   w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;
   dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

IV

1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 6 znaków.
3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
4. Kopie zapasowe:
   a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
   b) usuwa się niezwłocznie po ustaniu ich użyteczności.

V

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, o którym mowa w § 4 pkt 1 rozporządzenia, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

VI

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

1) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
3) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

VII

Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego

2. Administrator danych lub Administrator Bezpieczeństwa Informacji ma obowiązek zapoznać z treścią Polityki każdego użytkownika.
3. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
4. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.
5. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
6. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
7. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy oraz rozporządzenia.

Zatwierdzam

.....

B. Środki bezpieczeństwa na poziomie podwyższonym

VIII

W przypadku gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

IX

Urządzenia i nośniki zawierające dane osobowe, o których mowa w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przekazywane poza obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

X

Instrukcja zarządzania systemem informatycznym, o której mowa w § 5 rozporządzenia, rozszerza się o sposób stosowania środków, o których mowa w pkt IX załącznika.

XI

Administrator danych stosuje na poziomie podwyższonym środki bezpieczeństwa określone w części A załącznika, o ile zasady zawarte w części B nie stanowią inaczej.

C. Środki bezpieczeństwa na poziomie wysokim

XII

1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one:

   a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;
   b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

XIII

Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

XIV

Administrator danych stosuje na poziomie wysokim środki bezpieczeństwa, określone w części A i B załącznika, o ile zasady zawarte w części C nie stanowią inaczej.

Zarządzenie

Zarządu Stowarzyszenia "Rozwój Bukowiny" 84-311 Bukowina 5

z dnia 20.08.2018r.

w sprawie zmiany treści "Polityki Zatrudniania" stanowiącej załącznik do Regulaminu Pracy w Stowarzyszeniu "Rozwój Bukowiny"

I. Działając na podstawie art. 77^2 Kodeksu Pracy ustawy z dnia 23.12.1997r. (Dz. U. z 1998r. Nr 21, poz. 94 z późn. zmian.) Zarząd wprowadza z dniem **01.09.2018r.** w brzmieniu obowiązującym "Politykę Zatrudniania" dla wszystkich pracowników stanowiący załącznik do niniejszego zarządzenia.

II. Polityka Zatrudniania w dniu 01.09.2018r. zostaje przekazana do wiadomości pracownikom.

III. Każdy pracownik przez zapoznanie się z Regulaminem Pracy, lub podpisanie odpowiedniej umowy, albo aneksu przyjmuje do wiadomości niniejszą "Politykę Zatrudniania"

Zarząd Stowarzyszenia "Rozwój Bukowiny"