ПОЛИТИКА ЗА ИНФОРМАЦИОННАТА СИСТЕМА И ДОКУМЕНТООБОРОТА

Ръководството на Синдикална Взаимозастрахователна Кооперация (СиВЗК), в лицето на Управителния съвет, официално декларира Политиката по ИНФОРМАЦИОННА СИГУРНОСТ на информационните ресурси на СиВЗК в обхвата на дейността на Кооперацията по животозастраховане.
Политиката е документирана, огласена и разбрана от всички служители, които имат достъп до информацията и информационните системи на СиВЗК. Политиката е одобрена от УС и се прилага в рамките на цялата Кооперация. Политиката по информационната сигурност се поддържа от Ръководителя на ИТ проекти.
Настоящата политика по информационна сигурност задава рамката на система от мерки, насочени към:

- Гарантиране на конфиденциалност на информацията, чрез прилагането на одобрени ограничения върху достъпа и разкриването на информация;
- Осигуряване на цялостност на информацията, чрез защита срещу неправомерни изменения или разрушаване на информация;
- Осигуряване на достъпност на информацията, чрез осигуряване на надежден и навременен достъп на информацията;
- Постигане на отчетност на информацията, чрез въвеждане на контрол върху достъпа и правата върху информационните ресурси.

Обхват на системата за управление на информационната сигурност:

Териториален обхват:
Системата за управление на информационната сигурност обхваща централния офис на СиВЗК в сградата на пл. Македония № 1 в гр. София.
Обхват на процесите:
Системата за управление на информационната сигурност обхваща следните процеси:

- Приемане и обработване на заявления и други документи за полици;
- Създаване и отпечатване на застрахователни полици и сертификати;
- Приемане и обработване на премии;
- Превеждане на субсидии;
- Изчисление и превеждане на суми по застрахователни събития;
- Извеждане на справки за застрахователната дейност;
- Изготвяне на отчети;
- Периодично архивиране и съхранение на електронната информация и досиета по полиците.

Обхват на информационните ресурси:

Системата за управление на информационната сигурност (СУИС) обхваща всички документи, записи и информация (в електронен вид и на хартия) намиращи се или касаещи:

- Системи за връзки с клиенти;
- Системи за управление на застрахователната дейност;
- Бази данни;
- Компютри, в т.ч. преносими;
- Софтуерни активи;
- Локална мрежа;
- Електронната страница на кооперацията;
- Носители на информация (дискове, USB памети и др.);
- Устройства за копиране и предаване на данни;
- Комуникационни устройства;
- Инфраструктура на Кооперацията (електрозахранване, кабели за локална мрежа и др.) ;
- Персонал.

Целите на настоящата политика са:

- Осигуряване на непрекъснатост на застрахователната дейност;
- Минимизиране на рисковете за сигурността на информацията, причиняващи загуби или вреди на СиВЗК, нейните клиенти, партньори и други заинтересовани страни;
- Минимизиране на степента на загуби или вреди, причинени от пробиви в информационната сигурност;
- Осигуряване на необходимите ресурси за внедряване на ефективна СУИС;
- Информиране на служителите за техните отговорности и задължения по отношение на информационната сигурност;
- Осигуряване на съответствие с нормативни и договорни изисквания.

Ръководството на Кооперацията ще прилага **следните основни принципи** при разработване, внедряване и поддържане на СУИС:

- Спазване изискванията на законите:
- Защита на данни и неприкосновеност на лична информация;
- Опазване на архивите на организацията;
- Защита на авторски права, търговска информация и други права върху интелектуална собственост.

От общоприетите най-добри практики за информационна сигурност:

- Разработване на политика по информационна сигурност;

- Разпределяне на отговорностите по информационна сигурност;
- Обучение по информационна сигурност;
- Докладване на инциденти, свързани със сигурността;
- Управление непрекъснатостта на работа;
- Дисциплинарен процес вследствие от нарушенията на политиката по сигурността.

Усилията на Ръководството са насочени към:

- Критичната (чувствителната) информация и системи да бъдат подлагани на редовен анализ на риска;
- За критичните (чувствителни) информационни ресурси и системи да бъдат определени „собственици" – служители отговорни за конкретните бизнес приложения, компютри и мрежи;
- Информацията да бъде класифицирана по начин, който показва нейната критичност и чувствителност по отношение на организацията;
- Персоналът да осъзнава проблемите на информационната сигурност;
- Организацията да се съобразява с лицензите за софтуер, авторските и други свързани права, както и с други правни, регулаторни и договорни задължения;
- Нарушаването на политиката по сигурността и евентуалните недостатъци в системата за информационна сигурност да бъдат докладвани;
- Информационните ресурси да бъдат защитавани от гледна точка на изискванията за конфиденциалност, цялостност и достъпност.

Въвеждането и спазването на политиката по информационна сигурност цели да се забранят:

- Използването на информацията и системите на организацията без оторизация или за цели, които не са свързани с дейността й;
- Изнасяне на оборудване или информация от офисите и производствените помещения на организацията без оторизация;
- Неоторизирано копиране на информация и софтуер;
- Компрометиране на пароли (например със записване или разпространяване);
- Използване на персонална информация за бизнес цели, освен ако няма изрична оторизация;
- Фалшифициране на доказателства в случай на инцидент.
- Правене на порнографски/неприлични, дискриминационни или нападателни изявления, които могат да бъдат противозаконни (например с използване на електронна поща или интернет);
- Разпространение на незаконни материали (например с неприлично или дискриминационно съдържание).

Отговорности:

За осъществяване на настоящата политика и за осигуряване функционирането на СУИС, Ръководството определя следните отговорности на:

Ръководител на ИТ проекти

Формулира, преглежда и одобрява Политиката по информационна сигурност и контролира ефикасността на нейното изпълнение;

- Планира необходимите ресурси за сигурността на информационната система;
- Определя ролите и отговорностите свързани със сигурността на информацията, изготвя планове за обучение и осъзнаване;
- Координира прилагането на мерки за защита на информационната сигурност.

Системен администратор

- Отговарят за управление и поддържане на интернет, електронна поща, сървъри, локална мрежа, архивиране, техническа защита (софтуер и хардуер) от вреден софтуер;
- Нива на достъп;
- Проследимост на включване и опити за включване;
- Изготвяне и поддръжка на цялостната документация, свързана с администрирането на информационната система и нейните подсистеми.
- Координира дейностите по прилагане на Политиката и мерките по осигуряване на информационна сигурност;
- Отговаря за изготвяне на методика за оценка на риска и за класификация на информацията;
- Извършва оценка на риска и адекватност на мерките при изменения в информационната система;
- Управлява възникнали несъответствия и инциденти;
- Съдейства за осигуряване на обучението и осъзнаването на потребителите на информационната система.

Потребители

- Потребителите на информационната система, се задължават да следват процедурите и инструкциите по информационна сигурност, да докладват за проблеми и инциденти в информационната система.

Оценка на риска:

Оценката на риска се прилага за всеки актив на СиВЗК или извън нея, обхванат от споразумение с трета страна. Оценката на риска се прилага към

цялата информационна система и включва приложения, сървъри, мрежата, и всеки процес или процедура, чрез които системата се администрира и/или поддържа.
Идентифицирането и оценката на риска се извършва на базата на разработената и внедрена от СиВЗК **Методика за оценка на риска.**
Критериите за оценка на риска се базират на вероятността даден източник на заплаха да се възползва от определена потенциална уязвимост и да окаже въздействие върху организацията.
За да се определи вероятността да се случи неблагоприятно събитие се анализират заплахите за Информационната система заедно с потенциалните уязвимости и съществуващи мерки. Въздействието се отнася до степента на вреда, която може да бъде причинена от проявата на уязвимостта.
Резултатите от оценката на риска определят мерките за контрол за намаляване на риска всъответствие с нивата на риска.
Оценката на риска се извършва минимум веднъж годишно, за да бъдат отчетени измененията в изискванията за сигурност, активите, заплахите, уязвимостите, въздействията или други настъпили промени. При необходимост се извършва незабавно.
Изпълнението на политиката по оценка на риска е отговорност на Ръководителя на ИТ проекти.

Вътрешна организация на информационната сигурност:

Ръководството провежда политика за координиране на цялата дейност в организацията по внедряването и поддържането на мерките за защита.
СиВЗК е извършила разпределяне на отговорностите по сигурността на информацията в съответствие с Политиката по сигурност на информацията. Ангажиментите на служителите са дефинирани в длъжностните им характеристики.
Координирането на дейностите по отношение на сигурността на информацията е възложено на Ръководителя на ИТ проекти.
Организацията е определила и документирала отговорностите за изпълнението на следните дейности:
 собственост и защита на активите;
 поддръжка на ключови ресурси на организацията – мрежа, сървъри, клиентски поръчки;
 закупуване, изменения и поддръжка на софтуерните ресурси;
 закупуване, изменения и поддръжка на хардуерни компоненти;
 правилата за поддръжка на инфраструктурата, вътрешния ред и контактите с външни организации;

 управление на инциденти;
 непрекъснатостта на дейността;
 сключване на споразумения за поверителност с трети страни и изисквания за защита на поверителната информация на организацията.

Управление на активите:

Правилата се отнасят до служители, договарящи страни, консултанти, временно работещи за Кооперацията и други, включително и персонал на трети страни. Те се отнасят до цялото информационно оборудване, собственост или използвано от СиВЗК.
Политиката на Кооперацията за използване на активите, цели не да налага ограничения, противоречащи на установената фирмена култура на откритост и доверие, а да защитава служителите на СиВЗК, нейните партньори и самата фирма от незаконни и увреждащи действия, извършени предумишлено или несъзнателно.
Информационният регистър, Счетоводният и друг приложен софтуер и Локалната мрежа, включително сървърите, компютърното оборудване, операционните системи, средствата за съхранение на информация, електронната поща и други са собственост на СиВЗК. Регистърът е предназначен да се използва за целите на бизнеса в интерес на Кооперацията, на нашите клиенти и потребители, което налага въвеждане на правила за употреба.
Данните, които се обработват и съхраняват в Информационния регистър са собственост на Кооперацията. Поради необходимостта от спазване на Закона за защита на личните данни, Информационната система на СиВЗК се изгражда така, че да се гарантира конфиденциалност, цялостност и достъпност на личната информация, съхранявана в Регистъра.
Служителите са задължени да правят добра преценка относно разумността на личната употреба.
За целите на сигурността и поддръжката на мрежата, системните администратори наблюдават оборудването, системите и мрежовия трафик по всяко време.
СиВЗК си запазва правото, чрез Системния администратор да деинсталира всякакъв софтуер или файлове, които не са свързани със служебните задължения на потребителя. Примери за такъв софтуер или файлове включват, но не се ограничават до: игри, музикални файлове, файлове с изображения, споделени и свободни програми, и др.
СиВЗК си запазва правото периодично да одитира мрежите и системите, за да провери спазването на тази политика.

Потребителите, имащи достъп до информацията разположена в системите свързани с Интернет/Локална мрежа, са длъжни да спазват Политиката за чисто бюро, чист екран и защита на не надзиравани устройства.
Служителите трябва да прилагат изключително внимание когато работят с електронната поща, за да се предпазят от вируси, бомби, троянски коне, червеи и друг вреден софтуер.
Изброените по-долу дейности са забранени. Служителите могат да бъдат освободени от тези ограничения само в резултат на техните утвърдени служебни задължения:

- Служителите на СиВЗК нямат право при никакви обстоятелства да участват в каквато и да е дейност, която е незаконна спрямо националното или международното законодателство, когато използват ресурсите на СиВЗК;
- Нарушение на правата на личност или организация, защитени от законите или разпоредбите за авторско право, търговски тайни, патенти или друга интелектуална собственост, включително и инсталирането или разпространението на „пиратски" или друг софтуерен продукт, който не е лицензиран за нуждите на СиВЗК (вж. Лицензионна политика).
- Копиране на материали, защитени с авторско право, в т.ч. дигитализиране и разпространение на фотографии от списания, книги, музика или други защитени източници и инсталиране на софтуер, за който СиВЗК или крайния потребител нямат активен лиценз.
- Въвеждане на вреден софтуер в мрежата или сървъра (напр. вируси, троянски коне, e-mail бомби и др.)
- Разкриване на паролите или допускане на друг човек да използва акаунтите. Това включва членове на семейството или други, живеещи в дома, когато се работи вкъщи.
- Представяне на фалшиви оферти за продукти или услуги на СиВЗК.
- Въвеждане на пробиви и разриви в мрежовите комуникации. Пробивите включват достъп до данни, до акаунт или до сървър, за които служителят не е оторизиран.
- Извършване, на каквато и да е форма на наблюдение на мрежата, която ще прихваща данни, които не са предназначени за работните станции на служителите, с изключение на случаите, когато тази дейност е част от нормалните служебни задължения.
- Проваляне на автентификацията на потребителя или

сигурността, на която и да е станция, мрежа или акаунт.

- Използване на програма/скрипт/акаунт или изпращане на съобщения от всякакъв вид с намерение да се попречи или да се прекъсне сесията на потребителя, чрез всякакви средства локално или чрез Интернет/Локална мрежа.
- Предоставяне на информация за служителите и клиентите на СиВЗК на страни извън организацията.

Политика по сигурност, свързана с човешките ресурси:

Човешките ресурси са основен елемент от СУИС. Политиката по сигурността на човешките ресурси на СиВЗК е насочена основно към осъзнаване на необходимостта от осигуряване на информационната сигурност чрез адекватно дефиниране на отговорности и обучение.
Администрирането на човешките ресурси на Организацията обхваща целия процес – проучване на кандидатите, назначаване, определяне на задълженията, промяна на длъжността и прекратяване на договорите.
Контролът по връщането на активите на организацията се осъществява чрез подписване на декларация за поверителност, протокол за предоставяне на достъп до информационните ресурси на Организацията при постъпване на работа и обходен лист – при напускане на работа.
Правата за достъп се дават от Системния администратор в съответствие функционалните задължения на служителя.
Всички служители на СиВЗК, и където е уместно, доставчиците и потребителите от трета страна, в съответствие с техните функции на работа, преминават подходящо обучение и редовно актуализиране на знанията по политиката и процедурите на организацията.
Всички служители на СиВЗК и други физически лица, които използват ресурсите на Кооперацията, подписват Декларация за поверителност.
В случаи на сериозно нарушение на политиката и правилата за сигурност на човешките ресурси се прилага дисциплинарен процес, който включва отнемане на права за достъп до информационни ресурси, на активи и ако е необходимо, отстраняване от работа.

Политика по физическа сигурност и сигурност на заобикалящата среда:

СиВЗК провежда политика на защита на средствата за обработка и съхранение на информацията чрез определяне на граници на физическа сигурност и организация на зона за сигурност.
Работните помещения и техниката се защитават от физическо влизане чрез

система за Контрол на достъпа с една зона за достъп.
Контролът на физическото влизане в зоната за достъп се допълва от денонощно видеонаблюдение от камери и микрофони в помещенията и коридорите на офиса на Кооперацията.
Определени са местата за достъп на клиенти, доставки и зареждане. За да се избегне неразрешен достъп, не се допуска влизане на външни лица в работните помещения на офиса.
Политиката на СиВЗК по отношение на защита на устройствата цели намаляване на риска от неразрешен достъп до информацията с всички възможни последствия, загуба, повреда, кражба, прекъсване на дейността. Прилагат се технически мерки за защита от пожар, защита на окабеляването и комуникационните връзки. Осигурено е непрекъсваемо електрозахранване за сървърите, системата за физически достъп и ключови работни места.
СиВЗК провежда и политика за осигуряване на условия за безопасна работа в съответствие със Закона за здравословни и безопасни условия на труда.

Политика по контрол на достъпа:

Политиката на СиВЗК за контрол на достъпа е базирана на принципите „необходимост да знае” или „необходимост да се ограничи”, „всеки достъп, който не е изрично разрешен е забранен” и минимизиране на привилегиите.
Ръководството на Кооперацията прилага мерки на контрол на достъпа, които да осигуряват:
 физическа защита на информационните ресурси;
 достъп до съответните информационни ресурси в съответствие с политиката на собственика на ресурса и на ръководството на организацията;
 определяне на нивата на достъп в съответствие с ролята, която трябва да изпълняват служителите на организацията и нивата на класификация на информацията;
 механизми за контрол на физическото влизане;
 определяне на зони за обществен достъп, доставки и зареждане;
 контрол на нивото на достъп за всеки служител от регистрирането до крайната дерегистрация;
 разделяне на ролите за контрол на достъпа;
 минимизиране на необходимостта от специални привилегии;
 спазване на правилата за „чисто бюро и чист екран”;
 защита на не надзиравани устройства;
 ограничаване нивата на достъп на външни потребители на информационната система;
 отнемане на права на достъп при напускане;

 периодичен преглед на достъпа;
 ъпгрейд на контрола на достъп в отговор на нови заплахи, възможности, изисквания на бизнеса или изводи от инциденти.

Политика по Разработване, внедряване и поддържане на информационните системи:

Политиката на СиВЗК по разработване, внедряване, изменение и поддържане на информационните системи е базирана на принципа на превантивната оценка на риска от измененията, включително ъпгрейд на съществуващи и внедряване на нови елементи от системата, разделение на средата за изпитване от действащата информационна система и планирана поддръжка на цялата информационна система.
С цел предотвратяване на грешки, загуба, неразрешено изменение или използване на информация в приложни системи се прилагат механизми за контрол върху входните данни, вътрешната обработка, изходните данни и данните за изпитването на системата, които са дефинирани в Процедура „Правилна обработка на информацията в приложните системи".
Всички изменения в хардуера и в софтуера на системата се извършват само с предварително разрешение и в съответствие с процедура „Управление на сигурността при придобиване, разработване и поддържане на информационни системи".
Приложени са мерки за управление на технически уязвимости, които включват приложенията, операционните системи и оценка на риска, свързан с техническите уязвимости.
Организацията определя изискванията за сигурност, които трябва да се спазват при придобиване, разработване и поддържане.

Политика по Управление на инциденти и подобряване на сигурността на информацията:

С цел намаляване на риска и произтичащите от появата на инциденти разходи, Ръководството на СиВЗК обръща внимание на разработването и внедряването на процедури и средства за ефективно третиране на слабостите и пробивите, свързани със сигурността на информацията. Мерките обхващат непрекъснато наблюдение, реагиране, оценяване, подобряване и цялостно управление на слабостите и инцидентите.
Всички потребители на информационната система на Организацията са задължени да докладват за наблюдавани събития и слабости в информационната сигурност.

Действията свързани с управление на инциденти включват докладване, анализ на причината, планиране на коригиращи и превантивни мерки за предотвратяване от повторна поява, възстановяване на системата и съобщаване за инцидента.
Действията за възстановяване след нарушение на сигурността и за коригиране на грешки на системата се извършват от персонала в ИТ-сектора.
Където се изискват доказателства, те се събират и съхраняват, за да се гарантира съответствие с изискванията на нормативните актове при последващи правни действия срещу лице или организация след инцидент със сигурността на информацията.
В Кооперацията се събират данни и се извършва анализ на вида и броя на инцидентите, и на направените разходи по разрешаване на инцидентите с цел да се идентифицират повтарящите се инциденти или инцидентите с голямо влияние, и да се ограничат честотата, щетите и загубите от появата им в бъдеще. Оценката на инцидентите е част от входните данни при Прегледа от ръководството.

Политика за осигуряване на непрекъснатостта на дейността:

Ръководството на Кооперацията разбира необходимостта от планиране непрекъснатостта на дейността. То осъзнава, че има значителен риск за неговите критични процеси при потенциални и неочаквани разрушителни събития. Увеличаващото се развитие на процеси, базирани на технологии и силната зависимост от информационните технологии е основание за създаване на План за непрекъснатост на работа.
В СиВЗК е осигурена непрекъснатост на работата на критичните ресурси на информационната система при настъпване на сериозни неблагоприятни условия. Осигурено е непрекъсваемо електрозахранване при спиране на тока за 8 часа. Периодично се архивират данните от информационния регистър. Същите се съхраняват на защитени места в офиса и извън него и могат да послужат за възстановяване на дейността след грабеж, изземване, голям пожар или разрушения.
Планът за непрекъснатостта на работа е разработен и приложен във всички отдели на Организацията с цел критичните бизнес задачи да бъдат възстановени в необходимия период от време. Планът представлява интегрална част от всички процеси по управление. Планът по непрекъснатостта е съгласуван и интегриран в Кооперацията по отношение на алтернативни офиси и възстановителни процеси.
Планът по непрекъснатостта е съгласуван с процедурите и мерките по управление на инциденти.

Планът определя специфичните отговорности на определените екипи, които да осигурят възобновяване и възстановяване на критичните информационни функции. Планът осигурява придобиване и поддържане на информационни ресурси, необходими за осъществяването непрекъснатост на работа.
Планът се поддържа и тества, с цел установяване на пропуски и слабости.
Промените в информационната система на Организацията се разглеждат и оценяват по отношение на влиянието и риска, свързани с плана за непрекъснатост.
Политиката и планът за непрекъснатост на работа са координирани с дейностите по информационна сигурност, включително физическа сигурност, човешки ресурси, архивиране.
Непрекъснатостта на поддържането на интернет и на интернет-страниците на организацията е отговорност от доставчиците на услугите и се базира на двустранни договори.

Лицензионна политика:

Политиката на Кооперацията е създадена с цел да се спазват всички авторски права на компютърния софтуер, както и условията по софтуерните лицензи, по които тя е страна. Организацията предприема всички необходими действия за предотвратяване на копирането на лицензиран софтуер от потребителите, както и използването на свързана с него документация в офисите на организацията или на друго място, освен ако не съществува изрично разрешение за това съгласно договора с лицензодателя. Забранява се на служителите да използват софтуера по начин, който не съответства на лицензионния договор, включително предоставяне или получаване на софтуер или шрифтове от клиенти, изпълнители по договори, потребители и други.
Целият софтуер, придобит от организацията, трябва да бъде закупен след съгласуване със системния администратор. Каналите за придобиване на софтуер са ограничени, за да гарантират, че организацията поддържа пълна документация за закупения софтуер и може да регистрира, поддържа и актуализира съответния софтуер. Това включва софтуер, който може да бъде свален и/или закупен от интернет.
Компютрите на СиВЗК са активи, собственост на Кооперацията и трябва да бъдат използвани с лицензиран софтуер и да бъдат защитени от вируси. Забранява се на потребителите да донасят софтуер отвън и да го инсталират на своите компютри в Кооперацията. Притежаваният от Кооперацията софтуер не може да бъде изнасян от потребителите и качван на други компютри.

Всички потребители трябва да използват целия наличен софтуер при спазване на съответните лицензионни договори и да съзнават, че те не притежават този софтуер или свързаната с него документация, и освен ако изрично не са упълномощени от издателя на софтуера, не могат да правят допълнителни копия, освен за нуждите на архива.
СиВЗК няма да толерира използването на никакви неоторизирани копия на софтуер или шрифтове. Всеки, който незаконно копира софтуер, може да бъде обект на граждански или наказателни санкции, включително налагане на глоби и затвор. Никой потребител не трябва да толерира незаконното копиране на софтуер при никакви обстоятелства, а всеки който разработва, използва или придобива нелицензиран софтуер ще бъде наказан дисциплинарно.
Никой потребител не може да дава софтуер или шрифтове на външни лица, включително клиенти и др. При никакви обстоятелства СиВЗК не може да използва софтуер, който е донесен от нелицензирано местонахождение, включително, но не само от интернет, дом, приятели и колеги.

Политика за защита на авторските права:

Политиката на СиВЗК за защита на авторските права е изцяло съобразена със Закона за авторското право и сродните му права.
Клиентът запазва всички авторски права върху информационните ресурси и материали, включително файлове, каталози и други готови изображения, върху техния дизайн, върху запазени знаци и марки, които предоставя на СиВЗК с цел използване на предлаганите му услуги.
СиВЗК съхранява цялата информация, подадена от клиента, при строга конфиденциалност. СиВЗК пази личните данни на застрахованите, като гарантира и поема задължение да не използва нито в интерес на СиВЗК, нито на негови други клиенти, партньори, свързани лица, служители и съдружници, запазени знаци, бази данни, лични данни, образи и друга информация на или за застрахованото лице или неговите наследници и ползващи лица, станала известна при изпълнение на поетите професионални ангажименти.

Политика за защита на личните данни:

Политиката на СиВЗК за защита на личните данни е изцяло съобразена със Закона за защита на личните данни.
СиВЗК събира лични данни единствено за уреждане на трудово-правните взаимоотношения със служителите. Информацията не се използва повторно

за цели, несъвместими с първоначалните.
Информацията, която СиВЗК може да събира, включва данни от лични карти, здравни досиета, телефонни и факс номера, адрес за електронна поща, и др.
Изрично се забранява събирането на информация, която:
 Разкрива расов или етнически произход;
 Разкрива политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели;
 Се отнася до здравето, сексуалния живот или до човешкия геном.
СиВЗК няма да продава, отдава, търгува с всякаква лична информация, получена от застрахованите, служителите си или от застрахователните брокери.
Определените отговорни служители, обработващи лични данни, са задължени да третират информацията като конфиденциална.
Предприети са мерки за физическа и логическа защита на личните данни и са ограничени правата за достъп до тях.
Всеки служител, за когото се отнасят данните („субект на данни“) има право на достъп до своите данни, както и да изиска тяхното коригиране.

Заключение
Политиката по информационна сигурност се преглежда редовно.
Политиката по информационна сигурност се ревизира, за да се вземат под внимание променящите се обстоятелства.
Всеки служител, който прецени, че има злоупотреба с настоящата политика в организацията, трябва да уведоми Отговорника по сигурността.
Всеки служител, за когото е установено, че е нарушил тази политика, подлежи на дисциплинарна отговорност.
Персоналът на СиВЗК се задължава да спазва всички правила, свързани с информационната сигурност, описани в процедури, инструкции и други документи от СУИС.
Разработването и внедряването на Система за управление на информационна сигурност съгласно международния стандарт ISO 27001:2005 е основополагаща цел за реализация на бизнес стратегията на Кооперацията.

ДОКУМЕНТООБОРОТ ИЗВЪН ПЕГЛАМЕНТИРАНОТО СЪС ЗАКОНОВИ И ПОДЗАКОНОВИ АКТОВЕ И ОБИЧАЙНИТЕ ПРАКТИКИ

1. Всяка молба за претенция се завежда с входящ номер и датата на получаване на молбата в деловодството на Кооперацията и се разглежда от

упълномощеното за целта лице.
2. При необходимост от допълнителни доказателства по претенцията ЗАСТРАХОВАТЕЛЯ уведомява писмено ползващото лице. Получените допълнително доказателства се завеждат с входящия номер на молбата, а срокът за отговор започва да тече от датата на получаването им.
3. При постъпване на първа молба за претенция се съставя досие по застрахователния договор. Всяка следваща молба се прилага към досието, както и всички писма изпратени от ЗАСТРАХОВАТЕЛЯ до ЗАСТРАХОВАНИЯ или други компетентни по случая органи, както и техните отговори и становища.
4. Документите касаещи здравословното състояние на ЗАСТРАХОВАНИЯ, като: епикризи, болнични листи, здравни декларации и др., се разглеждат и резюлират от ЗМК на ЗАСТРАХОВАТЕЛЯ.
5. След приключване на преписката по установяване на претенциите се предоставя писмено становище на ЗАСТРАХОВАНИЯ или ползващото лице.
6. Сумите дължими от ЗАСТРАХОВАТЕЛЯ се изплащат в рамките на 15 (петнадесет) дни от събирането на всички документи по съответната претенция.
7. Ако претенцията не е свързана с изплащане на суми от ЗАСТРАХОВАТЕЛЯ, а с промени в параметрите на застрахователните договори се издава нова застрахователна полица или притурка към старата, която носи същия регистрационен номер, като се отбелязва в нея датата на настъпване промените в договора и документите се прилагат към досието, като се извършват и съответни корекции в информационния масив на Кооперацията.
8. Документите издадени във връзка със състоянието и поддържането на застрахователните договори се съхраняват, съгласно съответните давностни срокове предвидени в ОУЖЗ и Закона за счетоводството. Информацията на магнитни носители се съхранява 5 (пет) години след изтичане на съответните давностни срокове.
9. УС периодично проверява документацията по уреждане на претенциите и набелязва мероприятия за усъвършенстване на процеса.
10. Отговорно лице за съставяне и съхранение е административния директор на Кооперацията.
11. За администриране в по-сложни случаи може да се привличат вещи лица и да се прилага индивидуален подход по решение на УС на Кооперацията, като се спазва и регламентираното в ОУ и Устава на Кооперацията.

РАЗГЛЕЖДАНЕ НА ЖАЛБИ

1. Възникналите между страните спорове и разногласия по повод на уреждане на застрахователни претенции се уреждат чрез преговори. Когато не се постигне съгласие между страните, застрахованият или ползващото лице може да обжалва отказа за изплащане на застрахователната сума или обезщетение, или техния размер. Това обжалване може да бъде извършено както пред органите на Застрахователя, така и пред компетентния съд, съгласно действащото българско законодателство. Правото на иск пред съда е независимо и самостоятелно, без да е обвързано с процедурата по обжалване пред Застрахователя.
2. Обжалването на решението на Застрахователя пред неговите вътрешни органи се осъществява от заинтересованото лице с писмена жалба, която се депозира в Централно управление (ЦУ) на Застрахователя, гр. София. Жалбата може да бъде подадена лично или чрез упълномощено лице (напр. член на семейството или адвокат) и за това не се дължат такси.
3. Към жалбата могат да се приложат писмени доказателства, които не са били представени на Застрахователя по преписката и са относими към застрахователното събитие, причините за настъпването му, основанието и размера на застрахователната сума или обезщетение. В жалбата задължително се посочват:
- трите имена, ЕГН и адрес за кореспонденция на жалбоподателя;
- пълномощно, в случаите, когато жалбата се подава чрез пълномощник;
- номер на завеждане на претенцията съгласно заявлението за нея;
- първоначалното решение на Застрахователя относно претенцията;
- възраженията и тяхното основание;
- искането;
- дата и подпис на подателя.
4. Деловодството на ЦУ на Застрахователя:
- оформя преписка и води досие на всяка жалба и ги съхранява в каса за срок от 5 години;
- поддържа електронен регистър на жалбите, който, освен задължителната за всяка жалба информация, съдържа следната допълнителна информация:
- пореден номер;
- предмет на жалбата;
- вид, тарифа и номер на застрахователната полица/договор;
- входящ номер;
- дата на завеждане;
- резолюция на председателя, отговорни лица и срокове за изпълнение;
- резултат от действията по жалбата;

- други бележки и коментари при необходимост.
4.Жалби, подадени повторно по въпрос, по който има решение, не се разглеждат, освен ако са във връзка с изпълнение на решението или се основават на нови факти и обстоятелства.
5. Оценката на поставените в жалбата въпроси и вземането на решение по нея се извършва от определените длъжностни лица безпристрастно, с оглед на действащото българско законодателство и настоящата политика за уреждане на претенции и в срок до 30 (тридесет) дни от нейното получаване. При констатиране на конфликт на интереси от страна на определено длъжностно лице по дадена жалба, същото незабавно информира Председателя на кооперацията, който възлага дейността по жалбата на друг специалист.
6. Определените за работа по жалбата длъжностни лица:
а) се стремят да съберат и проучат всички относими доказателства и информация по отношение на жалбата;
б) общуват на ясен език, който е лесноразбираем;
в) използват посочените от жалбоподателя лични данни в съответствие със закона за защита на личните данни и само за целите на решаване на проблема, посочен в жалбата.
7. На всеки етап от разглеждането на жалбата, както и при запитване, Застрахователят предоставя на жалбоподателя информация за хода на разглеждането на жалбата.
8. Решението на застрахователя и мотивите към него се съобщават на жалбоподателя с писмо на посочения в неговата жалба адрес без излишно забавяне или поне в рамките на срока, посочен в т. 4. Когато в рамките на очаквания срок не може да бъде предоставен отговор, Застрахователят уведомява жалбоподателя за причините за забавянето и посочва кога се очаква да приключи проверката по жалбата.
9. Когато се предоставя окончателно решение, което не удовлетворява напълно искането на жалбоподателя, последният има право на иск по съдебен ред по седалището на Застрахователя, съгласно разпоредбите на Гражданския процесуален кодекс. В такива случаи Застрахователят включва пълно обяснение на позицията на застрахователното предприятие по отношение на жалбата и посочва на жалбоподателя възможността да продължи защитата на интересите си, предмет на жалбата. Това решение се представя в писмена форма.
10. В длъжностните характеристики на служебните лица, определени за работа по жалби се отразява изискването за детайлно познаване на настоящата политика за уреждане на претенции и в частност реда за разглеждане на жалби. Същите се допускат до изпълнение на служебните задължения след проведено обучение и изпит.

11. За всяка жалба отговорникът за цялостния процес по разглеждане на жалбите изготвя докладна записка до Председателя на кооперацията, която съдържа анализ на причините за отделните жалби с цел установяване на първопричините, общи за различните видове жалби, преценка дали тези първопричини могат да засегнат и други процеси или продукти, включително тези, във връзка с които не са постъпили преки жалби и предложение за коригиране на тези първопричини, когато това се налага. На годишното Общо събрание същият докладва обобщен анализ на постъпилите жалби.