PODRĘCZNIK BEZPIECZEŃSTWA

Wersja 3.0

	Imię i Nazwisko	Stanowisko służbowe	Data	Podpis
Opracował	N-serwis Sp. Z.o.o			
Sprawdził				
Zatwierdził:				

1 SPIS TREŚCI

2 Pojęcia i definicje 2
3 Postępowanie w przypadku przyjęcia nowego pracownika 3
4 Udzielanie informacji przez telefon 3
5 Zasady ochrony fizycznej i zabezpieczania dokumentacji 3
5.1 Podstawowe zasady zabezpieczania danych 3
6 Zasady ochrony danych w systemach informatycznych 4
6.1 Polityki haseł i uwierzytelnianie użytkowników 4
6.2 Korzystanie z oprogramowania i systemów informatycznych 5
6.3 Zasady korzystania z poczty elektronicznej 5
6.4 Korespondencja z kontrahentami i podmiotami zewnętrznymi 6
6.5 Wysyłanie wiadomości do wielu odbiorców 6
7 Zasady korzystania z Internetu 6
8 Postępowanie w przypadku wystąpienia naruszenia 7
9 Obowiązki pracowników w zakresie ochrony danych 7
10 Odpowiedzialność z tytułu nieprzestrzegania przepisów 7
11 Dokumenty związane 8

2 POJĘCIA I DEFINICJE

1) **Dane osobowe** –wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Za osobę możliwą do zidentyfikowania przyjmuje się osobę, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.
2) **Administrator Danych (AD)** –rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 4, ust. 7 RODO, decydujący o celach i środkach przetwarzania danych osobowych, dalej AD lub Spółdzielnia.
3) **System informatyczny** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
4) **Administrator Systemu Informatycznego (ASI)** – osoba lub dział zajmujący się w szczególności nadzorowaniem pracy serwerów, zarządzaniem kontami użytkowników, konfiguracją komputerów, instalowaniem oprogramowania, dbaniem o bezpieczeństwo systemu i opcjonalnie samych danych, nadzorowanie, wykrywanie i eliminowanie nieprawidłowości, asystowaniem i współpracą z zewnętrznymi specjalistami przy pracach instalacyjnych, konfiguracyjnych i naprawczych oraz innych zadań wynikających z zaleconych obowiązków;
5) **Inspektor Ochrony Danych (IOD)** - osoba nadzorująca z upoważnienia AD przestrzeganie obowiązujących przepisów o ochronie danych osobowych oraz stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w sposób odpowiedni do zagrożeń oraz kategorii danych objętych ochroną, zgodnie z obowiązkami określonymi w art. 37-39 RODO. Kontakt z IOD możliwy jest pod adresem poczty elektronicznej: iod@smpraszka.com.pl
6) **Użytkownik systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych zarejestrowaną w systemie informatycznym AD.
7) **Sieć lokalna** – należy przez to rozumieć połączenie systemów informatycznych AD wyłącznie dla jego własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.
8) **Sieć publiczna** – należy przez to rozumieć publiczną sieć telekomunikacyjną w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

9) **Użytkownik zdalny** - użytkownik systemu łączący się z sieci rozległej z systemem informatycznym AD znajdującym się w sieci lokalnej, lub pracujący zdalnie na danych poza siedzibą AD.
10) **Program komputerowy** – zbiór instrukcji, które po umieszczeniu na rozpoznawalnym przez maszynę nośniku i automatycznym przetłumaczeniu na język zrozumiały dla tej maszyny powoduje, że osiąga on zdolność do wykonywania danej czynności lub też wykonuje daną czynność.
11) **Serwer** - wyróżniony komputer świadczący usługi na rzecz mających z nim łączność innych komputerów np. Przechowujący pliki, pośredniczący w przekazywaniu poczty itp.
12) **Baza danych** - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. W pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze rekordów lub obiektów, w których są zapisane dane jednostkowych obiektów.
13) **Kopie bezpieczeństwa (zapasowe)** – kopie plików danych lub plików programowania tworzone na nośniku wymiennym lub dysku twardym komputera w celu ich odtworzenia w przypadku utraty lub uszkodzenia danych.
14) **Teletransmisja (przesyłanie) danych** - przesyłanie danych przy pomocy dostępnych łączy.
15) **Plik** – nośnik informacji, ciąg bajtów posiadający swoją nazwę odróżniającą ją od innych plików i parametry: rozmiar, datę powstania lub datę ostatniej modyfikacji itp.
16) **Nośnik komputerowy (wymienny, lub pamięć/nośnik przenośny)** – nośnik służący do zapisu informacji, np. Dyskietka, taśma, płyta CD, wymienny dysk twardy, pamięć typu „pendrive" lub jakakolwiek inna forma pamięci nadająca się do przenoszenia danych (np. Pamięć w urządzeniach tj. Smartphone).
17) **Szkodliwe oprogramowanie** – (np. Tzw. Wirus, koń trojański itd.) Program, który uaktywniony w pamięci operacyjnej, powoduje wadliwe działanie, zniszczenie lub modyfikację systemu operacyjnego, programu komputerowego lub danych, program, który udaje pracę innego legalnego programu, a w międzyczasie wykonuje szereg niepożądanych czynności (np. Fałszywy program „login" kradnie hasło użytkownika).

3 POSTĘPOWANIE W PRZYPADKU PRZYJĘCIA NOWEGO PRACOWNIKA

1. W momencie rozpoczęcia współpracy z nową osobą (pracownikiem, zleceniobiorcą, praktykantem, stażystą lub osobą fizyczną prowadzącą działalność gospodarczą) osoba odpowiedzialna za przygotowanie umowy jest zobowiązana przedstawić osobie do podpisu oświadczenie o zachowaniu poufności oraz zadbać o nadanie odpowiedniego **Upoważnienia do przetwarzania danych osobowych**, zgodnie z załącznikami do Polityki Bezpieczeństwa Danych Osobowych.
2. W przypadku, gdy osoba nie będzie miała do czynienia z danymi osobowymi, stosuje się oświadczenie o zachowaniu poufności. Oświadczenie o zachowaniu poufności może również mieć postać odrębnej umowy o zachowaniu poufności w przypadku osób fizycznych prowadzących działalność gospodarczą, lub odpowiednich zapisów zawartych w umowie głównej w zależności od ustaleń między stronami umowy.
3. Jeśli nowozatrudniona osoba ma mieć dostęp do systemu informatycznego, w którym przetwarzane są dane osobowe – przełożony tej osoby uzupełnia pisemny **Wniosek o nadanie/zmianę/odebranie uprawnień w systemie**.
4. Wypełniony wniosek przekazywany jest do ASI, a ten tworzy konto w systemie i nadaje osobie uprawnienia zgodnie z wnioskiem.
5. Także zmiana lub odebranie uprawnień odbywa się na podstawie pisemnego **Wniosku o nadanie/zmianę/odebranie uprawnień w systemie**. Odebrania lub zmiany zakresu uprawnień dokonuje ASI.
6. W przypadku odebrania uprawnień identyfikator osoby nie jest przydzielany ponownie żadnej innej osobie.
7. Dostęp do wszystkich systemów przetwarzających dane osobowe wymaga uwierzytelnienia. Jeśli do uwierzytelnienia wymagane jest hasło, musi się ono składać min. Z 10 znaków oraz zawierać małą i dużą literę oraz cyfrę lub znak specjalny.
8. Pierwsze hasło podawane jest użytkownikowi ustnie przez ASI, po pierwszym logowaniu wymagana jest zmiana hasła.
9. Hasła do systemów są zmieniane raz na 90 dni. W przypadku, gdy zmiana hasła nie jest wymuszana systemowo, użytkownik zobowiązany jest do samodzielnej zmiany hasła.

4 UDZIELANIE INFORMACJI PRZEZ TELEFON

Nie należy udzielać telefonicznie informacji o danych osobowych instytucjom, podmiotom zewnętrznym (np. Bankom) oraz osobom trzecim. W takich sytuacjach należy zwrócić się do strony o przekazanie wniosku o udostępnienie danych w formie pisemnej (na adres korespondencyjny AD lub poprzez skierowanie pisma na adres: smpraszka@interia.pl

5 ZASADY OCHRONY FIZYCZNEJ I ZABEZPIECZANIA DOKUMENTACJI

5.1 PODSTAWOWE ZASADY ZABEZPIECZANIA DANYCH

1. Wszystkie dokumenty zawierające dane osobowe w formie papierowej po zakończonej pracy muszą być przechowywane w zamykanych szafach bądź szafkach. Klucze do szaf należy zabezpieczyć przed dostępem osób nieupoważnionych, w tym również osób sprzątających.

2. Ekrany monitorów stanowisk dostępu do danych osobowych muszą zostać wyłączone nie później niż po 10 minutach nieaktywności pracownika.
3. Ustawienie ekranu komputera lub innego urządzenia służącego pracy w sposób uniemożliwiający osobom nieupoważnionym podejrzenie wyświetlanej na nim informacji – dotyczy to również podejrzenia informacji przez osobę wchodzącą do pomieszczenia, bez względu na to czy jest pracownikiem czy osobą trzecią. Dopuszcza się również stosowanie filtrów prywatyzujących zabezpieczających przed wglądem osób nieupoważnionych w treści wyświetlane na ekranie monitorów.
4. Po opuszczeniu pomieszczenia przez ostatnią osobę upoważnioną należy sprawdzić, czy zostały pozamykane wszystkie szafki/szafy oraz czy został wyłączony sprzęt i urządzenia peryferyjne.
5. Nie należy pozostawiać kluczy w drzwiach do pomieszczeń (od strony zewnętrznej) podczas pracy oraz kluczy w szafkach po zakończonej pracy. Wszystkie klucze należy zabezpieczyć poprzez schowanie.
6. Dokumenty zawierające dane osobowe po ustaniu przydatności należy niszczyć w sposób mechaniczny za pomocą niszczarek dokumentów. Zabronione jest wyrzucanie dokumentacji zawierającej dane osobowe (np. Po ustaniu okresu jej przydatności, czy też błędnie sporządzonej) do kosza.
7. Po zakończeniu drukowania pracownik jest zobowiązany do niezwłocznego zabrania wydrukowanych dokumentów z urządzenia.
8. Nie należy pozostawiać osób postronnych (np. Kontrolerów, audytorów, kurierów, gości i innych stron trzecich) w pomieszczeniach, gdzie przetwarzane są dane osobowe, bez nadzoru pracowników AD. W przypadku, gdy istnieje konieczność opuszczenia pomieszczenia przez pracownika, osoby postronne nie powinny przebywać w pomieszczeniu bez nadzoru i należy poprosić o nadzór innego pracownika lub wyprosić osobę trzecią do części ogólnodostępnej.

6 ZASADY OCHRONY DANYCH W SYSTEMACH INFORMATYCZNYCH

1. Każda osoba posiada swój login i hasło do komputera oraz systemów informatycznych, i jest zobowiązana do tego, aby nie ujawniać haseł ani danych do logowania innym osobom, również innym pracownikom.
2. Pracownik odpowiada za zachowanie poufności swojego hasła, zatem nieuprawnione jest:
   - Zapisywanie haseł;
   - Korzystanie z funkcji zapamiętywania haseł;
   - Przekazywanie haseł innym osobom;
   - Pozostawianie haseł w widocznych miejscach.
3. Jeśli do uwierzytelnienia wymagane jest hasło, musi się ono składać min. Z 10 znaków oraz zawierać małą i dużą literę oraz cyfrę lub znak specjalny. Odchodząc od komputera za każdym razem należy się wylogować poprzez naciśnięcie kombinacji klawiszy Ctrl + Alt + Del lub Windows + L.
4. Po zakończeniu pracy należy wylogować się z wszystkich programów i aplikacji oraz wyłączyć komputer.

6.1 POLITYKI HASEŁ I UWIERZYTELNIANIE UŻYTKOWNIKÓW

1. Dostęp do Informacji objętych obowiązkiem zachowania poufności wprowadzonych lub dostępnych za pośrednictwem systemów informatycznych wykorzystywanych przez Spółdzielnię może być realizowany wyłącznie po poprawnym uwierzytelnieniu użytkownika.
2. Proces logowania oraz autoryzacja dostępu do systemów informatycznych wykorzystywanych przez Spółdzielnię musi spełniać następujące wymogi:
   - Brak możliwości ominięcia procesu uwierzytelniania do systemu informatycznego;
   - Proces musi wymuszać użycie indywidualnych identyfikatorów i haseł oraz musi zapewniać rozliczalność żądań dostępu;
   - Wprowadzanie hasła do systemu musi być realizowane w postaci uniemożliwiającej jego bezpośrednie odczytanie - hasło nie może być widoczne podczas wpisywania go na ekranie w formie jawnej;
   - Proces uwierzytelniania powinien, o ile jest to technicznie możliwe, ujawniać jak najmniejszą ilość informacji w trakcie swojego przebiegu, tak aby nie pozwolić nieuprawnionemu użytkownikowi na uzyskanie dodatkowych wskazówek, np. Brak wyświetlania identyfikatora ostatniego zalogowanego użytkownika, brak informacji o typie błędu przy uwierzytelnianiu, czyli brak informacji, iż użytkownik podał błędne hasło - wyświetlenie jedynie ogólnej informacji, że nazwa użytkownika lub hasło są nieprawidłowe;
   - Umożliwiać okresowe wymuszanie zmiany haseł, w tym wymuszać zmianę haseł tymczasowych przy pierwszym zalogowaniu.
3. Tworzone hasła dostępu nie powinny być złożone z pojedynczych wyrazów, skrótów, nazw własnych czy jakichkolwiek słów występujących w słowniku (zarówno w języku polskim jak i językach obcych). Hasła nie mogą też być prostymi transformacjami tych słów (np. Poprzez zapisania wspak czy poprzez podstawnie '@' zamiast 'a', '$' zamiast S, itd.).
4. Przy tworzeniu haseł należy unikać używania ciągów sąsiadujących ze sobą znaków na klawiaturze jako haseł. Hasła nie powinny być powiązane z osobą użytkownika w jakikolwiek możliwy do odgadnięcia sposób (np. Identyfikator użytkownika, imię, nazwisko użytkownika, data urodzenia, numer telefonu, itd.).

5. Zdalny dostęp do systemów informatycznych Spółdzielni jest możliwy tylko poprzez technologie zapewniające akceptowalny poziom bezpieczeństwa, w szczególności rozwiązania zapewniające wiarygodny proces uwierzytelniania, nadzorowany przez ASI.

6.2 KORZYSTANIE Z OPROGRAMOWANIA I SYSTEMÓW INFORMATYCZNYCH

Spółdzielnia przyjmuje następujące zasady korzystania z oprogramowania:

1. Pracownik zobowiązuje się do korzystania wyłącznie z oprogramowania objętego prawami autorskimi i nie ma prawa kopiować oprogramowania zainstalowanego na powierzonym sprzęcie na swoje własne potrzeby ani na potrzeby osób trzecich;
2. Instalowanie jakiegokolwiek oprogramowania na powierzonym sprzęcie może być dokonane wyłącznie przez osobę upoważnioną. Pracownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez AD.
3. Pracownicy nie mają prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez ASI.
4. W przypadku naruszenia któregokolwiek z powyższych postanowień AD ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.

Ilekroć pracownik uzyska, w związku z realizacją obowiązków pracowniczych bądź zobowiązań umownych, dostęp do systemów informatycznych Spółdzielni, przez co w szczególności należy rozumieć również dostęp do firmowego konta pocztowego bądź sieci wewnętrznej wykorzystywanej w Spółdzielni, zobowiązany jest przestrzegać następujących zasad:

- Zakazane jest przechowywanie plików zawierających informacje objęte obowiązkiem zachowania poufności na pulpicie;
- Zabronione jest logowanie się do systemów informatycznych z użyciem danych identyfikacyjnych innych osób;
- Zabronione jest fotografowanie i filmowanie systemów zabezpieczeń, pomieszczeń technicznych i pomieszczeń serwerowni, o ile nie uzyskano na to uprzedniej pisemnej zgody osoby upoważnionej do jej udzielenia lub bezpośrednio Zarządu;
- Użytkownik w przypadku stwierdzenia niezgodności wyświetlonej daty oraz czasu logowania ze stanem ostatniego faktycznego logowania jest zobowiązany do natychmiastowego zgłoszenia incydentu do ASI oraz do IOD.

6.3 ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

Spółdzielnia przyjmuje następujące zasady przyznania służbowego konta poczty elektronicznej pracownikowi:

1. Każdemu pracownikowi może zostać udostępnione konto pocztowe.
2. Adres konta pocztowego tworzony jest wg stałego wzorca dla wszystkich pracowników w domenie smpraszka.com.pl.
3. Założenie konta, w tym schemat zarządzania uprawnieniami i kontroli dostępu, odbywa się zgodnie z **Procedurą Zarządzania Systemem Informatycznym.**
4. Konto pocztowe jest aktywne dla użytkownika na czas trwania zatrudnienia lub współpracy (w zależności od formy zatrudnienia i zawartej umowy). W sytuacji zakończenia zatrudnienia lub współpracy, poczta może być udostępniona bezpośredniemu przełożonemu w uzasadnionych przypadkach, w ramach ochrony tajemnicy przedsiębiorstwa oraz zapewnienia ciągłości ustaleń poczynionych z klientem/stroną trzecią, lecz z poszanowaniem prywatności korespondencji użytkownika. Przy dłużej nieobecności konta użytkownika mogą być blokowane na wniosek przełożonego.

Zasady korzystania z służbowego poczty elektronicznej przez użytkowników są następujące:

1. Użytkownik jest zobowiązany do korzystania z przyznanego mu adresu mailowego do wszelkiej korespondencji z innymi pracownikami wewnątrz organizacji, klientami oraz innymi podmiotami wyłącznie celem realizacji komunikacji służbowej.
2. Użytkownik nie może posługiwać się prywatną (spoza domeny) pocztą email w celach służbowych.
3. Użytkownik może posługiwać się pocztą email wyłącznie w celach zgodnych z prawem, przestrzegając między innymi prawa autorskiego, praw własności intelektualnej oraz wszelkich innych przepisów których złamanie mogłoby narazić pracodawcę na szkodę, straty finansowe, wizerunkowe lub konsekwencje prawne.
4. Jeśli przedmiotem korespondencji są jakiekolwiek dane osobowe, które nie mogą być publicznie dostępne, nie należy ich umieszczać w treści wiadomości, a w załączniku do wiadomości, który należy zabezpieczyć hasłem. Hasło należy przekazać inną drogą niż mail (telefonicznie, smsem, osobiście).
5. Użytkownik nie może posługiwać się służbowym adresem email w celach prywatnych oraz rejestrować służbowego adresu poczty elektronicznej w serwisach internetowych niezwiązanych z wykonywaną pracą.
6. W przypadku uzyskiwania dostępu do poczty email spoza siedziby Spółdzielni, użytkownik zobowiązany jest do zachowania szczególnej ostrożności, w szczególności niedozwolone jest logowanie do systemów z:
   - Sieci ogólnodostępnych typu hotspot;
   - Komputerów ogólnodostępnych np. W hotelach, kawiarniach internetowych;
   - Komputerów współużytkowanych przez inne osoby (np. Dzieci);
   - Komputerów co do których zachodzi podejrzenie, że mogły zostać zainfekowane szkodliwym oprogramowaniem.
7. Podczas pracy z systemem pocztowym użytkownik zobowiązany jest do:
   - Zapewniania poufności danych uwierzytelniających (loginu i hasła);
   - Zapewnienia poufności korespondencji poprzez ograniczenie wglądu do danych osób postronnych;

- Nie otwierania i zapisywania załączników lokalnie na dysku, lecz wyłącznie w wydzielonych zasobach sieciowych;
- Komputerów co do których zachodzi podejrzenie że mogły zostać zainfekowane szkodliwym oprogramowaniem.

8. Każda korespondencja wysyłana przez użytkownika musi zawierać:
   - Imię i nazwisko nadawcy;
   - Tytuł wiadomości;
   - Zunifikowaną, firmową stopkę zawierającą dane identyfikujące osobę jak i organizację;
   - Klauzulę dotyczącą zachowania poufności: *„Niniejsza korespondencja przeznaczona jest wyłącznie dla osoby lub firmy, do której jest zaadresowana. Dalsze przekazywanie wiadomości otrzymanej omyłkowo, rozpowszechnianie lub innego rodzaju wykorzystanie, podejmowanie jakichkolwiek działań w oparciu o zawarte w niej informacje przez osobę lub podmiot nie będący adresatem, jest niedozwolone. Odbiorca korespondencji, który otrzymał ją omyłkowo, proszony jest o zawiadomienie nadawcy i usunięcie tego materiału z komputera".*
   - Informację dotyczącą przetwarzania danych osobowych: *„Informacje dotyczące zasad przetwarzania danych osobowych oraz praw osób, których dane dotyczą i sposobu ich realizacji dostępne są opublikowane na stronie internetowej Spółdzielni pod adresem:* smpraszka@interia.pl
9. Użytkownik ponosi pełną odpowiedzialność za sposób wykorzystywania poczty email i treść przesyłanej korespondencji.
10. Użytkownik przyjmuje do wiadomości że administrator poczty może uzyskiwać dostęp do przesyłanej poczty email w celach dowodowych.
11. Wszelkie nieprawidłowości w pracy systemu pocztowego należy zgłaszać ASI.
12. Administrator w dowolnym momencie może zablokować użytkownikowi dostęp do konta pocztowego w przypadku
    - Wielokrotnych prób błędnego uwierzytelnienia;
    - Niestosowania się do zaleceń dokumentacji ochrony danych osobowych oraz innych dokumentów stanowiskowych określających bezpieczne zasady pracy;
    - Blokada może być trwała lub obowiązywać do czasu wyjaśnienia nieprawidłowości.
13. W przypadku, gdy użytkownik, niezależnie od nadawcy, **NIE SPODZIEWA SIĘ** otrzymać wiadomości email zawierającej dodatkowe dokumenty w załączniku lub w postaci pliku do pobrania, powinien powstrzymać się od otwarcia takiej wiadomości na czas 48h od czasu jej otrzymania i poinformować ASI, który dokona sprawdzenia załącznika pod kątem bezpieczeństwa informacji.

6.4 KORESPONDENCJA Z KONTRAHENTAMI I PODMIOTAMI ZEWNĘTRZNYMI

1. Nie należy realizować wniosków o udostępnienie danych osobowych, które zostały dostarczone jako wiadomość e- mail, w ten sposób nie należy też udzielać odpowiedzi – udostępnianie wymaga zachowania formy pisemnej.
2. W przypadku stałej współpracy z kontrahentem, któremu przekazywane są dane osobowe (np. Kancelaria prawna) można te dane przekazać mailem.
3. Danych osobowych nie należy umieszczać w treści wiadomości, a w załączniku do wiadomości, który należy zabezpieczyć hasłem. Hasło należy przekazać inną drogą niż mail (telefonicznie, smsem, osobiście). Ze stałym kontrahentem można umówić się na stałe hasło, z okresową jego zmianą.

6.5 WYSYŁANIE WIADOMOŚCI DO WIELU ODBIORCÓW

1. W przypadku wysyłania wiadomości do wielu odbiorów, którzy się nie znają (np. W przypadku życzeń świątecznych) ich adresy mailowe należy umieścić w polu UDW: wiadomości (ukryte do wiadomości).
2. Nie należy używać w takich wiadomościach (w tym masowej wysyłce) pola DO: W przeciwnym przypadku, wysłanie takiej wiadomości traktowane jest jako naruszenie ochrony danych osobowych i wymaga zgłoszenia do IOD.

7 ZASADY KORZYSTANIA Z INTERNETU

W Spółdzielni przyjmuje się następujące zasady korzystania z Internetu:

1. Pracownicy mają prawo korzystać z Internetu w celu wykonywania obowiązków służbowych.
2. Przy korzystaniu z Internetu, pracownicy mają obowiązek przestrzegać prawa własności przemysłowej, praw ochrony własności intelektualnej i praw autorskich. Pracownicy nie mają prawa korzystać z Internetu w celu przeglądania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec obowiązujących zasad postępowania.
3. W zakresie dozwolonym przepisami prawa, AD zastrzega sobie prawo kontrolowania sposobu korzystania przez pracownika z Internetu pod kątem wyżej opisanych zasad. Ponadto, w uzasadnionym zakresie, AD zastrzega sobie prawo kontroli czasu spędzanego przez pracownika w Internecie.
4. Pracodawca może również blokować dostęp do niektórych treści dostępnych przez Internet.

8 POSTĘPOWANIE W PRZYPADKU WYSTĄPIENIA NARUSZENIA

W przypadku naruszenia ochrony danych osobowych należy postępować zgodnie z wytycznymi Polityki bezpieczeństwa danych osobowych. W przypadku naruszeń dotyczących systemów informatycznych (np. Podejrzenie wirusa, ransomware lub inne problemy związane z infrastrukturą teleinformatyczną) należy poinformować również ASI.

9 OBOWIĄZKI PRACOWNIKÓW W ZAKRESIE OCHRONY DANYCH

Każdy pracownik zobowiązany jest zachować w poufności dane osobowe, z którymi styka się w związku z pełnieniem obowiązków oraz dbać o bezpieczeństwo przetwarzanych danych. Pracownik jest zobowiązany przetwarzać dane tylko w zakresie niezbędnym do realizacji zadań służbowych – zgodnie z nadanym upoważnieniem. Zabronione jest np. Pozyskiwanie szerszego zakresu danych niż wynika to z wewnętrznych przepisów Spółdzielni, przekazywanie danych służbowych osobom (także innym pracownikom),którzy nie są do tego upoważnieni zgodnie ze swoim zakresem obowiązków służbowych.

Obowiązkiem pracownika jest informowanie o dostrzeżonych naruszeniach bezpieczeństwa przetwarzanych danych lub wystąpieniu sytuacji, które mogą do takiego naruszenia doprowadzić.

Każdy pracownik powinien zapoznać się z dokumentacją ochrony danych osobowych, w szczególności niniejszym Podręcznikiem i Polityką bezpieczeństwa danych osobowych oraz poświadczyć pisemnie fakt takiego zapoznania.

10 ODPOWIEDZIALNOŚĆ Z TYTUŁU NIEPRZESTRZEGANIA PRZEPISÓW

Pracownik i osoby wykonujące pracę na rzecz Spółdzielni odpowiedzialni są za wywiązywanie się z zakresu obowiązków oraz ponoszą odpowiedzialność za potencjalne szkody wyrządzone AD. W przypadku naruszenia tajemnicy przedsiębiorstwa lub ochrony danych osobowych, pracownik może zostać pociągnięty do odpowiedzialności przez pracodawcę oraz osobę, której dane dotyczą i której wyrządzono szkodę. Odpowiedzialność pracowników realizowana może być w szczególności z tytułu: przepisów prawa pracy (w szczególności Kodeksu pracy), przepisów o ochronie danych osobowych (RODO, ustawa o ochronie danych osobowych), przepisów prawa cywilnego, (w szczególności Kodeksu cywilnego), przepisów prawa karnego (w szczególności Kodeksu karnego), przepisów praw autorskich i praw pokrewnych. .

Wśród przepisów dotyczących odpowiedzialności z tytułu ochrony informacji oraz ochrony danych osobowych wymienia się co następuje:

- **Art. 107 ustawy o ochronie danych osobowych** – *Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne, albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Jeżeli czyn dotyczy danych (szczególnej kategorii – przyp. Aut.)Ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności lub pozbawienia wolności do lat 3.*
- **Art. 266 Kodeksu karnego** – *Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*
- **Art. 267 Kodeksu karnego** – *Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem. Tej samej karze podlega, kto informację uzyskaną w sposób określony powyżej ujawnia innej osobie.*
- **Art. 268 Kodeksu karnego** – *Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Jeżeli czyn dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3. Kto, dopuszczając się czynu, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.*
- **Art. 269a Kodeksu karnego** – *Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.*
- **Art. 269b Kodeksu karnego** – *Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3.*
- **Art. 23. Kodeksu cywilnego** - *Dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach.*
- **Art. 24. § 1 Kodeksu cywilnego** - *Ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się*

naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny.

- **Art. 24 § 2. Kodeksu cywilnego** - *Jeżeli wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych. § 3. Przepisy powyższe nie uchybiają uprawnieniom przewidzianym w innych przepisach, w szczególności w prawie autorskim oraz w prawie wynalazczym.*

11 DOKUMENTY ZWIĄZANE

1. Polityka Bezpieczeństwa Danych Osobowych
2. Procedura Zarządzania Systemem Informatycznym

Zatwierdzono na posiedzeniu
Zarządu w dn. **14.11.2023 r.**
Prot. nr **11/2023,** uchwała nr **54 /2023**

SPÓŁDZIELNIA MIESZKANIOWA
w Praszce
ul. A. Mickiewicza 18
46-320 Praszka
tel. 34 35 91 046, fax 34 35 91 330
NIP 576-000-63-85, REGON 000130244