ПОЛИТИКА ЗА ИНФОРМАЦИОННА СИГУРНОСТ

НА

КОРНЕР ООД

ИСТОРИЯ НА ДОКУМЕНТА

Текуща версия	Описание на промените	Направил промените	Дата
1.0	Създадена е първа версия на политиката за информационна сигурност.		10.07.2018

СЪДЪРЖАНИЕ

1. ВЪВЕДЕНИЕ

1.1. Настоящият документ представя политиката за сигурност на информацията на КОРНЕР ООД по отношение на всички данни, съхранявани и обработвани от информационните системи, мрежите и приложенията (ИТ активите) на компанията.

1.2. Собственик на данните, които се съхраняват и обработват от ИТ активите, както и на работните процеси по тяхното управление е КОРНЕР ООД.

1.3. Отговорностите на КОРНЕР ООД по отношение на информационната сигурност обхващат цялостната организация и ръководство на информационната сигурност в Компанията, поддържането на сигурността на ИТ активите, както и контрол върху действията на служебните потребители, които използват ИТ активите на Компанията.

1.4. Основните аспекти на сигурността на информацията се управляват във всички фази на нейния жизнен цикъл — създаване, обработка, съхранение, пренасяне, унищожаване.

1.5. Политиката е разработена в съответствие с признати и общоприети международни стандарти в областта на информационната сигурност, както и спрямо изискванията въведени от Общия регламент за защита на личните данни (Регламент (ЕС) 2016/679). Списъкът на всички използвани стандарти и нормативни документи е предоставен в Приложение 2 към настоящата политика.

2. ХАРАКТЕРИСТИКИ НА ПОЛИТИКАТА

1.1. Основните цели, поставени от настоящата политика са:

1) гарантиране на конфиденциалност на информацията чрез изграждане на система от мерки за ефективната й защита от неправомерно придобиване, неправомерно модифициране, унищожаване или загуба;
2) развитие и поддържане на сигурна и надеждна ИТ инфраструктура за осигуряване на интегритет и достъпност на информацията;
3) установяване на правила и процедури за оперативно използване на ИТ активите на КОРНЕР ООД, осигуряващи достоверност, актуалност и пълнота на информацията в системата;
4) своевременна и адекватна управленска реакция в случай на злоупотреба, загуба или неупълномощено придобиване на информация, както и при бедствия, и аварии;
5) опазване репутацията и имиджа на КОРНЕР ООД, ангажирана с обработването и съхранението на лични данни.

1.2. Обхват на политиката

1) настоящата политика се прилага върху информационните активи на КОРНЕР ООД, включващи неговата ИТ инфраструктура (собствена и наета от други организации) и данните, съдържащи се в системите;
2) политиката се отнася до всички потребители, които използват системите на КОРНЕР ООД;
3) документът е в съответствие с всички национални закони и приложими наредби, както и с изискванията поставени от Общия регламент за защита на личните данни (Регламент (ЕС) 2016/679);

4) КОРНЕР ООД не използва механизми за сигурност, които са в противоречие с тези документи.

1.3. Роля на ръководството на КОРНЕР ООД

2.3.1. Ръководството носи цялостна отговорност за ИТ инфраструктурата на системите, обработващи и съхраняващи лични данни, и като такъв упражнява всички права и задължения по гарантиране на сигурността на данните, чрез:

1) гарантиране на нормалното функциониране на системите на приложно и на системно ниво;
2) предоставяне и оторизиране на необходимите човешки и материални ресурси по управление и контрол на сигурността на системите;
3) създаване, актуализиране и прилагане на Политиката за информационна сигурност;
4) предприемане на необходимите действия за създаване и поддържане на необходимите споразумения, нормативни и поднормативни актове с които изискванията на настоящата политика да станат задължителни за изпълнение от служителите на всички звена и организации (външни и вътрешни), които имат достъп до системите, обработващи и съхраняващи лични данни;
5) поемане на отговорността за разпространението и запознаването на всички заинтересовани страни с тази политика и свързаните с нея документи.

2.4. Възприетият подход цели:

1) възможност за поддържане на сигурността на системите, обработващи и съхраняващи лични данни по съответните правила наложени в организацията;
2) прилагане на единен подход съобразно утвърдени стандарти за информационна сигурност и гарантиране съответното ниво на предоставяните услуги.

2.5. Инструменти за постигане на целите

2.5.1. Настоящата политика използва следните стратегически инструменти за постигане на по-горе поставените цели:

1) осигуряване на пълна поддръжка на мерките по сигурността на информацията в системите, обработващи и съхраняващи лични данни от страна на Ръководството на КОРНЕР ООД;
2) гарантира запознаване, разбиране и сътрудничество на всички лица и организации, влизащи в обхвата на политиката;
3) дефиниране на подходяща организационна структура за управление на сигурността на информацията;
4) разпределяне на отговорностите за защита на информационните активи на КОРНЕР ООД между отделните лица и организации, свързани с използването и поддържането на ИТ активите;
5) дефиниране на мрежа от контроли (регулации). Контролите са подбрани в съответствие с изискванията на международните стандарти в областта на информационната сигурност;
6) дефиниране на средства за контрол на изпълнението на изискванията на политиката и при необходимост извършване на корективни действия върху тях.

3. УПРАВЛЕНИЕ НА ПОЛИТИКАТА

3.1. Собственик на настоящата политика и всички свързани с нея документи е ръководството на КОРНЕР ООД.

3.2. Контролът върху рисковите фактори по сигурността и съответните мерки по ограничаването на тяхното въздействие е непрекъснат процес. В политиката са осигурени механизми за проверки, отчитащи промените в средата и технологиите.

3.3. В тази връзка, на политиката се извършва преглед на годишна база, с цел осигуряване на съответствието ѝ с непрестанно променящите се бизнес изисквания.

3.4. Ръководството на КОРНЕР ООД е отговорно за събирането и обобщаването на постъпили предложения за промени, извършването на необходимите корекции в документите и тяхното съгласуване и утвърждаване.

3.5. Източници на информация за промени в сигурността на информацията са:

1) обратна връзка от заинтересованите страни;
2) резултати от наблюдения;
3) анализ на предприети проактивни или коригиращи действия;
4) промени в системите, обработващи лични данни, които биха имали ефект върху информационната сигурност, като: структура, ресурси, техническа инфраструктура, договорни отношения;
5) промени в регулаторни и законови рамки;
6) одитни доклади и други препоръки, дадени от експерти.

4. ОРГАНИЗАЦИЯ НА УПРАВЛЕНИЕТО И КОНТРОЛА НА ИНФОРМАЦИОННАТА СИГУРНОСТ

4.1. Ръководството на КОРНЕР ООД поддържа адекватни административни и функционални отговорности по отношение изпълнението на изискванията по сигурността на ИТ активите. Посоченото по-долу представлява кратко описание на организационните единици, ангажирани с управлението и контрола на настоящата политика:

4.1.1. **Ръководство на КОРНЕР ООД**. Отговорностите по отношение на ИТ активите и тяхната сигурност обхващат:

1) цялостната организация и ръководство на сигурността;
2) ръководство и контрол върху стопанисването и поддържането на ИТ активите на Компанията;
3) издава заповеди по разпределянето на различните роли и отговорности при поддържането на ИТ активите и потребителите на системите, обработващи лични данни и сигурността на информацията в тях;
4) осигурява управленска подкрепа в рамките на инициативи, свързани със сигурността на ИТ активите;
5) съобразно своята компетентност подписва документи (заповеди, договори) за осигуряване поддръжката на ИТ активите.

4.1.2. При изпълнението на посочените дейности ръководството на КОРНЕР ООД се подпомага от юрисконсулта на Компанията и отговорното за сигурността техническо лице.

4.1.3. **Специалист техническа поддръжка и отговорник по информационна сигурност.** Задълженията му включват:

1) управление и поддържане на необходимото техническо ниво на сигурност на ИТ активите на Компанията спрямо идентифицираните рискове;

2) съгласуване на документите по информационна сигурност и промените в тях с ръководството на Компанията;
3) контролиране на изпълнението на политиката, както и организиране на прегледи на информационната сигурност;
4) разследване на предполагаеми нарушения на сигурността и съгласуване на докладите за проверките и съответствието;
5) представляване на ръководството на КОРНЕР ООД по всички въпроси на информационната сигурност.

4.1.4. Потребители/Служители

1) Задължават се да следват политиката за информационна сигурност и да докладват за инциденти и проблеми, свързани с ИТ активите на Компанията.

5. СЪОТВЕТСТВИЕ, НАРУШЕНИЯ, РЕАКЦИЯ

5.1. Съответствието с тази политика е задължително за всички действия, извършвани от потребителите на ИТ активите на КОРНЕР ООД във връзка с изпълнението на служебните им задължения.

5.2. Всяко действие, несъобразено с тази политика, което води до разкриване на конфиденциална информация или нарушаване на други нейни параметри по сигурността (цялост, достоверност и др.), може да завърши с предприемане на адекватни мерки от страна на ръководството на КОРНЕР ООД, включително прекратяване на трудовите или договорни взаимоотношения и възможност за съдебно преследване съгласно действащото законодателство.

5.3. В зависимост от степента на нарушението, от страна на ръководството или от контролиращите органи може да бъде изготвен „Доклад за инцидент по сигурността" с описание на нарушението и ангажираните лица. В допълнение, правата на достъп на потребителя или организацията, които са нарушили правилата, могат да бъдат отнети за времето на разследването на нарушението.

6. СИГУРНОСТ НА ЧОВЕШКИТЕ РЕСУРСИ

6.1. Всички служители се запознават с тези части от настоящата политика и свързаните с нея документи, които отговарят на техните роли и отговорности. Служителите потвърждават чрез подписването на декларация, че са запознати и че разбират задълженията си по тези документи.

6.2. Всички служители са наясно какво представлява инцидент или нарушение на сигурността и какви действия трябва да предприемат при възникване на такъв случай.

6.3. Служителите са запознати и с мерките, които техните ръководители могат да предприемат по отношение на тях при нарушаване на поетите ангажименти по отношение на информационната сигурност.

6.4. Ръководителите на звената, чиито служители имат достъп до ИТ активите на КОРНЕР ООД, имат задължението при оформянето на документите за прекратяване на трудово-правни или други отношения с наети лица да гарантират, че всички отговорности и средства за достъп до активите на Компанията са прекратени или прехвърлени.

6.5. Ръководителите имат задължението в определен от свързаните документи срок след подписването на заповед за напускане или промяна на служебното положение на служител, да изпратят уведомление за тази промяна до съответните технически лица, които да отразят своевременно промяната в достъпите на съответното лице.

6.6. Когато е уместно, отговорностите по отношение на информационната сигурност се продължават и за определен период след края на службата, чрез въвеждане на съответни клаузи в договора на лицето или подписване на специална декларация.

7. УПРАВЛЕНИЕ НА ИНФОРМАЦИОННИТЕ АКТИВИ

7.1. Отговорността по сигурността на информационните активи на КОРНЕР ООД носи ръководството на Компанията.

7.2. Отговорността за сигурността на информация, която е изтеглена от оторизиран потребител върху устройство за обработка и/или съхранение, е само и единствено негова, както и на неговия пряк ръководител.

7.3. Информационните активи на КОРНЕР ООД се използват само по тяхното предназначение. Потребителите са наясно, че използването подлежи на непрекъснато наблюдение.

7.4. Използването на индивидуални идентификатори за достъп до ИТ активите не означава, че потребителите трябва да очакват секретност за данните, които създават или получават или за дейностите, които извършват в съответните системи.

7.5. Ръководството на КОРНЕР ООД приема, че потребителите на ИТ активите на Компанията имат подобаващо поведение и действат по

правилния начин до появата на подозрение или доказателство за обратното. Ръководството си запазва правото да извършва случайни наблюдения и инспекции за потвърждаване сигурността на информационните активи.

7.6. Ръководството на КОРНЕР ООД зачита следните принципи за защита на интелектуалната собственост:

1) при доставката на готови продукти, които ще бъдат използвани от КОРНЕР ООД, се включват ясни договорни клаузи относно правата за интелектуалната им собственост;
2) при разработката на нови или усъвършенстването на текущи функционалности на ИТ активи, собственост на КОРНЕР ООД, в договорите на съответния доставчик, се включват ясни клаузи относно правата за интелектуалната собственост;
3) осъществяват се проверки относно инсталирането и използването само на лицензирани продукти, както и на условията на лицензa — срок, максимален брой потребители и др.

8. ФИЗИЧЕСКА СИГУРНОСТ И СИГУРНОСТ НА ОКОЛНАТА СРЕДА

8.1. Принципите за прилагане на физически мерки за сигурност на ИТ активите на КОРНЕР ООД, които да са в състояние ефективно да ограничат рисковете, са свързани с противодействието на следните групи заплахи:

1) злоумишлени или непредпазливи действия на хора — кражба, вандализъм, злонамерени действия;
2) аварийни събития — повишаване на температурата, огън, дим, вода, прекъсвания на електрозахранването и други вредни влияния;

3) природни заплахи.

8.2. За гарантиране на физическата сигурност на ИТ активите на КОРНЕР ООД се осигурява подходяща защитена зона за ИТ инфраструктурата, с определени параметри - контролиран достъп, видео-наблюдение, параметри на околната среда и защита срещу аварийни ситуации и природни бедствия.

8.3. Допълнителните механизми за сигурност, които защитават физически помещенията и устройствата със специални изисквания за безопасност, включват:

1) 24 часово наблюдение на устройствата;
2) системи за откриване на проникване;
3) телевизионна система за наблюдение (ССПУ);
4) контрол на служителите;
5) наблюдение на мрежата;
6) незабавни действия при нарушения.

8.4. При експлоатация на защитените зони, се гарантира, че всички окабелявания на ИТ инфраструктурата са защитени от прихващане или повреда, както и от взаимно влияние между тях.

8.5. Електрозахранването в защитените физически зони е автономно, чрез използване на външни и вътрешни възможности за захранване, като по този начин се осигурява защита на оборудването от прекъсване или повреди в електрозахранването.

8.6. Разрешение за изнасяне на оборудване от инфраструктура на КОРНЕР ООД се предоставя от ръководството на Компанията

8.7. На всяко изнесено ИТ оборудване се изисква лицето осъществило изнасянето да осигури условия за неговото опазване, както и опазването на съдържащата се в него информация.

8.8. Цялата отговорност за сигурността на изнесеното ИТ оборудване, както и на информацията, която се съдържа в него се носи от лицата, разрешили и изнесли оборудването.

8.9. Ръководството на Компанията поема отговорността за получаване на съответните гаранции при изваждане от употреба и при повторно използване на оборудване.

8.10. За изтриване на конфиденциални данни от физически носители, ръководството назначава специална комисия, която да следи процесът по заличаване на данните. Отговорните лица, осигуряват проверка на всички ИТ активи, които подлежат на бракуване или смяна на собствеността, с оглед гарантиране, че всякакви чувствителни данни и лицензиран софтуер са премахнати и при необходимост предварително презаписани на друго устройство.

8.11. Физическата сигурност на работните станции на служебните потребители следват всички дефинирани мерки за физическа сигурност на ИТ активите на Компанията.

9. КОНТРОЛ НА ДОСТЪПА ДО ИНФОРМАЦИОИНИТЕ АКТИВИ

9.1. Политиката на КОРНЕР ООД за контрол на достъпа до информационните активи на Компанията е базирана на принципите *„ необходимост от познаване или ползване ".* Това означава, че по подразбиране се приема *„без право на достъп"* до установяване на необходимостта от познаване или ползване на информацията, а също така означава и периодично потвърждаване, че тази необходимост все още съществува.

9.2. При определяне на кръга от потребители за достъп до определена категория ИТ активи на КОРНЕРООД, отговорните за това служители отчитат:

9.3. изискванията на работните процеси за извършване на определени действия върху информацията или ИТ системите;

9.4. изискванията относно сигурността на съответните активи.

9.5. Всеки отделен потребител отговаря за своите действия при използване на информационните активи на КОРНЕР ООД. Достъпът до тях е само индивидуален и се осъществява на база персонален потребителски профил.

9.6. Основните данни, които се съдържат в един профил включват лични данни, индивидуален идентификатор (потребителско име и парола) и права за достъп на съответния потребител до различните ИТ активи на Компанията.

9.7. Всички потребителските профили се управляват съобразно „жизнения цикъл" на един потребител в системата — създаване на нов потребителски профил, внасяне на промени в него и закриване на профила.

9.8. Дефинират се и се спазват основните параметри на потребителските пароли, като: минимален брой и тип на символите, период на смяна, ограничения по отношение на използване на едни и същи пароли в последователни периоди, брой неуспешни опити и др.

9.9. Не се допуска използването на групови идентификатори, освен ако възможностите на съответния ИТ актив не го изискват.

9.10. Осигурява се периодичен преглед на потребителските права на достъп, като срокът се указва в съответния специализиран документ. Прегледът включва като минимум:

1) спазването на процедурата по управление на потребителските профили;

2) проверка за евентуални промени в служебния статус на потребители, водещи до промени в правата им за достъп;
3) проверка дали предоставеното ниво на достъп отговаря за служебните задължения;
4) наличие на излишни потребителски имена и профили.

9.11. Потребители със специални права се считат тези, имащи права за администриране на ИТ активите на КОРНЕР ООД, както и на потребителските профили по различните приложения.

9.12. Политика на КОРНЕР ООД е разпределението и употребата на специални права да бъде ограничено и контролирано.

9.13. Изискванията към идентификаторите на потребители със специални права надхвърлят изискванията към нормалните потребители и са защитени чрез възможност за резервен достъп за случаите на авария.

9.14. Всички действия на потребителите със специални права се записват в регистрационни файлове (log-files) за последващ контрол.

9.15. Отдаленият достъп до ИТ активите на КОРНЕР ООД се осъществява само чрез криптиран канал — Virtual Private Network (VPN) или друго техническо средство, което осигурява необходимото ниво на сигурност на комуникацията.

10. ОСИГУРЯВАНЕ НА ДОСТОВЕРНОСТ И АКТУАЛНОСТ НА ИНФОРМАЦИЯТА

10.1. Основна отговорност по достоверността и актуалността на информацията, съдържаща се в ИТ активите на КОРНЕР ООД носят собствениците на отделните ИТ масиви или, в случай че такива не са

назначени, ръководството на Компанията. Ръководството определя специалисти, които единствено имат права за промени (въвеждане, редактиране, изтриване) на съответния информационен масив.

11. ОСИГУРЯВАНЕ НА ИНТЕГРИТЕТ И ДОСТЪПНОСТ НА ИНФОРМАЦИЯТА

11.1. Политиката на КОРНЕР ООД включва съхраняването на информацията в ИТ инфраструктурата на Компанията, по начин, осигуряващ нейните интегритет и достъпност.

11.2. Ръководството на КОРНЕР ООД е отговорно за въвеждането на подходящи технически и организационни мерки, осигуряващи надеждно и своевременно възстановяване на важната за КОРНЕР ООД информация, независимо дали тази информация е повредена, унищожена или не е на разположение за продължителен период от време (виж също и т. 17 „Управление на непрекъсваемостта на работните процеси").

12. ОСИГУРЯВАНЕ НА КОНФИДЕНЦИАЛНОСТ НА ИНФОРМАЦИЯТА

12.1. КОРНЕР ООД осъществява политика по защита на личната и фирмената информация, както собствена, така и на външни организации, предоставена по силата на договорни задължения.

12.2. Посочената защита се осъществява в съответствие с действащите законови разпоредби.

12.3. Осигуряването на конфиденциалност на информацията е лична отговорност на всеки, чийто профил осигурява достъп до нея. Отговорността се ограничава до нивото на предоставените му права.

12.4. В случаите, когато определена информация е определена като чувствителна, то КОРНЕР ООД може да поиска от съответните потребители подписването на споразумения за конфиденциалност (неразпространение).

12.5. Защитата на личните данни се осъществява в съответствие Регламент (ЕС) 679/2016 (Общ регламент за защита на личните данни, GDPR), както и съобразно Закона за защита на личните данни на Република България.

13. РЕГИСТРАЦИЯ НА ДЕЙСТВИЯ И СЪБИТИЯ, СВЪРЗАНИ С ИНФОРМАЦИОННАТА СИГУРНОСТ

13.1. Записите се осъществяват във файлове за регистрация *(log-files)* на системно и приложно ниво на ИТ активите на Компанията. Файловете са защитени от манипулации на потребители и са достъпни само за упълномощени технически лица и се съхраняват за определен период от време.

13.2. Действията на персонала със специални (административни) права също се записват. Системните администратори нямат възможност да изтриват или деактивират записи на свои собствени действия.

13.3. Политиката на КОРНЕР ООД включва периодични и внезапни проверки на регистрационните файлове. Случаите, които могат да представляват заплаха за сигурността на информацията, се докладват на ръководството и се третират като инциденти по информационна сигурност.

14. ТЕХНИЧЕСКИ СРЕДСТВА ЗА ЗАЩИТА ОТ ЗЛОНАМЕРЕНО ПРОНИКВАНЕ

14.1. Настоящата точка се отнася до осигуряване на надеждна защита от проникване на злонамерен код (напр. вируси), хакерски атаки и др. Проникването може да се осъществи както през Интернет, така и от неправилно използване на информационните системи или чрез преносими информационни носители със системен достъп до ИТ активите на Компанията.

14.2. Отговорността по поддържане на системите за защита от злонамерен код е на екипа за техническата поддръжка.

14.3. За целта се използват системи за защита *(Firewalls),* чиято основна функция е филтрирането на неправомерен трафик.

14.4. Задължително е използването на софтуер за откриване на вируси, както за сканиране на входящия трафик към ИТ системите, така и на потребителските персонални компютри използвани за работа. Софтуерът трябва да бъде инсталиран, периодично актуализиран и използван за сканиране на компютрите и носителите на информация.

14.5. Задължителни допълнителни контроли за сигурността включват: сигурна мрежова архитектура, криптиране на твърдите дискове на

информационните системи обработващи и съхраняващи чувствителни данни, контрол на достъпа, заключване на компютрите на определени интервали на неактивност, сложност на паролите, редовна актуализация на операционните системи и инсталираните приложения и всички други технически и организационни контроли, служещи за третиране на риска от инциденти, свързани със сигурността.

14.6. Екипът за техническата поддръжка следва да осигури:

1) инсталиране и непрекъснат контрол и актуализация на системите за сигурност;
2) извършване на необходимите настройки на защитните системи за осигуряване на постоянно обновяване на защитата;
3) анализ на инциденти, свързани със злоумишлени проникванията и предприемане на мерки по тях.

15. ПОЛИТИКА ЗА ЧИСТО БЮРО

15.1. Всички служители на КОРНЕР ООД се задължават да спазват следните правила при работата си с ИТ активите на Компанията:

1) Да съхраняват познатите им пароли според нужното ниво на конфиденциалност. Паролите не трябва да се записват на хартия или в програмни файлове, освен ако методът на съхранение не отговаря на дефинираните от Компанията добри практики;
2) Да закриват активните сесии на системите, с които работят след приключване на работата с тях;

3) При напускане на работното място, документите и носителите на чувствителна информация, трябва да бъдат прибрани на сигурно място (заключващи се шкафове, сейфове и др.);
4) Входът на потребителите към системите не трябва да се извършва автоматично. При напускане на работното място, потребителите трябва да блокират компютъра (използвайки комбинацията Win + "L" или Ctrl + Alt + Delete → "Заключване на компютъра");
5) Документите, съдържащи чувствителна информация, трябва незабавно да се събират от принтерите;
6) В края на работния ден всеки служител трябва да почисти бюрото си и да прибере всички офис документи в заключващ се шкаф или сейф;
7) За унищожаване на чувствителни документи трябва да се използват определените за целта устройства – шредери;
8) В края на работния ден и в случай на продължително отсъствие всички шкафове и сейфове трябва да бъдат заключени на работното място.

16. УПРАВЛЕНИЕ НА ПРОМЕНИТЕ В ИТ ИНФРАСТРУКТУРАТА

16.1. Всички промени, които имат пряко отношение върху обработването и съхраняването на лични данни, се регистрират в специален регистър. Осигурен е процес на регулярното му преглеждане с оглед контрол на ефикасността на действията на поддържащите екипи.

16.2. За конкретните дейности по въвеждане на промени се предвижда точна оценка, категоризация и приоритизация на постъпили заявки за промени.

16.3. Следене на статуса на всички промени — заявени, в процес на реализация, приключени, отхвърлени и др., както и контрол върху

изпълнението на самата промяна, е отговорност на съответните технически лица, отговарящи за поддръжката на системите.

16.4. Всички тестове на промени се извършват в тестова среда.

16.5. При необходимост се осигурява обучение на персонала.

17. УПРАВЛЕНИЕ НА НЕПРЕКЪСВАЕМОСТТА НА РАБОТНИТЕ ПРОЦЕСИ

17.1. РОЯЛ КОУВ ЕООД осигурява адекватни процедури и системи за резервно копиране с цел да се гарантира, че всяка важна информация може да бъде възстановена след случай на бедствие или повреда.

17.2. С оглед максимална степен на сигурност на информацията и функционирането на ИТ активите на КОРНЕР ООД, създадените резервни копия на информацията и софтуера се проверяват редовно за достоверност и съответствие на нивото на защита.

17.3. Процедурите за възстановяване се проверяват редовно, за да се гарантира тяхната ефективност.

17.4. Архивиране се прилага и към информация, до която няма необходимост от редовен достъп, но която следва да бъде съхранявана за определен период от време, съгласно изисквания на работните процеси и/или на законови разпоредби.

17.5. Всички резервни и архивни копия се съхраняват извън основното работно помещение на Компанията.

18. УПРАВЛЕНИЕ НА ИНЦИДЕНТИ ПО ИНФОРМАЦИОННА СИГУРНОСТ

18.1. Всички потребители, вкл. външни за Компанията, с достъп до ИТ активите на КОРНЕР ООД, са инструктирани относно задължението им да докладват всички събития отнасящи се до информационната сигурност по най-бързия възможен начин. Те също така са запознати с контактната точка за докладване на подобни събития – (email за докладване на инциденти).

18.2. Потребителите са информирани, че всяка неизправност или друго анормално поведение на ИТ активите може да е индикатор на атака или пробив в сигурността и затова винаги следва да се докладва като събитие отнасящо се до информационната сигурност.

18.3. Управлението на инциденти по сигурността включва и събиране на данни с оглед:

1) анализ на инцидента;
2) наблюдение на сходни инциденти с оглед идентифициране и устойчиво решаване на проблеми — свързани инциденти, дължащи се на общи причини;
3) събиране на данни с оглед нотифицирането на надзорния орган – Комисия за защита на личните данни (КЗЛД), в случай че се касае за инцидент, свързан с лични данни;
4) събиране на данни с оглед предявяване претенции по количество, качество и срокове на изпълнение на договорни задължения с външни доставчици;
5) бъдещи одитни проверки.

18.4. Всички инциденти се регистрират в специален регистър. Осигурен е процес на регулярното му преглеждане, с оглед идентифициране на повтарящи се събития.

18.5. В случай на инцидент, свързан с лични данни се прави допълнителна оценка на риска спрямо правата и свободите на засегнатите индивиди. При идентифициране на висок риск се предприемат мерки за предупреждаване на пострадалите лица и на надзорния орган –КЗЛД в рамките на 72 ч. от потвърждаването на инцидента.

19. ВЗАИМООТНОШЕНИЯ С ВЪНШНИ СТРАНИ

19.1. Ръководството на КОРНЕР ООД предприема всички договорни и други мерки (заповеди, споразумения, инициране на нормативни документи) по отношение на сигурността на информационните активи на Компанията, така че информацията, която е предадена или до която е осигурен достъп на външни организации по електронен път, да бъде опазвана от тези организации, докато е на тяхно разположение, до същата степен, до която тя е защитена съгласно настоящата политика.

19.2. За целта КОРНЕР ООД осигурява необходимото за всеки конкретен случай запознаване с необходимите елементи на Политиката и свързаните документи на всички външни организации, които имат достъп до ИТ активите на Компанията.

19.3. КОРНЕР ООД следи в договорите и другите обвързващи документи с външни страни ясно да бъдат указани:

1) видът и обемът на предоставяните услуги и тяхната стойност;
2) сроковете за предоставяне;

3) правата и задълженията на двете страни;
4) органите и процедурите за управление;
5) качествените показатели на услугите (вкл. споразумения по качеството-SLAs);
6) задължения по сигурността на информацията, които двете страни поемат;
7) контролът, който ще се осъществява от КОРНЕР ООД;
8) неустойките при неизпълнение, вкл. на споразуменията по качеството (ако е приложимо).

19.4. В случаите, когато външната организация, притежава знание, собственост на КОРНЕР ООД или придобито в изпълнение на задълженията по договор към нея, което е от значение за съществуващите процеси, ръководството на КОРНЕР ООД изисква това знание да бъде документирано и да и бъде прехвърлено преди приключване на договорните отношения.

ПРИЛОЖЕНИЕ 1: Термини и дефиниции

Специфичните за настоящата политика термини и дефиниции са дадени в долната таблица.

ТЕРМИН		ДЕФИНИЦИЯ
Достоверност	*Reliability*	Параметър на информацията, отразяваща нейната вярност спрямо обектите, която тя отразява. Обикновено към този параметър се присъединяват и актуалността и пълнотата на информацията.

Достъпност	*Availability*	Параметър на сигурността на информацията, осигуряващ, че всички оторизирани потребители при необходимост имат достъп до нея.
Собственик на информация	*Owner*	Служител или звено, което отговаря за достоверността и актуалността на определена част (масив) от информацията и в чийто състав има потребители с права за извършване на промени.
Интегритет	*Integrity*	Параметър на сигурността на информацията, осигуряващ нейната цялост във вида, в който тя е въведена в системите.
Информационни активи ИТ активи	*Information Assets*	Информация и средствата за нейната обработка и съхранение. В политиката по информационна сигурност двата термина — „информационни активи" и "ИТ активи" са използвани като синоними, като се отнасят до ИТ инфраструктурата и информацията, която се съхранява и обработва от съответната КОРНЕР ООД.
Инцидент, засягащ информационната сигурност	*Information Security Incident*	Неочаквано и нежелано събитие, засягащо информация или инфраструктурата на системата, което води или би могло да доведе до нарушаване на сигурността ѝ.
ИТ	*IT (ICT)*	Информационни (и комуникационни) технологии.

ИТ инфраструктура	*IT (ICT) Infrastructure*	Всички средства за обработване и съхранение на информация в електронна форма. Включва хардуера, софтуера — системен и приложен, телекомуникационните мрежи, спомагателни системи и т.н., които се изискват за предоставяне на ИТ услугите. ИТ инфраструктурата е технологичният компонент на ИТ услугите. В нея не се включват поддържащия персонал, работните процеси и информацията.
ИТ услуга	*IT Service*	Услуга, базирана на използването на информационни технологии и предназначена за поддържане на един или повече бизнес-процеси на потребителите. ИТ услугата представлява комбинация от ИТ инфраструктура, процеси и. изпълнителски екипи. Самата информация е обект и може да не е част от ИТ услугата, т.е. доставчикът на услуга не е непременно доставчик и на информация (съдържание).
Контрола (регулация)	*Control*	Система от мерки за управление на риска от нарушаване на информационната сигурност, включващ правила, процедури и организационни структури.

Конфиденциалност	*Confidentiality*	Параметър на сигурността на информацията, осигуряващ достъп само на оторизирани лица до нея.
КОРНЕР ООД	*Company*	КОРНЕР ООД или друга структура, притежаваща служители и други ресурси.
Политика по информационна сигурност	*Information Security Policy*	Политика, която определя целите и начините на управление на информационната сигурност в една организация.
Потребител	*User*	Всички служители на Компанията и на външни организации, които по силата на своите трудови или договорни задължения имат достъп до ИТ активите на Компанията.
Управление на информационната сигурност	*Information Security Management*	Процесът, осигуряващ конфиденциалността, интегритета и достъпността на информацията и системите за нейната обработка.

ПРИЛОЖЕНИЕ 2: Използвани стандарти и нормативни документи

(1) ISO/IEC 27001:2013, Information security management systems — Requirements.

(2) ISO/IEC 27002:2013, Code of practice for information security management.

(3) Control Objectives for Information and Related Technology (COBIT 4.1, 2007).

(4) Information Technology Infrastructure Library - ITIL v3 — 2007.

(5) General Data Protection Regulation (GDPR) – 679/2016