



**ПОЛИТИКА ЗА ИЗВЪНРЕДНИ СИТУАЦИИ И ИНФОРМАЦИОННА
СИГУРНОСТ**

ПОЛИТИКА ЗА ИЗВЪНРЕДНИ СИТУАЦИИ И ИНФОРМАЦИОННА СИГУРНОСТ

ОБЩИ ПОЛОЖЕНИЯ И ОСНОВНИ ПОНЯТИЯ

Какво е извънредно положение?

Кои са основните компоненти на извънредното положение?

Защо този проблем е важен?

Кои основни управленски принципи трябва да се съблюдават при обявено извънредно положение?

Кои човешки права не могат да се ограничават при извънредно положение?

Какви специални пълномощия могат да бъдат обявени при извънредно положение?

Какви механизми и подходи помагат да се избегне злоупотребата със специални пълномощия при извънредно положение?

Кой може да обяви извънредно положение?

Свързани теми

Какво е извънредно положение?

Извънредното положение се обявява с правителствена декларация в отговор на извънредна ситуация, представляваща изключителна заплаха за страната. Декларацията може да отмени някои обичайни функции на правителството, да предупреди гражданите за възникнала необходимост от промяна на тяхното нормално състояние или да оторизира правителствените органи да прилагат на практика планове за готовност в условия на извънредно положение, както и да ограничат или отменят временно някои граждански свободи и човешки права.

Необходимостта от обявяване на извънредно положение може да възникне вследствие на разнообразни причини като например въоръжено нападение срещу страната от вътрешно-държавен или външен характер, природно бедствие, пожари, наводнения, тероризъм, граждански вълнения, епидемия, финансова или икономическа криза или всеобща стачка. Обявяването на извънредно положение не е нещо необичайно, най-вече в държави, управлявани от диктаторски режими, където то може да продължи през цялото управление на режима. В някои случаи се обявява и военно положение, което дава на военните по-голяма свобода на действие.

Други термини, с които се обозначава извънредното положение, са „тревога” и „блокада”.

Кои са основните компоненти на извънредното положение?

Извънредното положение има два компонента:

- правна рамка, представляваща конституционната и законодателната база на извънредното положение;
- оперативна рамка, включваща организационната структура и стратегическото планиране на извънредното положение.

Въпреки, че са два отделни компонента, те трябва да са съвместими. С други думи правната рамка трябва да взема под внимание оперативните изисквания, а оперативните изисквания трябва да са съобразени с правната рамка, включително и с международното право. Акцентирайки върху правната рамка, настоящата разглежда въпросите за подотчетността, човешките права и върховенството на закона в условия на извънредно положение.

Защо този проблем е важен?

Прилагането на закона при извънредно положение неизбежно води до ограничаване на нормалната икономическа, гражданска и политическа активност и на правата на гражданите с цел справяне с извънредните обстоятелства, станали причина за обявяване на извънредно положение. Някои от ограниченията могат да бъдат напълно оправдани. Същевременно съществува опасност правителството да се възползва от извънредното положение за налагане на неоправдани ограничения на човешките права и граждански свободи, за неутрализиране на политически опоненти, за отлагане на избори или за други собствени цели. В някои държави съществува тенденция за запазване на извънредното положение в продължение на десетилетия, дълго след изчезването на причината за неговото обявяване. Опасността от появата на “конституционна диктатура” вследствие на обявено извънредно положение не трябва да бъде подценявана.

Кои основни управленски принципи трябва да се съблюдават при обявено извънредно положение?

Конституцията и законите на държавата описват обстоятелствата, при които може да бъде обявено извънредно положение, установяват процедурите, които трябва да се следват при тези обстоятелства и определят ограничения за упражняване на извънредни пълномощия или изброяват правата, които могат да бъдат временно отменени. Съществуващите международноправни норми могат да послужат като полезна насока за всяка отделна държава, която би желала да установи своя собствена практика. Важни международни договори като например Европейската конвенция за правата на човека и основните свободи (ЕКПЧОС) и Международната конвенция за гражданските и политическите права (МКГПП) постановяват, че държавите трябва да се придържат към следните принципи:

- временен характер: има се предвид изключителния характер на обявеното извънредно положение;
- изключително голяма заплаха: кризата трябва да представлява реална, непосредствена и най-малкото неизбежна заплаха;
- обявяване: извънредното положение трябва да бъде обявено публично – така се информират гражданите за правния характер на обстоятелствата и се намалява опасността от възникването на ситуация, в която държавата ограничава човешките права, без официално да е обявено извънредно положение
- информиране: уведомяване на международната общност и релевантните международни органи за предприетите мерки; например ако държавата възнамерява да ограничи някои от човешките права според ЕКПЧОС или МКГПП, тя трябва да съобщи това на Генералния секретар на Съвета на Европа или Генералния секретар на ООН, както и да ги уведоми за мерките, които е предприела, за основанията за тези мерки и за продължителността на периода, в който ще действат тези ограничения;
- пропорционалност: предприетите мерки за справяне с кризата трябва да бъдат пропорционални на заплахата от извънредната ситуация; това се отнася за сферата на тяхното приложение, техния характер и продължителност на действия;
- законност: човешките права и свободи в условията на извънредно положение трябва да бъдат съобразени с ограниченията, наложени от съответните инструменти на международното и националното право; освен това извънредното положение не предполага временна отмяна на действащото законодателство, нито оторизира упражняващите държавна власт да предприемат действия, незачитащи принципите на законност, от които са винаги обвързани;
- неприкосновеност: имат се предвид онези основни права, които са неотменими дори и в условия на извънредно положение.

Кои човешки права не могат да се ограничават при извънредно положение?

Определени човешки права са неотменими, при каквито и да било обстоятелства. Според ЕКПЧОС и МКГПП такива права са:

- правото на живот;
- забраната за изтезания;
- забраната на робството;
- забраната на закони с обратно действие;
- правото на справедлив съдебен процес;
- свободата на мисълта, съвестта и религията.

Комисията за човешки права на ООН, наред с изброените неотменими права, е постановила и следните ненарушими положения:

- хуманно отношение към лишените от свобода;
- забрана за взимане на заложници и неправомерно задържане;
- защита правата на малцинствата;
- забрана на пропагандата на война, национална, расова или религиозна омраза;
- процедурни гаранции за запазване интегритета на съдебната система.

Какви специални пълномощия могат да бъдат обявени при извънредно положение?

Специалните пълномощия в условия на извънредно положение се дават на правителството от конституцията или законите. Пример за извънредни мерки или пълномощия са:

- ограничаване на свободата на медиите и забрана на обществените събрания;
- разполагане на въоръжени сили на територията на страната;
- евакуация на населението от домове и работни места;
- обискиране на домове и друга частна собственост без заповед и арести без повдигане на обвинения;
- конфискация на частна собственост (*с или без компенсация*) и/или нейното унищожаване;
- регулиране на дейността на частните предприятия; намеса във финансовите операции и регулация на експорта;
- приемане на специално законодателство, наказващо неподчинението на извънредните мерки. При извънредно положение управлението на страната трябва да се осъществява от гражданските власти на национално и местно ниво. Силите за сигурност трябва да имат помощна функция, подпомагайки гражданските власти.

Какви механизми и подходи помагат да се избегне злоупотребата със специални пълномощия при извънредно положение?

Ролята на парламента

Повечето правни системи ограничават правото на изпълнителната власт да обявява извънредно положение и изискват парламентарно одобрение на едно такова решение на правителството, често пъти с квалифицирано мнозинство. Като общо правило правителствата под контрола на парламента трябва добре да мотивират, както решението си за обявяване на извънредно положение, така и специалните мерки, които възнамеряват да предприемат за справяне с извънредната ситуация. Повечето парламенти се упълномощени също да преразглеждат регулярно извънредното положение и да го отменят, ако

сметнат за необходимо. Тази роля на парламента е изключително важна при продължително действие на извънредното положение, когато принципът на върховенство на гражданските власти над сектора за сигурност може да бъде изложен на риск. Каквото и да е естеството на извънредната ситуация, правомощията на парламента, т.е. правото му да отправя запитвания и да провежда разследвания относно начина на прилагане на извънредните правомощия, трябва да бъдат уредени със закон. Това е от съществено значение, както за правилната оценка на действията на правителството, така и за извличане на опит, който да бъде използван при бъдещи извънредни ситуации.

Ролята на съдебната власт

Съдебната система трябва да продължи да гарантира правото на справедлив съдебен процес и в условията на извънредно положение. Тя също трябва да предостави на гражданите ефикасни средства за защита срещу нарушения на техните човешки права от правителствени служители.

За да бъде защитена неприкосновеността на основните и неотменими човешки права, правото на съдебен процес във връзка със законността на прилаганите извънредни мерки трябва да бъде гарантирано чрез независимостта на съдебната власт. Съдът може да играе ключова роля при вземането на решения по отношение, както на законността на обявеното извънредно положение, така и относно законността на специфичните извънредни мерки.

Ролята на гражданското общество

Извънредното положение поставя под огромен натиск държавата и обществото. За да се справи ефективно с нея, правителството трябва да си сътрудничи с гражданите. Нарушаването или неоправданото ограничаване на човешките права в условия на извънредно положение подкопават това сътрудничество и поставят пречки пред преодоляването на извънредната ситуация. В изключителен интерес на държавата е да се справи с извънредното положение по един прозрачен и отговорен начин.

Ролята на съседни страни и международната общност

Извънредното положение може да се отрази и на отношенията на страната със съседни държави и да има последствия за международната общност. От интерес за всяка държава е да гарантира, че обявяването на извънредно положение и прилагането на съпътстващите го мерки съблюдават международните норми. Международната общност трябва да бъде активно ангажирана да гарантира за спазването на тези норми от правителствата. По-

специално трябва да сътрудничи със заинтересованите правителства за премахване на извънредното положение и възстановяване на конституционния ред, който напълно гарантира спазването на човешките права.

Кой може да обяви извънредно положение?

В повечето държави съществуват законови механизми, уреждащи обявяването на извънредно положение и прилагането на съпътстващите го ограничения на гражданските права. Що се отнася до правото на обявяване на извънредно положение, най-често срещаните случаи са три:

- изпълнителната власт обявява извънредно положение, като е длъжна да информира за това парламента в рамките на установен срок (*например в САЩ*);
- изпълнителната власт обявява извънредно положение, но парламентът трябва да утвърди това решение преди предприемането, на каквито и да било извънредни мерки (*например в Германия*);
- парламентът обявява извънредно положение (*например в Унгария*);

Най-често извънредното положение дава право на изпълнителната власт да определи съответните служители, които да се справят с извънредната ситуация, както и да пренебрегне нормалната административна процедура относно създаването на административни правила.

След като сме наясно с какви извънредни ситуации може да се наложи да се справяме, подобно на много други неща, подготовката за спешни случаи започва в дома. Много световни организации за готовност при бедствия са съгласни, че подготовката за извънредни ситуации основно се свежда до три неща:

- създаване или спазване на изготвен за целта план;
- създайте комплект/и за оцеляване;
- бъдете информирани – следете официалните новини.

Повечето организации напомнят на хората, че след каквото и да е голямо бедствие, е малко вероятно услугите за спешна помощ да бъдат в състояние да реагират веднага на нуждите на всички. Така, че е важно да бъдем подготвени да се грижим за себе си и семейството си. Трябва да планираме да се справим сами най-малко през първите 3 дни (72 часа).

Следните стъпки ще помогнат за съставяне на план, за да бъдем по-добре подготвени за всякакви спешни случаи, като формата на изразяване има за цел да се възприеме като заповедна, като се има пред вид, че до 85% от

извънредните ситуации са възникнали в извънработно време:

- Определете лице за контакт извън района, в който се намирате. Изберете някой, който е достатъчно далеч за да не бъде засегнат от същата ситуация. Осигурете на този човек имената и информация за контакт с хората, които искате да бъдат информирани за ситуацията. Инструктирайте членовете на семейството да се обаждат на тези хора и да им кажат къде са. В много спешни случаи, междуградските телефонни връзки всъщност се възстановяват по-бързо от местните.
- Копирайте важните си документи и съхранявайте копията на защитено място, извън дома ви, например в банков сейф, при доверен човек и др. Такива документи могат да бъдат: паспорт, шофьорска книжка, здравна карта, завещания, нотариални актове, финансови отчети, осигурителна информация, брачно свидетелство, актове за раждане и др.
- Направете опис на ценностите, които имате, в писмена форма и със снимки или видео. Пазете копия от тази информация извън дома си, заедно с другите важни документи.
- Направете план. Ангажирайте всички ключови хора в планирането.
- Направете дома и офиса си безопасен.
- Направете комплект с провизии. Планирайте провизиите за себе си и семейството си за най-малко 3 дни след бедствието.
- При планирането, помислете за специалните нужди и медикаменти на децата, възрастните и хората с увреждания, или членове на семейството, които не говорят местния език, както и за вашите домашни любимци.

Стъпка 1: Семейен план

- Говорете със семейството си за потенциалните бедствия и защо е необходимо да се подготвят за тях. Ангажирайте всеки член на семейството в процеса на планиране. Показвайки им прости стъпки, които могат да увеличат тяхната безопасност, така ще им помогнете да намалят тревогата при извънредни ситуации.
- Уверете се, че всеки знае къде да намери комплекта с провизии при бедствие, както и собствените им сървайвър-раници.
- Планирайте къде да се срещнете след бедствие, ако вашия дом стане опасен. Изберете две места, едно извън дома ви и едно извън квартала в случай, че трябва да се евакуирате. Уверете се, че резервоарът на автомобила ви е винаги поне наполовина пълен.
- Определете най-добрите начини за евакуация. Опитайте се да определите поне два пътя за бягство.
- Уверете се, че всеки член на семейството знае кой е човека, извън района ви

и ги инструктирайте да се обаждат на този човек при първа възможност и да му кажат къде могат да бъдат намерени.

- Намерете газопроводите и други комунални услуги в дома си и се уверете, че членовете на семейството знаят кога и как да ги изключат.
- Практикувайте маршрутите за евакуация, а също и тренирайте практики като „Залегни – Скрий се – Изчакай – Спри – Бягай”.
- Научете всеки член на семейството и офиса как да използва пожарогасител.

Направете дома и офиса си безопасни!

По време на бедствие обикновените предмети могат да ви наранят. Съществуват прости стъпки, които можете да предприемете за да направите дома и офиса си по-безопасни. Започнете като обходите всяка стая и определите потенциалните опасности – библиотечки или шкафове, които могат да се преобърнат при земетресение или друго бедствие и да блокират изхода, или тежки предмети, които биха могли да паднат и да причинят наранявания.

- Ако можете инсталирайте детектори за дим на всяко ниво и сменяйте батериите на всеки 6 месеца;
- Преместете леглата и столовете по-далеч от прозорците;
- В земетръсна зона сме, преместете огледалата и тежките снимки и картини далеч от дивани и от местата, където стоят хора;
- Разчистете коридорите и изходите за лесна евакуация;
- Съхранявайте тежките предмети върху най-ниските рафтове;
- Имайте поне един или два пожарогасителя в къщата и офиса си и се уверете, че всички членове на семейството знаят как и кога да ги използват;
- Тъй-като сме в земетръсна зона, подсигурете картините и украшенията на стената и използвайте ограничения за подсигуряване на тежки предмети, като библиотеки и шкафове;
- Съхранявайте запалимите или силно реактивни химикали (като белина, амоняк и разреждатели за бои) на сигурно място и отделени един от друг. Смесването на тази вещества при бедствие може да ви коства живота;
- Знайте как и кога да изключите комуналните услуги (газ, електричество, вода и др.);
- Ако домът или офисът Ви е оборудван с решетки за прозорци или други такива защитни елементи, уверете се, че всички те имат функционални спешни изходи;
- Уверете се, че номерът на дома или офиса Ви се вижда от улицата, така че спешните превозни средства да могат да ви намерят.

Допълнителни съображения за Вашия план.

Ако имате деца в дома си:

- Не забравяйте да включите децата си в семейните дискусии и планиране за аварийна безопасност;
- Научете децата си на основна информация, така че да могат да се идентифицират и да получат помощ, ако бъдат отделени от родителя или настойника;
- Направете им карти с информация за всяко дете, включително неговото/нейното пълно име, адрес, телефонен номер, телефонен номер на работното място на родителите и номера е лицето, което сте определили за контакт извън района, в който живееете;
- Знайте политиките на училището или детската градина, които децата Ви посещават. Направете планове да има някой да ги вземе в случай, че не можете да стигнете до тях;
- Редовно давайте актуална информация на училището или детската градина как да се свържат с вас при спешни случаи, а също и с хората, упълномощени да вземат детето;
- Уверете се, че всяко дете знае местата за алтернативна среща ако се разделите при бедствие и не можете да се върнете в дома си;
- Уверете се, че всяко дете знае как да стигне до човека, определен като семеен контакт, извън района ви;
- Научете децата как да набират вашия номер или спешните номера;
- Научете децата как мирише газта и ги посъветвайте да кажат на възрастен ако подушат миризмата на газ в извънредни ситуации;
- Предупредете децата никога да не докосват проводници и кабели върху стълбове или лежащи на земята;
- Проиграйте с децата как да запазват спокойствие в критични ситуации и практикувайте основни реакции в извънредни ситуации, като например маршрутите за евакуация или практиките Залегни – Скрий се – Изчакай – Спри – Бягай;
- Играйте с децата на игра какво да правят ако единият родител внезапно се разболее или е ранен;
- Проиграйте с децата какво да кажат, когато се обаждат на спешните номера.

Ако сте възрастен човек или човек с увреждания:

- Определете някой, който да Ви провери в извънредна ситуация и да Ви

помогне с евакуация или подслон.

- Подгответе и носете със себе си спешна карта със здравна информация. Това ще Ви помогне да комуникирате, дори ако сте в безсъзнание или амнезия. Включете информация за Вашите лекарства, адаптивно оборудване, кръвна група, алергии, застрахователни полици, дати на имунизация, трудности в общуването и предпочитано лечение, както и информация за връзка с Вашите здравните служби, мрежа от лични асистенти и спешни контакти.

- Ако получавате помощ от агенция за помощ по домовете или от местна компания, разберете как ще реагират те в случай на бедствие. Определете резервни или алтернативни доставчици, с които можете да се свържете.

- Ако имате нужда от инвалидна количка: планирайте как ще се евакуирате в спешни случаи и го обсъдете с хората, които полагат грижи за вас. Ако използвате моторизирана инвалидна количка, пригответе си и ръчна количка като резерва.

- Ако сте слепи или с увредено зрение: пригответе допълнителен бастун до леглото си. Прикрепете и свирка към него в случай, че се наложи да привлечете вниманието. Бъдете внимателни, когато се движите, пътищата могат да бъдат възпрепятствани и непознати.

- Ако сте с увреден слух: имайте допълнителни батерии за вашия слухов апарат. Помислете за съхраняване на слухов апарат в контейнер, прикрепен към нощното Ви шкафче или рамката на леглото, така че да можете да го намерите бързо при бедствие.

- Ако не можете да говорите или имате комуникационни увреждания: пригответе си хартия, пособия за писане и копия с думи или предварително отпечатани ключови фрази във вашия спешен комплект, портфейл, чанта и т.н.

Стъпка 2: Създаване на комплект за оцеляване

Втората важна стъпка в спешната подготовка е да създадете комплект за оцеляване в дома. Комплекта за оцеляване не означава само "раница за оцеляване", която можете да вземете със себе си ако трябва да се евакуирате, въпреки че тя пък е част от общия Ви комплект за готовност при бедствия. "Комплекта за оцеляване в дома" трябва да съдържа всичко, което ще Ви трябва за да оцелеете най-малко три дни в случай на авария или природно бедствие, ако услугите, на които обикновено разчитате като течаща вода, електричество и телефони, вече не са на разположение.

Какво трябва да знаете за изграждане на комплекти за оцеляване за дома.

Вашият домашен комплект за оцеляване не трябва да е на тавана, в мазето, в гаража или на някакво друго недостъпно място. Няма да Ви помогне ако не можете да стигнете до него! Трябва да го сложите на леснодостъпно място. Сложете цялото съдържание в голяма непромокаема торба или раница, които могат да се движат лесно.

Комплекта за оцеляване да включва:

- Вода – три литра на човек на ден.
- Храна – готови за консумация или изискващи минимално количество вода храни (също и дехидратирани храни).
- Отварачка за консерви и други продукти за готвене.
- Чинии, прибори за хранене и други консумативи.
- Аптечка и инструкции.
- Копия на важни документи и телефонни номера.
- Топли дрехи и дрехи за дъжд за всеки член от семейството.
- Работни ръкавици.
- Фотоапарат за еднократна употреба.
- Таблетки или филтри за водно пречистване.
- Лични вещи за хигиена за всеки член на семейството, включително тоалетна хартия, дамски принадлежности, дезинфектант за ръце, сапун, шампоан и др.
- Пластмасови плоскости, тиксо и многофункционален нож за покриване на разбити прозорци.
- Инструменти като лост, чук, пирони, щапелен пистолет, регулируем гаечен ключ и бърнджи въжета.
- Одежда или спални чували.
- Големи найлонови торби и пластмасова кофа за отпадъци и хигиенизиране.
- Всички специални неща за деца, възрастни и хора с увреждания. Не забравяйте вода и провизии за вашите домашни любимци.

Критичен компонент на комплекта ви за бедствие е вашата "Раница за Оцеляване". Сложете следните неща в раница или друг лесно преносим контейнер в случай, че трябва да се евакуирате бързо. Трябва да подготвите раница за всеки член от семейството и се уверете, че всяка има табелка с името. Може да не сте у дома, когато настъпи извънредна ситуация, така че може също да си пригответе раница в колата и на работното място, като сложите това, което ви трябва за вашата безопасност в случай на авария или бедствие.

Основната сървайвъл раница трябва да включва:

- Вода – три литра на човек на ден (резерв за три дни);
- Храна - трайни, лесни за приготвяне храни (резерв за три дни);
- Фенерче;
- Радио на батерии или с динамо (също метеорологична станция ако е възможно);
- Допълнителни батерии и зарядно;
- Джобно ножче;
- Комплект за първа помощ;
- Лекарства (резерв за 7 дни) и медицински инструменти;
- Многофункционален инструмент;
- Комплект тоалетни принадлежности и вещи за лична хигиена;
- Копия от лични документи (списък с лекарства и уместна медицинска информация, доказателство за адрес, нотариален акт/договор за наем, паспорти, свидетелства за раждане, застрахователни полици);
- Мобилен телефон със зарядни устройства;
- Спешна информация за контакт със семейството;
- Допълнителни пари;
- Термо одеяло;
- Карта/карти на областта;

Но когато става въпрос за пълна подготовка, никога не е добра идея да спрете само до основното.

Ето и някои други неща, които можете да включите:

- Свирка;
- Дихателна маска (противогазова маски ако е възможно);
- Здрави обувки, резервни дрехи, топла шапка и ръкавици;
- Перманентен маркер, хартия и тиксо;
- Снимки на членове на семейството и домашните любимци за повторна идентификация;
- Списък на спешни телефонни номера за контакт;
- Списък на алергии към всяко лекарство (особено антибиотици) или храна;
- Копие от здравния картон и други идентификационни карти;
- Допълнителни очила с диоптър, слухови апарати или други жизнено важни лични вещи (ако използвате такива);
- Копие от ключовете за дома и автомобила;
- Всички специални неща за деца, възрастни и хора с увреждания.

Ако имате деца, трябва да подготвите специална сървайвъл раница за тях, която да включва:

- Семейна снимка и любима играчка, игра или книга.
- Карта за бедствия на Вашето дете, която да включва информация за алтернативни места за среща и контакт с човека, извън района, в който живеете.
- Комфортни хранителни продукти и любимите им лакомства.

Точно толкова важно, колкото и съхраняването на Вашия комплект за оцеляване на леснодостъпно място в случай на авария, също е толкова важно да е добре поддържан. Ето няколко съвета за запазване на провизиите Ви готови и в добро състояние:

- Пазете консервираните храни на хладно и сухо място;
- Съхранявайте опакованата храна в плътно затворени пластмасови или метални контейнери за защита от вредители и удължаване срока за годност;
- Изхвърлете всички консерви, които са се подули или ръждясали;
- Периодично изяждайте храните, преди да се развалят и ги заменете с пресни такива;
- Поставайте новите продукти в задната част на помещението за съхранение, а по-старите такива отпред;
- Подменяйте съхранената храна и вода на всеки шест месеца. Не забравяйте да напишете датата на поставяне на всички контейнери;
- Преосмисляйте вашите нужди всяка година и актуализирайте комплекта си, тъй като нуждите на семейството Ви се променят;
- Пазете продуктите в херметически затворени найлонови торби, а целия си комплект за бедствие в един или два лесни за носене контейнери, като например непромокаеми найлонови чували или сакове.

Още за храната и водата

ВОДА

Като част от вашия сървайвъл комплект трябва да съхранявате най-малко три литра вода на човек на ден. За да определите водните си нужди, вземете под внимание следното:

- Три литра вода на човек на ден, за пиене и хигиенизиране.
- Децата, кърмачките и болните хора могат да се нуждаят от повече вода.
- Спешни медицински случаи могат да изискват допълнително количество

вода.

- Ако живеете на място с топъл климат, може да имате нужда от повече вода. При прекалено високи температури, нуждите от вода могат да се удвоят.
- Подсигурете вода поне за три дни на човек.

Препоръчително е да закупите търговска минерална вода, за да подготвите най-надеждния воден резерв за извънредна ситуация (макар че бутилираната минерална вода не е най-добрия избор откъм вода). Дръжте водата в оригиналната ѝ бутилка и не я отваряйте, докато не се наложи да я използвате. Наблюдавайте срока на годност. Съхранявайте я на тъмно и хладно място.

ХРАНА

Имайте предвид следните предложения при подбора на храна за извънредни ситуации:

Готови за консумация месни консерви, плодове, зеленчуци и отварачка за консерви; протеинови или плодови пакетирани храни; сухи зърнени култури или мюсли; фъстъчено масло; сушени плодове; ядки; бисквити; консервирани сокове; трайно пастьоризирано мляко; храни с високо съдържание на енергия; витамини; храна за кърмачета; комфорт - стрес храни.

Стъпка 3: Включете се / Бъдете информирани

Отново и отново виждаме как изправени пред бедствие, хората застават заедно със смелост, състрадание и единство и питат: *"Какво мога да направя, за да помогна?"* Тази трета стъпка ще Ви отговори на този въпрос.

Това започва с важното разбиране, че шансовете за Вас, Вашия дом и Вашето семейство се увеличават значително, ако Вашата общност като цяло е по-добре подготвена да се справи с бедствие. И това започва с участие.

Повечето организации за гражданска защита насърчават цели общности да участват в програми и дейности, които могат да направят техните семейства, домове и региони по-безопасни от рискове и заплахи.

Лидерите на общностите са съгласни, че формулата за осигуряване на по-безопасна среда се състои от доброволци, обучено и информирано общество и засилена подкрепа на агенциите за спешно реагиране по време на бедствия. Големи бедствия могат да разрушат организацията на агенциите за спешно

реагиране, давайки сила на индивидуалните хора да оказват помощ.

Включете се преди да е настъпило бедствие! Ето няколко начина да помогнете:

*Станете доброволци в подкрепа на усилията срещу бедствия във Вашата общност;

*Станете обучени доброволци в аварийните екипи в общността, медицински екипи и/или други граждански програми или организации;

*Много от местните обществени организации имат програми за активна подкрепа във времена на бедствия;

*Бъдете част от процеса на планиране в общността. Свържете се и помагайте на местни групи за аварийно планиране, граждански съвети или местни агенции за управление на извънредни ситуации;

*Присъединете се към или започнете проект за готовност;

*Помогнете в големи бедствия като дарите пари или стоки, които могат да помогнат на нуждите на общността по време на бедствие.

Бъдете информирани

Да бъдете информирани не означава само да знаете какви бедствия или извънредни ситуации могат да се появят във Вашата област, но също така и да се уверите, че знаете как ще бъдете предупредени и как ще бъдете информирани, ако те настъпят. Трябва:

- Да определите как местните власти ще Ви уведомят по време на бедствие и как ще получите информация, независимо дали, чрез местното радио, телевизия или метеорологични радио станции или канали.

- Да знаете разликата между различните сигнали и предупреждения и какви действия да предприемете при всяко едно от тях.

- Да знаете какви действия да предприемете за да се предпазите при бедствия, които могат да възникнат в районите, където пътувате или сте се преместили наскоро. Например, ако пътувате до място, където земетресенията са често срещани и не сте запознати с тях, уверете се, че знаете какво да направите за да се предпазите ако се случи такова.

При воденето на дискусии за готовност, комплекти за оцеляване, раници за оцеляване и други подобни, обсъждане на застраховките може да изглежда малко не на място. Част от това да бъдете напълно подготвени да оцелеете от сериозно природно бедствие е да можете да се възстановите и да продължите

напред, а това може да бъде невъзможно без адекватна застраховка. Като защита срещу финансови загуби, за жилището и офиса трябва да се закупят застраховки за дома и офиса и да се запознаете с тяхното съдържание. Най-малкото, покритието трябва да предоставя пълна замяна или покриване разходите за подмяна. Също така застрахователната полица трябва да покрива и природни бедствия.

Заклучение

Изглежда ли Ви от последните няколко страници, че има твърде много за правене? Както и във всичко друго – всичко, което трябва да направите е да се ангажирате и да започнете сега –днес, не утре.

Ако отидете и вземете голям непромокаем чувал за боклук, който да използвате за домашен комплект за готовност и отделяте по няколко минути всеки ден за да слагате едно или две от препоръчаните неща в него, през следващите десет до двадесет дни вече ще имате основен комплект. Семейството Ви не заслужава ли тези усилия? И вероятно е много по-лесно, отколкото си мислите.

Разгледайте из къщата и офиса си, вероятно вече имате много от нещата, които Ви трябва. Тези, които нямате – всяка седмица, когато правите списъка си с покупки, сложете няколко допълнителни неща за оцеляване в него, като консерви, батерии и т.н.

Изборът е ваш, можете да живеете, както досега или можете да започнете да правите някои прости промени за да бъдете по-добре подготвени следващия път, когато спре тока.

ПОЛИТИКА ПО ИНФОРМАЦИОННА СИГУРНОСТ

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;
- ☐ Базы 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 ѝ;
- ☐ 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 документирила 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 въкъщи.
- 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.
- Проваление 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 с 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 deregистрация;
- ☐ разделяне на ролята 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 третираат 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.