

# ПОЛИТИКА

По качество  
и информационна сигурност

## Раздел А. Политика по качеството

Ръководството, в лицето на Управителя, официално декларира своята политика по качеството, която е огласена, разбрана и поддържана на всички равнища в Организацията.

**Ротопринт ООД работи за утвърждаване на България, като високоразвита индустриална държава**

- ▶ **Подпомага конкурентоспособността на българските си клиенти, като:**
  - ▶ **Им доставя етикети в срок и с необходимото качество;**
  - ▶ **Своевременно изпраща полезна информация на клиентите си за нови материали, тенденции в етикирането и др.**
  - ▶ **Инвестира в материали, оборудване и технологии даващи възможност за печат на етикети с по-добри характеристики.**
- ▶ **Създава условия за развитието на пазара на самозалепващи етикети като поддържа близки връзки с колегите от бранша**
- ▶ **Стреми се да работи за външни пазари, като с качеството и експедитивността на доставките спомага за утвърждаване на мнението, че България е високоразвита индустриална страна.**

Гаранция за качеството на продуктите е осъществяваният контрол върху целия производствен цикъл, обхващащ: подбор на доставчици, проверка на използваните ресурси и материали, текущ контрол на производствените процеси и краен контрол на готовия продукт, потвърждаващ окончателно качеството му.

За пълното удовлетворяване на потребителските очаквания ръководството на фирма **Ротопринт ООД** провежда активна и целенасочена дейност в следните направления:

- Оптимизиране на процесите в организацията – за адекватност, целесъобразност и съответствие с регламентираните изисквания, на базата на непрекъснато усъвършенстване и устойчиво развитие;
- Наблюдение и оценка на глобалните климатични промени и въздействието им върху дейността.
- Разнообразни форми на обучения на служителите:
  - задължително обучение на всички новопостъпили кадри;
  - повишаване квалификацията на служителите при всяко нововъведение в производството;
  - мотивацията на персонала чрез традиционни ежегодни семинари, на които се разглежда състоянието на фирмата и насоките на развитие;
- Създаване и поддържане на добри партньорски отношения с клиенти и партньорски организации;

- Развиване и поддържане на конкурентни предимства на база цена, качество и удовлетвореност на всички клиенти и партньори на фирма "Ротопринт"ООД ;
- Периодичен анализ и оценка на постигнатите резултати от повишаване на качеството на извършваните дейности и системен контрол за изпълнението на поставените задачи.

За ефективно провеждане на Политиката по качеството, ръководството определя основните цели по качеството в документ „ЦЕЛИ ПО КАЧЕСТВОТО”. Ръководството е създадо условия за стриктно спазване изискванията на Системата за управление на качеството в Организацията и за активното съдействие на ръководния и изпълнителски персонал в нейното развитие. Като Управител на РОТОПРИНТ ООД, ДЕКЛАРИРАМ ЛИЧНОТО СИ УЧАСТИЕ И ОТГОВОРНОСТ ЗА ИЗПЪЛНЕНИЕ НА ОБЯВЕНАТА ПОЛИТИКА ПО КАЧЕСТВОТО, ОСИГУРЯВАЩА РАЗВИТИЕТО И ПРОСПЕРИТЕТА НА ОРГАНИЗАЦИЯТА.

## **Раздел Б. Политика по информационна сигурност**

Ръководството на Ротопринт ООД, в лицето на Управителите, официално декларира Политиката по ИНФОРМАЦИОННА СИГУРНОСТ на информационните ресурси на Ротопринт ООД в обхвата на дейността на дружеството: „Печат на етикети и опаковки върху самозалепващи и други материали”. Политиката е документирана, огласена и разбрана от всички служители, които имат достъп до информацията и информационните системи на Ротопринт ООД. Политиката е одобрена от Управителите и се прилага в рамките на цялата организация. Политиката по информационната сигурност се поддържа от Съвета по информационна сигурност.

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 офис и печатна база на Ротопринт ООД в община Елин Пелин, село Равно поле, Индустриална зона.

#### **Обхват на процесите:**

Системата за управление на информационната сигурност обхваща следните процеси:

- Офериране;
- Приемане на заявка;
- Предпечатна подготовка, включително одобрения от клиента;
- Изработка на цветни дигитални проби ;

- Печат;
- Предаване на готовата продукция.

### **Обхват на информационните ресурси:**

Системата за управление на информационната сигурност 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 бизнеса
- Бази данни;
- Компютри, в т.ч. преносими;
- Софтуерни активи;
- Локална мрежа;
- Електронната страница на фирмата;
- Носители на информация (дискове, USB памети и др.);
- Устройства за копиране и предаване на данни;
- Комуникационни устройства;
- Инфраструктура на фирмата (електрозахранване, кабели за локална мрежа и др.) ;
- Персонал.

### ***Целите на настоящата политика са:***

- Осигуряване на непрекъснатост на бизнес процесите;
- Минимизиране на рисковете за сигурността на информацията, причиняващи загуби или вреди на Ротопринт ООД, 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;
- Информирание на служителите за техните отговорности и задължения по отношение на информационната сигурност;
- Осигуряване на съответствие с нормативни и договорни изисквания.

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

- От законова гледна точка:
  - 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:***

---

Версия 07/10.04.2024

- 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:

- **Съвет по информационна сигурност (определен със Заповед)**
  - 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.
- **Системни администратори**
  - 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.

---

Версия 07/10.04.2024

- **Отговорник по сигурността (определен със Заповед)**
  - 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.
- **Собственици на риска**
  - Участват в определяне на степента на риска, идентификацията и оценката на мерките за сигурност, правата и привилегиите за достъп до съответния актив.
  - Отговарят за определяне на политики, спазването на правилата за правилна употреба активи, генерирането, събирането, обработката, разпространението и предоставянето на информацията; защитата на Активите.
  - Собствениците носят отговорност даже когато активът е споделен. Те отговарят за контрола върху използването, поддръжката и сигурността на актива, но не придобиват право на собственост.
- **Потребители**
  - Потребителите на информационната система, се задължават да следват процедурите и инструкциите по информационна сигурност, да докладват за проблеми и инциденти в информационната система.

### ***Политика по оценка на риска:***

*Собственик: Управител*

Оценката на риска се прилага за всеки актив на организацията 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 Организацията **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 в съответствие 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 Съвета по информационна сигурност.

### ***Политика по вътрешна организация на информационната сигурност:***

*Собственик: Управител*

---

Версия 07/10.04.2024

Ръководството провежда политика за координиране на цялата дейност в организацията по внедряването и поддържането на мерките за защита.

Ротопринт ООД 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. За координиране на дейностите по отношение на сигурността на информацията е създаден Съвет по информационна сигурност.

Организацията е определила и документирала отговорностите за изпълнението на следните дейности:

- собственост и защита на активите;
- поддръжка на ключови ресурси на организацията – мрежа, сървъри, клиентски поръчки;
- закупуване, изменения и поддръжка на софтуерните ресурси;
- закупуване, изменения и поддръжка на хардуерни компоненти;
- правилата за поддръжка на инфраструктурата, вътрешния ред и контактите с външни организации;
- управление на инциденти;
- непрекъснатостта на дейността;
- сключване на споразумения за поверителност с трети страни и изисквания за защита на поверителната информация на организацията.

### ***Политика по управление на активите:***

*Собственик: Управител*

Политиката се отнася до служители, договарящи страни, консултанти, временно работещи за фирмата и други, включително и персонал на трети страни. Тази политика се отнася до цялото информационно оборудване, собственост или използвано от Ротопринт ООД.

Политиката на фирмата за използване на активите цели не да налага ограничения, противоречащи на установената фирмена култура на откритост и доверие, а да защитава служителите на Ротопринт ООД, нейните партньори и самата фирма от незаконни и увреждащи действия, извършени предумишлено или несъзнателно.

Системите свързани с Интернет, Локална мрежа, включително компютърното оборудване, приложния софтуер, операционните системи, средствата за съхранение на информация, електронната поща и други са собственост на Ротопринт ООД. Системата за подготовка на файлове (Kodak Prinergy), системата за приемане на поръчки и електронни каталози на клиентите (Kodak InSite) са собственост на Булгед ООД и се ползват съвместно. Тези системи са предназначени да се използват за целите на бизнеса в интерес на фирмата, на нашите клиенти и потребители, което налага въвеждане на правила за употреба.

Данните, които потребителите обработват и съхраняват в корпоративната система са собственост на фирмата и/или на клиентите на организацията. Поради необходимостта да се защитава информационната система на Ротопринт ООД, Ръководството на фирмата не гарантира конфиденциалност и/или цялостност и/или достъпност на личната информация, съхранявана на което и да е устройство, принадлежащо на Ротопринт ООД.

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.

Ротопринт ООД си запазва правото, чрез Системните администратори 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.

Ротопринт ООД 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.

## ***Политика за чисто работно място и екран***

*Собственик: Управител*

Политиката за „чисто бюро и чист екран“ цели да намали рисковете свързани с неоторизиран достъп, загуба или повреда на информация по време или извън обичайното работно време. Политиката взема предвид класификацията на информацията, законовите и договорните изисквания към сигурността на информацията.

Изискванията на тази политика са свързани с:

- Ограничаване на физическия и логическия достъп до конфиденциална информация чрез:
- изключване или заключване на компютрите, когато са не надзиравани
- недопускане на съхранение на конфиденциална информация в зони с достъп на външни лица

Политиката се прилага задължително в зоните с достъп на външни лица.

За реализация на политиката е разработена Инструкция Чисто работно място и екран

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 Ротопринт ООД 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 Ротопринт ООД;
- 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 Ротопринт ООД (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 Ротопринт ООД или крайния потребител нямат активен лиценз.
- Въвеждане на вреден софтуер в мрежата или сървъра (напр. вируси, троянски коне, e-mail бомби и др.)
- Разкриване на паролите или допускане на друг човек да използва акаунтите. Това включва членове на семейството или други, живеещи в дома, когато се работи вкъщи.
- Представяне на фалшиви оферти за продукти или услуги на Ротопринт ООД.
- 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 Ротопринт ООД на страни извън организацията.

## ***Политика за обмен на информацията***

*Собственик: Управител*

Политиката на организацията не налага ограничения за използване на средства за обмен на информация, но въвежда следните механизми за контрол:

- При използване на електронна поща, конфиденциална информация и информация за служебно ползване да се изпраща в прикачен файл
- Забрана за използване на незащитени мрежи при предаване конфиденциална информация и информация за служебно ползване
- Използване на антивирусни програми
- Използване на VPN за достъп до информация на сървъра на организацията и ограничаване на съхранението и на преносими компютри
- Забрана за оставяне на съобщения, съдържащи конфиденциална информация и информация за служебно ползване на телефонни секретари.
- Ограничаване на въвеждането на е-мейл адреси по подразбиране и автоматично препращане на съобщения
- Забрана за водене на служебни разговори на обществени места, отворени офис пространства или по несигурни информационни канали.

Организацията, работи само с одобрени куриерски служби и доставчици на комуникационни услуги  
Политиката на Организацията забранява съхранението на всякакъв вид служебна информация на преносими информационни средства (USB, оптическа медия).

За реализация на политиката са разработени следните документи:

- Инструкция за използване на мобилни устройства и външна памет
- Комуникационен план
- Инструкция за управление на конфиденциални поръчки
- Инструкция за управление на пароли
- Инструкция за ползване на електронна поща и интернет

## ***Политика за работа с мобилни устройства и работа от разстояние***

*Собственик: Управител*

Организация разрешава работата с мобилни устройства и работа от разстояние при спазване на следните мерки за сигурност:

- Управителите могат да използват мобилни компютри, които са конфигурирани по начин, позволяващ достъп до сървъра в съответствие с правата на съответния потребител;
- Техника не следва да се оставя без наблюдение или на видно място в автомобили
- Забранено е използване на опции „запомни паролата“ за достъп до служебна поща, VPN и сървър

---

Версия 07/10.04.2024

- Забранено е използването на свободни Wi-Fi зони за трансфер на информация;
- Забранена е работата по служебни документи от публични зони (заведения, бензиностанции, летища);
- В случай на загуба / кражба на компютър незабавно следва да се уведоми Управител или Отговорник ИТ;
- При нужда от достъп до информация от сървъра следва да се използва VPN
- За подобряване сигурността при работа с мобилни телефони и предаваната информация са въведени следните правила:
  - Използване кода за заключване или пин-кода;
  - Съхранението на конфиденциални данни и лични данни в мобилния си телефон са забранени;
  - Телефоните, на които е конфигурирана служебна поща следва да са с активирани Anti-Theft функции.

За реализация на политиката е разработена Инструкция за използване на мобилни устройства и външна памет.

### ***Политика по сигурност, свързана с човешките ресурси:***

Собственик: Управител

Човешките ресурси са основен елемент от СУИС. Политиката по сигурността на човешките ресурси на Ротопринт ООД 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, и се извършва в съответствие с разработена, документирана и внедрена **„Процедура за набиране, подбор, назначаване и освобождаване на персонал в „Ротопринт ООД”** .

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 в съответствие с **„Процедура за набиране, подбор, назначаване и освобождаване на персонал в „Ротопринт ООД” ООД”, Приложение 1**.

Всички служители на организацията, 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 Ротопринт ООД и други физически лица, които използват ресурсите на Организацията, 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:***

Собственик: Управител

---

Версия 07/10.04.2024

Ротопринт ООД провежда политика на защита на средствата за обработка и съхранение на информацията чрез определяне на граници на физическа сигурност и организация на зони за сигурност. Работните помещения и техниката се защитават от физическо влизане чрез система за сигурност с различни зони за достъп и определени права за достъп до всяка зона, посочени в **„Заповед относно различните зони на сигурност в „Ротопринт ООД” ООД и регламентирания достъп до тях”** (вж. Карти за зонирание на офисите).

Прилагат се механизми за контрол на физическото влизане, които ограничават достъп до зоните с чувствителна или критична информация само на упълномощени служители.

Определени са местата за достъп на клиенти, доставки и зареждане. За да се избегне неразрешен достъп, не се допуска присъствие на външни лица в производствените помещения на организацията без придружител от страна на служителите.

Политиката на Ротопринт ООД 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 и прекъсване в електрозахранването, защита на окабеляването и комуникационните връзки.

Изнасянето на устройства и работа извън офисите на фирмата, начините за поддръжка на информационните ресурси, както и за тяхното унищожаване или повторно използване, се извършва в съответствие със **„Заповед относно изваждане от употреба или относно повторна употреба на оборудване”**.

Ротопринт ООД провежда и политика за осигуряване на условия за безопасна работа в съответствие със Закона за здравословни и безопасни условия на труда.

След обявената в световен мащаб пандемия COVID-19 се предприемат адекватни мерки за ограничение на въздействието и в организацията, с оглед защита живота и здравето на служители, клиенти и доставчици.

- Минимизиране на социалните контакти;
- Стриктно спазване на личната хигиена и стриктно използване на лични предпазни средства;
- Дезинфекция

## ***Политика по контрол на достъпа:***

*Собственик: Управител*

Политиката на Ротопринт ООД за контрол на достъпа е базирана на принципите „необходимо да знае” или „необходимо да се ограничи”, „всеки достъп, който не е изрично разрешен е забранен” и минимизиране на привилегиите.

Ръководството на Организацията 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 де-регистрация;
- разделяне на ролите за контрол на достъпа;
- минимизиране на необходимостта от специални привилегии;
- спазване на правилата за „чисто бюро и чист екран”;
- защита на не надзиравани устройства;
- ограничаване нивата на достъп на външни потребители на информационната система

---

Версия 07/10.04.2024

- 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:***

*Собственик: Управител*

Политиката на Ротопринт ООД 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:***

*Собственик: Управител*

С цел намаляване на риска и произтичащите от появата на инциденти разходи Ротопринт ООД е разработила и внедрила политика за управление на инциденти, която е насочена към разработване и внедряване 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 в съответствие с Процедурата за докладване на слабости и пробиви в информационната сигурност.

Действията свързани с управление на инциденти се извършват в съответствие с Процедурата за управление на инциденти и 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 определен и упълномощен персонал и са документирани, и докладвани.

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 организацията 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 класифициране на информацията***

*Собственик: Управител*

Ротопринт ООД класифицира информацията, с която работи, на няколко нива, като нивото на класификация се определя на база изискванията на заинтересованите страни и на направената оценка на риска спрямо дадената информация. За целта информационните ресурси в Организацията се идентифицират като активи, записват се в Регистър на активите на Ротопринт ООД, след което се оценяват по одобрената и приета в Организацията Методика за оценка на риска. На базата на тази оценка (и по-специално на степента на въздействие върху Информационната сигурност) информацията се разделя на:

- Публична / не критична – при ниска степен на въздействие (10)
- За служебно ползване – при средна степен на въздействие (50)
- Поверителна ( вкл. клиентска ) – при висока степен на въздействие (100)

В организацията е утвърдена **Инструкция за управление на конфиденциални поръчки**, която регламентира работата с чувствителна информация на клиента.

## ***Политика за резервиране***

*Собственик: Управител*

В Организацията се извършва резервиране на работната информация и бази данни според критичността и динамичността на информационния ресурс.

Процесът на резервиране е автоматичен или ръчен и се извършва в определен времеви период. Отговорникът за резервиране следи периодично дали процесите са протекли коректно и дали резервирането на отделните системи отговаря на изискванията, заложи в плановете за непрекъснатост. Резервните копия се съхраняват на специализиран back-up сървър, където са физически защитени и отделени от оригиналните носители на информация. Системните администратори са отговорни за регулярно тестване на резервните копия за пригодност.

Обектите на резервиране на критична за всички системи в Ротопринт информация, както и точните времена и отговорностите при извършване на резервиране на информация са описани в **Процедура резервиране на информацията и Приложение1** към същата процедура.

## ***Политика за криптографски механизми за контрол***

*Собственик: Управител*

Организацията използва криптографски механизми за контрол на достъпа до критични активи. Криптографски механизми се използват при:

---

Версия 07/10.04.2024

- Използване на валиден електронен подпис за провеждане на онлайн операции с официални институции като НАП, НОИ, Търговски регистър, банки. Софтуерен токен , СМС-ТАН
- VPN - Връзката се установява чрез (TLSv1/SSLv3) автентификация на базата на цифрови сертификати, генерирани от Системните администратори. Те са отговорни за използването на този криптографски контрол.
- Възможен е и достъп през система за отдалечен достъп GUACAMOLE достъпна през https криптирана връзка. Достъпите и потребителите са описани също в регистъра за отдалечен достъп.

Ползването на криптографски механизми за контрол е регламентирано в договор с доставчика на услугата.

### ***Политика за осигуряване на непрекъснатостта на бизнеса:***

*Собственик: Управител*

Ръководството на Организацията разбира необходимостта от планиране непрекъснатостта на бизнеса. 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.

Ротопринт ООД е разработила план за непрекъснатост на работата на информационната система на Организацията, който да обезпечи непрекъснатост на работата на критичните ресурси на системата при настъпване на сериозни неблагоприятни условия и прекъсване по-голямо от 48 часа. Планът е разработен от Отговорника по сигурността и е съгласуван с ръководителите отдели и отговорниците на пряко подчинение на Управителя.

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 Организацията 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:***

*Собственик: Управител*

Политиката на организацията 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

Версия 07/10.04.2024

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 системните администратори и Отговорника по сигурността или да е с GPL лицензи. 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 РОТОПРИНТ ООД са активи собственост на организацията 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 организацията. Притежаваният от организацията 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.

Ротопринт ООД 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 Ротопринт ООД 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:***

*Собственик: Управител*

Политиката на Ротопринт ООД 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 Ротопринт ООД с цел използване на предлаганите му услуги.

Ротопринт ООД съхранява цялата информация, подадена от клиента, при строга конфиденциалност. Ротопринт ООД пази търговската тайна на клиента и на неговите клиенти и потребители, като гарантира и поема задължение да не използва нито в интерес на Ротопринт ООД, нито на негови други клиенти, партньори, свързани лица, служители и съдружници, запазени знаци, бази данни, лични данни, образи и друга информация на или за Клиента или неговите клиенти и потребители, станала известна при изпълнение на поетите професионални ангажименти.

## ***Политика за защита на личните данни:***

*Собственик: Управител*

### **Обща информация**

От 25 май 2018г. влиза в сила РЕГЛАМЕНТ (ЕС) 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 27 април 2016 година (GDPR). Регламентът има за цел да гарантира защитата на данните

---

Версия 07/10.04.2024

на физическите лица от всички държави членки на ЕС и да уеднакви регулациите за тяхната обработка.

В качеството си на администратор на лични данни Ротопринт ООД отговаря на изискванията на Регламента, като събира единствено данни на лицата дотолкова, доколкото са необходими за уреждането на трудово-правни отношения и предоставянето на услуги, и ги пази законосъобразно и отговорно.

Ротопринт ООД осъществява дейността си в съответствие със Закона за защита на личните данни и Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни.

### ***Данни за Ротопринт ООД***

ЕИК/БУЛСТАТ :130605294

Седалище и адрес на управление: 1000 гр. София, ул. Кузман Шапкарев №4

Печатница: 2129 с. Равно поле, общ. Елин Пелин, Индустриална зона

### **За връзка с длъжностно лице по защита на личните данни:**

E-mail: [administrative@rotoprint-bg.com](mailto:administrative@rotoprint-bg.com)

Телефон.: +359 2 973 2419; + 359 725 68777

### ***Компетентен надзорен орган***

Наименование: Комисия за защита на личните данни

Седалище и адрес на управление: гр. София 1592, бул. „Проф. Цветан Лазаров” № 2

Данни за кореспонденция: гр. София 1592, бул. „Проф. Цветан Лазаров” № 2

Телефон: 02 915 3 518

E-mail: [kzld@government.bg](mailto:kzld@government.bg), [kzld@cpdp.bg](mailto:kzld@cpdp.bg)

Уеб сайт: [www.cpdp.bg](http://www.cpdp.bg)

### **Цели и принципи при събирането, обработването и съхраняването на лични данни**

Ротопринт ООД събира и обработва личните данни, които ни се предоставят във връзка с използването на нашите услуги и за сключване на договор с дружеството, както и за записване за участие в наши събития, ***изцяло професионални и служебни цели:***

За да поддържаме контакт с вас и да ви предоставяме различна професионална и маркетингова информация, информация за обучения и събития в професионалната област, в която функционира фирмата ни, информация за събития които провеждаме ние, или доставчиците ни, информация за продукти и текущи промоции, както и за да таргетираме тази информация, така че тя да отговаря на професионалните ви интереси.

За да ви предоставяме информация подобряваща или свързана с ползването на продуктите които предлагаме на пазара и да подобрим предлаганите услуги на нашите клиенти като цяло.

За да осигурим необходимата техническа помощ при използването на продуктите и услугите които предоставяме на пазара.

За да осъществяваме нормалната си търговска дейност и производствена дейност- да изпращаме и получаваме информация за поръчки, информация за доставки, обсъждане на казуси, обработка на файлове, предоставени от вас и др. подобни

Във връзка със сключване на различни видове договори, изпращане/получаване на фактури, обработка на информация съгласно законови изисквания, предоставяне на информация на държавни институции съгласно законови изисквания, обработка и съхраняване на информация за защита на търговски интереси

Във връзка със защита на информационната сигурност;

Във връзка с обезпечаване на изпълнението на договор за предоставяне на съответната услуга.

### ***Ротопринт ООД спазва следните принципи при обработката на лични данни:***

законосъобразност, добросъвестност и прозрачност;

ограничение на целите на обработване;

съотносимост с целите на обработката и свеждане до минимум на събираните данни;

точност и актуалност на данните;

ограничение на съхранението с оглед постигане на целите;

---

Версия 07/10.04.2024



цялостност и поверителност на обработването и гарантиране на подходящо ниво на сигурност на личните данни.

При обработването и съхранението на личните данни Ротопринт ООД може да обработва и съхранява личните данни с цел защита на следните си легитимни интереси:

изпълнение на задълженията си към Национална агенция по приходите, Министерство на вътрешните работи и други държавни и общински органи.

Трети лица, администратори на лични данни- доставчици на услуги, необходими за осъществяването на извършваната от нас дейност

### **Какви видове лични данни събира, обработва и съхранява Ротопринт ООД?**

Информация, която ни се предоставя от субектите на лични данни:

При срещи, от постъпващи в Ротопринт e-mail-и : имена, служебен e-мейл адрес, служебен адрес, телефон, длъжност, организация в която работите, други данни съдържащи се във визитка, или e-mail, която ни е предоставена/получена.

Информация, необходима за изготвяне на договори и/или фактури- имена, ЕГН, адрес, дата на раждане и други- съгласно законовите изисквания в съответната област.

Информация от публични източници, като сайтове на фирми, рекламни материали и др. - имена, служебен e-мейл адрес, служебен адрес, телефон, длъжност, организация в която работите

Информация, която се събира автоматично- вашият IP адрес, друга обобщена не-идентифицираща Ви информация, която сайтът събира автоматично чрез използване на технологии ( напр. бисквитки) за събиране и измерване на подобна информация- напр. общ брой посещения, общо прочитания на даден материал и др. подобни.

Изрично се забранява събирането на чувствителна 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.
- Ротопринт ООД няма да продава, отдава, търгува с всякаква лична информация, получена от служителите си или от подизпълнителите.

### **Основание за събиране, обработване и съхраняване на лични данни**

Ротопринт ООД събира и обработва лични данни във връзка с наемането на персонал, уреждане на трудово-правни отношения, маркетингови цели, извършване на услуги на компании, чиито представители са субектите на лични данни на основание чл. 6, ал. 1, Регламент (ЕС) 2016/679, и по-конкретно въз основа на следното:

В някои случаи ние изискваме съгласие, за да събираме, съхраняваме и обработваме лична информация, за изпращане на информационни бюлетени, съобщения. В случай, че изберете да ни предоставите вашето съгласие, вие ще имате правото да го оттеглите във всеки един момент като заявите вашето желание или в съответния бюлетин, съобщение чрез кликане на бутон за отказ, който винаги ще присъства, или като изпратите e-мейл на адреса за съобщения, свързани с лична информация, който се намира в контактната информация по- долу. Моля имайте предвид, че оттеглянето на вашето съгласие няма да има реверсивна сила, тоест няма да се отрази на обработването, което вече е било направено през изминалия период.

В други случаи вашата лична информация се обработва съгласно законови изисквания, или във връзка с подписване на договор на който вие сте страна. Вие няма да имате възможност да промените избора си, или в случай че изберете да го промените, това ще повлияе на нашата възможност да Ви предоставим продукта, или услугата, която би била наше задължение съгласно съответния договор.

Има и случаи, в които ще обработваме данни на основание и следствие на търговски интерес на Ротопринт ООД- за да ви информира за услуги и продукти, за научни разработки, или за нови възможности, или за възможности за обучение. Вие имате възможност да се откажете от получаването на подобна информация, като изпратите съобщение до e-мейл адреса, намиращ се в контактните данни по- горе.

В случаите, когато вашата информация се обработва и използва с цел предоставяне на съответната услуга по отпечатване на етикети, вие ще имате възможност да оттеглите своето съгласие за обработване на данните ви. В случай че изберете тази възможност, това ще повлияе на възможността на Ротопринт ООД за предоставяне на тези услуги, както и на съответните договорни условия.

### **Дружеството не извършва автоматизирано взимане на решения с данни.**

#### **Споделяне на данни с трети страни**

Ротопринт може да предоставя данни на трети страни във връзка с осъществяване на различни рекламни и маркетингови цели. Тези данни са обобщени и анонимизирани и са получени чрез бисквитки и други технологии за проследяване на активности на сайта ни.

В някои случаи Ротопринт ООД може да участва в он-лайн поведенчески рекламни кампании (това в някои случаи се нарича ре-таргетирана реклама, или реклама, базирана на интереси). Можете да установите тези сайтове по иконката „AdChoices“ в съответната реклама. В тези случаи нашите партньори могат да са получили достъп до ваши данни вследствие на бисквитки, намиращи на нашия сайт, на други сайтове които сте посещавали, както и на други ваши активности в дигиталното пространство и ползват тази информация за да ви предоставят реклама, отчитаща вашите интереси. Можете да изберете да се откажете от тези рекламни съобщения като кликнете на иконката „AdChoices“ и на съответния сайт да промените данните за сайтовете и страниците които сте разглеждали, която информация се използва при подобен вид реклама. Има случаи в които тези трети страни може да продължат да събират данни за вашите интереси, но няма да ги използват за изпращане на рекламни съобщения. Можете да се откажете и сега като използвате

<http://youradchoices.com>.

Ротопринт ООД може по собствена преценка да предава част или всички Ваши лични данни на обработващи лични данни трети страни съгласно законови или договорни отношения за наемане на персонал и обработка на заплати, осигуровки, транспорт, охрана, социални придобивки при спазване на изискванията на Регламент (ЕС) 2016/679.

#### **Бисквитки:**

Системно необходими бисквитки: Това са бисквитки, без които функционирането на сайта е невъзможно или се поставя под висок риск. Тук спадат бисквитки за навигиране в уебсайта, запазване на попълнената информация при преминаване между различните стъпки, както и при вход или регистрация. Системно необходими са, също така бисквитките, осигуряващи контрол върху сигурността на връзката и защитата от нежелани външни намеси. Този тип бисквитки, често се определят като временни или сесийни, тъй като се съхраняват временно и изчезват след затварянето на сесията на браузъра.

Бисквитки за функционалност- Тази категория бисквитки служи за улесняване на потребителя при използване на уебсайта и съобразяване с индивидуални предпочитания на потребителя. Бисквитките за функционалност включват бисквитки за разпознаване на устройство, запазване на предпочитанията относно език и размер на шрифта и други. Този тип бисквитки, могат да се съхраняват по-дълго време на устройството, те могат да бъдат използвани при повече от една сесия на браузъра и се наричат постоянни.

Бисквитки на трети страни, за ефективност, анализи и реклама Бисквитките за анализ служат за събирането на статистическа информация

Можете да изберете да се откажете от събирането на лични данни чрез бисквитки чрез Деактивиране на бисквитки Като потребител имате възможност да контролирате използваните бисквитки, да изтривате запазените на Вашето устройство бисквитки, и да деактивирате употребата на бисквитки напред. Подробни инструкции за различните браузъри и операционни системи можете да откриете на адрес <http://www.aboutcookies.org/>. Имайте предвид, че блокирането на бисквитки ще се отрази на начина, по който работи уебсайтът, като може да доведе до нарушено функциониране на сайта.

#### **Срок на съхранение на личните данни**

Продължителността на съхранение на личните Ви данни зависи от целите на обработването, за които са събрани:

Личните данни, събиране с цел подбор на персонал се съхраняват до една година.

Личните данни, обработвани с цел издаване на счетоводни/финансови документи за осъществяване на данъчно-осигурителния контрол, като но не само – фактури, дебитни, кредитни известия, приемо-предавателни протоколи, договори за предоставяне на услуги/лизинг на устройства се съхраняват поне 7 до 10 години

---

Версия 07/10.04.2024

Личните данни събирани и обработвани във връзка с трудово-правни отношения се съхраняват мин. 50 години- съгласно нормативните изисквания

Лични данни, събирани и обработвани съгласно предоставяне на услуги по различни договори се съхраняват за срокове, съгласно условията на съответния договор и съгласно необходимостта от защита на съответния бизнес интерес.

#### **Защита на личните данни:**

Ротопринт ООД събира , обработва и съхранява лични данни съгласно вътрешни процедури и при спазване на съответните законови изисквания. За осигуряване на адекватна защита на данните на компанията и своите клиенти, ние прилагаме различни организационни и технически мерки.

#### **Ваши права:**

**Право на информация:** Вие имате право да поискате:

- информация за това дали отнасящи се до вас данни се обработват, информация за целите на това обработване, за категориите данни и за получателите или категориите получатели, на които данните се разкриват;

- съобщение в разбираема форма, съдържащо личните ви данни, които се обработват, както и всяка налична информация за техния източник;

**Право на корекция:** В случай, че обработваме непълни или сгрешени/грешни данни, Вие имате право, по всяко време, да поискате: да заличим, коригираме или блокираме Ваши лични данни, обработването на които не отговаря на изискванията на закона;

**Право на възражение:** По всяко време имате право да: възразите срещу обработването на личните Ви данни при наличие на законово основание за това; когато възражението е основателно, личните данни на съответното физическо лице не могат повече да бъдат обработвани;

**Право на жалба:** В случай, че смятате, че нарушаваме приложимата нормативна уредба, Ви молим да се свържете с нас за изясняване на въпроса. Разбира се, имате право да подадете жалба пред Комисията за защита на личните данни.

Заявленията за достъп до информация или за корекция се подават лично или от изрично упълномощено от Вас лице, чрез нотариално заверено пълномощно. Заявление може да бъде отправено и по електронен път, по реда на Закона за електронния документ и електронния подпис. Ротопринт ООД се произнася по Вашето искане в 14-дневен срок от неговото подаване. При обективно необходим по-голям срок – с оглед събиране на всички искани данни и това сериозно затруднява дейността ни, този срок може да бъде удължен до 30 дни. С решението си Ротопринт ООД може да даде, или откаже достъп и/или исканата от заявителя информация, като мотивира отговора си.

## ***Политика за работа с доставчици***

### *Собственик: Управител*

С всички доставчици, имащи отношение към сигурността на информацията, съответно имащи достъп до активи на организацията или предоставящи услуги и материали (комуникации, поддръжка, СОТ, логистични дейност и т.н) са обект на оценка на риска.

Всички външни експерти/организации, използвани при реализацията на основните процеси подписват задължително Декларации за конфиденциалност и/или клаузи в съответните договори.

Като допълнителни механизми за контрол се използват:

- С доставчиците на услуги задължително се подписва договор включващ договорено ниво на услугата (SLA).
- Физически достъп се осигурява в зависимост от специфичните нужди за реализация на услугата, но задължително в присъствието на упълномощен служител от Ротопринт ООД.
- Отговорност за избора на доставчици, както и за контрол върху дейността им носят управителите.
- Договорите / споразуменията специфицират правата на одит / контрол от страна на упълномощени служители от страна на Ротопринт ООД върху работата на трета страна или функционирането на системи на трета страна. Контролът върху работата на системи се осъществява чрез периодичен тест, който следва да се протоколира.

---

Версия 07/10.04.2024

## **Заклучение**

Политиката по информационна сигурност е разпространена до бизнес партньори които имат достъп до информацията и системите на организацията.

Политиката по информационна сигурност се преглежда редовно на базата на установен процес.

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 Ротопринт ООД 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 27001:2013 е основополагаща цел за реализация на бизнес стратегията на Организацията.

Разработването и внедряването на СУИС е в пълно съответствие с политиката, процедурите и практиките на Системата на управление на качеството, внедрена в Ротопринт ООД в съответствие с международния стандарт ISO 9001:2015.

***Ръководството на РОТОПРИНТ ООД декларира своята пълна ангажираност в процесите на развитие, поддържане и усъвършенстване на Интегрираната система за управление на качеството и сигурността на информацията.***