Ръководството на "ДЖИ ПИ ГРУП" АД, в лицето на Стефан Тотев, официално декларира Политиката по сигурност на информацията, която е одобрена и установява подхода на организацията към управлението на сигурността на информацията.

Политиката на "ДЖИ ПИ ГРУП" АД е да осигурява Информационна сигурност на финансовата, правна и техническа информация и данни на организацията, клиентите и трети страни във връзка с извършване на дейности по проектиране, изграждане, поддържане и ремонт на сгради, пътища и пътни съоръжения, битови и промишлени ВиК мрежи и съоръжения, електроразпределителни станции и високо строителство (обхват на сертификата)

"ДЖИ ПИ ГРУП" АД основава управлението на сигурността на информацията на базата на превенция на потенциални неблагоприятни събития, чрез систематичен анализ на средата, изискванията на заинтересовани страни, риска по отношение на сигурността и прилагане на комплекс от технически и организационни мерки за управление на риска.

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

- Осигуряване на съответствие с нормативни и професионални изисквания за конфидециалност
- защита на данни и неприкосновеност на лична информация;
- достъпност на информацията за реализация на основните процеси;
- опазване на архивите на организацията;
- защита на клиентска, търговска информация, права върху интелектуална собственост и фирмено ноу хау.

<u>Целите на настоящата политика са:</u>

- осигуряване на непрекъснатост на бизнес процесите;
- минимизиране на рисковете за сигурността на информацията, причиняващи загуби или вреди на Организацията, 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 функционирнато на ефективна Система за управление;
- информиране на служителите за техните отговорности и задължения по отношение на информационната сигурност;
- осигуряване на съответствие с нормативни и договорни изисквания.

Отговорности:

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

Системни администратори:

Отговарят за управление и поддържане на интернет свързаността в организацията, електронна поща, сървъри, локална мрежа, архивиране, техническа защита на активите (софтуер и хардуер); 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.

Отговорник по сигурността

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 на активите, 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.

Разработването и внедряването на Система за управление на информационна сигурност съгласно международния стандарт ISO 27001 е основополагащо средство за реализация на бизнес стратегията на Организацията.

Организацията е уведомила всички заинтересовани лица, че прилага политики за информационна сигурност чрез сайта си, както и чрез електронния подпис, с който се подписва кореспонденцията към трети лица по електронен път.

Политиката по информационна сигурност се преглежда редовно и 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 "ДЖИ ПИ ГРУП" АД се задължава да спазва всички правила, свързани с информационната сигурност, описани в процедури, инструкции и други документи от СУИС.

Политика за контрол на достъпа

Политиката на "ДЖИ ПИ ГРУП" АД за контрол на достъпа е базирана на принципите „необходимо е да знае" и „необходимо е да ползва" и минимализиране на привилегиите. Политиката за контрол на достъпа включва прилагането на механизми за контрол както на физическия, така и на логическия достъп.

Ръководството на Организацията прилага мерки на контрол на достъпа, които да осигуряват:

- физическа защита на информационните активи;
- Достъп до съответните информационни активи в съответствие с установена матрица за достъп и на ръководството на организацията и само след официално оторизиране на заявките за достъп от страна на изпълнителен директор.
- прилагане механизми за контрол на физическото влизане;
- определяне на нивата на достъп в съответствие с ролята, която трябва да изпълняват служителите на организацията и нивата на класификация на информацията и активите;
- отнемане на права на достъп при напускане;
- периодичен преглед на достъпа и правата на достъп
- Ъпргрейд на контрола на достъп в отговор на нови заплахи, възможности, изисквания на бизнеса или изводи от инциденти.

За реализация на политиката са разработени следните инструкции и процедури:

- Процедура за Управление на IT инфраструктора.

Политика за класифициране и обработка на информацията

Политиката за класифициране, обработване и съхранение на информацията и на физическите активи се основава на заинтересованите страни. Класификацията се извършва от собствениците на съответните активи/информация и включва три нива:

- A- Конфиденциална / критична
- B- За служебно ползване / с нормална важност
- C- Публична / не критична

Класификацията се извършва на база на стойността, чувствителността и критичността на информацията по време на целия и жизнен цикъл и потенциалните последствия, които компрометирането ѝ би имало върху организацията.

Ниво А обхваща:

- Контакти на клиенти, ценова информация, финансова информация(потоци,плащания)
- База данни (пазарни стойности)
- Информация за заплати и бонуси, финансова информация от договори и оценки.
- Печати, наеми и услуги.
- Лични данни на служители или клиенти (ЕГН, банкови сметки, адреси и др.)

Софтуер:

- Електронни подписи и спеиализиран софтуер.

Хардуер:

- Основен сървър, бекъп сървър, комуникационно оборудване (офиси) мобилни устройства на управители.

Ниво В обхваща:

- Уеб сайт, възлагателни писма, договори с клиенти, документи на клиенти (нотариални актове, скици, описи, планове) копия.
- Фактури, счетоводни документи, договори за външни услуги, договори на СУ.
- Досиета на служители, архиви, документи на всички софтуери и приложения в организацията.
- Административни документи (актуално състояние, декларации, учредителен акт и др.)

Софтуер :

- Операционна система (WINDOWS) SERVER.
- Счетоводен и ТРЗ софтуер.

Хардуер:

- Мобилни смарфони и мобилни компютри (лаптопи)

Услуги:

- Интернет свързаност, мобилна комуникация, наеми и услуги регионални офиси, банково обслужване и куриерски услуги.

Ниво С обхваща:

- Операционна система (WINDOWS) работни станции, антивирусни на работните станции, офис приложения (програми)

- Стационарна комуникация, хостинг.
- Мобилни телефони и периферни устройства (Принтери, скенери и др.)

Всички активи, както и тяхната класификация са описани в Регистър на информационните активи.

Политика по физическа сигурност и сигурност на заобикалящата среда

"ДЖИ ПИ ГРУП" АД 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.

Политиката на "ДЖИ ПИ ГРУП" АД по отношение на защита на устройствата цели намаляване на риска от неразрешен достъп до информационни активи, 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.

В офис сградата са определени местата за достъп на клиенти, доставки и зареждане. Физическата сигурност и защитата на заобикалящата среда в офис пространствата се осигурява чрез механизми за контрол на физическия достъп (ключ и карта за достъп). В зоните с достъп на външни лица не се разполагат критични информационни активи

За реализация на политиката са разработени следните инструкции и процедури:

- Инструкция за работа с доставчици и трети страни

Политика по управление на активите

Политиката се отнася до служители, външни експерти, временно работещи за фирмата и други, включително и персонал на трети страни. Тази политика се отнася до цялото информационно оборудване, собственост или използвано от "ДЖИ ПИ ГРУП" АД или нейни клиенти, както и до наличната информация.

Политиката на фирмата за използване на активите е свързана с налагане на стриктен контрол по отношение на всички физически и логически действия. 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 "ДЖИ ПИ ГРУП" АД, 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 "ДЖИ ПИ ГРУП" АД. Тези системи са предназначени да се използват за целите на бизнеса в интерес на фирмата, нейните 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 "ДЖИ ПИ ГРУП" АД, Ръководството на фирмата не гарантира конфиденциалност на личната информация, съхранявана на което и да е устройство, принадлежащо на "ДЖИ ПИ ГРУП" АД.

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.

За реализация на политиката са разработени следните инструкции и процедури:

- Процедура за управление на ИТ инфраструктура
- Инструкция за работа с интернет и електронна поща

Политика за „чисто бюро и чист екран“

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 ненадзиравани
  - 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 бюро / чист екран“

Политика за обмен на информацията и сигурност на комуникациите

Политиката на организацията не налага органичения 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
- 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 не позволява работа с преносими информационни средства (USB, оптическа медия).

За реализация на политиката са разработени следните инструкции и процедури:

- Процедура Управление на ИТ инфраструктура

- Инструкция за работа с интернет и електронна поща

Политика за работа с мобилни устройства и работа от разстояние

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

- Достъпът до сървър и други приложения на организацията се достъпват единствено през VPN;
- 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 и сървър;
- 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 Отговорник по сигурността;
- За подобряване сигурността при работа с мобилни телефони и предаваната информация са въведени следните правила:
    - Съхранението на конфиденциални данни и лична данни в мобилния си телефон са забранени;
    - Телефоните, на които е конфигурирана служебна поща следва да са с активирани пароли за отключване или друг начин на заключване.

За реализация на политиката са разработени:

- Процедура Управление на ИТ инфраструктура

Политика за инсталиране и използване на софтуер

Политиката на “ДЖИ ПИ ГРУП” АД 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.

Всички изменения в хардуера и в софтуера на системата се извършват само с предварително разрешение.

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 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. 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 “ДЖИ ПИ ГРУП” АД са активи собственост на организацията и трябва да бъдат използвани само с лицензиран софтуер, както и да бъдат защитени от вируси. Забранява се на потребителите да внасят 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.

Организацията е утвърдила списък с разрешен софтуер. Забранява се инсталирането на софтуер, различен от разрешения без съгласуване с Отговорника по сигурността или ръководител отдел.

Политика по резервиране

Политиката на резервиране е базирана на оценка на риска от загуба на информация, като се цели трикратна резервираност, както следва:

- Резервиране на проекта информация на сървъра
- Резервиране на виртуално копие извън организацията
- Резервиране на електронната поща

За реализацията на политиката е разработена Схема на back-up - част от процедурата за управление на IT инфраструктура

Политика по защита от злонамерен софтуер

Политиката е насочена към навременно откриване на злонамерен софтуер и възстановяване на работоспособността, както и осъзнаване на механизмите за контрол от злонамерен софтуер от страна на служителите. За целта се налагат следните правила за работа:

- използване на антивирусни програми за защина на сървър и работни станции
  - сканиране на всички файлове чрез външни памети или по мрежа
  - сканиране на интернет страници
  - сканирани на прикачени файлове
  - ежедневна актуализация на антивирусни дефиниции
- използване на защитни стени (Firewall)
- контрол на входящия трафик
- провеждане на редновни прегледи в рамките на профилактика на системите
- Използване само на лицезиран софтуер и/или freeware, забрана за използване на неоторизиран софтуер
- Редовна инсталация на updates на операционни системи
- Незабавно докладване според утвърдена процедура за управление на слабости и инциденти (част от Управление на ИТ инфраструктура)
- Спазване на Инструкция за работа с интернет и електронна поща

Политика за управление на техническата уязвимост

Управлението на техническата уязвимост в организацията се базира на:

- Поддържане на описи(регистри) на активите, включително информация за доставчици, версии на софтуер, отговорности за поддръжа;
- Извършване на изменения на системите под контрола на СА, Отговорника по сигурността и след оторизация от страна на Изпълнителен директор;
- Редовна профилактика на системите;
- Договор за поддръжка с регламентирани времена за реакция;
- Процедури за докладване на събития инциденти и уязвимости в информационните системи;
- Контрол върху инсталация на актуализации и security patches на софтуер;
- Редовен анализ на идентифицираните уязвимости и докладвани слабости / събития свързани със сигурността на информацията.

За реализация на политиката е разработена Процедура за Управление на ИТ инфраструктура.

Политика по сигурност, свързана с човешките ресурси

Човешките ресурси са основен елемент от СУИС. Политиката по сигурността на човешките ресурси на “ДЖИ ПИ ГРУП” АД е насочена основно към осъзнаване на необходимостта от осигуряване на информационната сигурност чрез адекватно дефиниране на отговорности и обучение.

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 “ДЖИ ПИ ГРУП” АД и други физически лица, които използват ресурсите на Организацията, подписват Споразумение за конфиденциалност, която представлява част от трудовите договори.

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 за използване на криптографски механизми за контрол

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

- Използване на валиден електронен подпис за провеждане на онлайн операции с официални институции
- VPN
- Уеб приложения
- Webmail

Политика за управление на паролите

Политиката за управление на паролите е базирана на оценката на риска в Джи Пи Груп АД, която взима под внимание достъпа на служители до класифицирана клиентска и вътрешна информация. Всеки служител, който има достъп до тези информационни активи е длъжен да използва силни пароли според политиката на организацията. Политиката важи за всички достъпи, които един служител използва.

След първото си влизане, всеки нов служител е длъжен да създаде собствена уникална парола, която да отговаря на следните правила:

- Минимум 8 символа при използване на поне 3 типа знаци.
- Паролата не трябва да включва имена или стандартни фрази
- Служителите не трябва да използват идентични пароли с тези на личните им акаунти

За Системните администратори добавени следните допълнителни мерки за сигурност:

- Минимум 9 символа при използване на 4 типа знаци.

Служителите нямат право да споделят паролите си на никого, както и да ги съхраняват на хартиен или електронен носител.

Политика за защита на личните данни

Политиката на “ДЖИ ПИ ГРУП” АД за защита на личните данни е изцяло съобразена със Закона за защита на личните данни.

“ДЖИ ПИ ГРУП” АД събира лични данни единствено за уреждане на трудово-правните взаимоотношения със своите служителите. Информацията не се използва повторно за цели, несъвместими с първоначалните.

Информацията, която “ДЖИ ПИ ГРУП” АД може да събира, включва данни от лични карти, телефонни, 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.

“ДЖИ ПИ ГРУП” АД няма да продава, отдава, търгува с всякаква лична информация, получена от служителите си или от подизпълнителите. Определените отговорни служители, обработващи лични данни, са задължени да третират информацията като конфиденциална.

Предприети са мерки за физическа и логическа защита на личните данни и са ограничени правата за достъп до тях.

Всеки служител, за когото се отнасят данните („субект на данни“) има право на достъп до своите данни, както и да изиска тяхното коригиране.

Политика за взаимоотношения с доставчици

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

Всички външни експерти, използвани при реализацията на основните процеси подписват задължително Договори с включена Клауза за конфиденциалност.

Като допълнителни механизми за контрол се използват:

- С доставчиците на услуги се подписва при необходимост договор включваш 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 "ДЖИ ПИ ГРУП" АД.
- Отговорност за избора на доставчици, както и за контрол върху дейността носи Изпълнителен директор.
- Договорите / споразуменията специфицират правата на одит / контрол от страна на упълномощени служители от страна на "ДЖИ ПИ ГРУП" АД 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.

За реализация на политиката е разработена Инструкция за работа с доставчици и трети страни.

Политика за сигурно разработване на софтуер от външни страни

В случай на възлагане на разработка на софтуер от външни страни се прилагат следните контроли за защита на информационната система на "ДЖИ ПИ ГРУП" АД:

- Възлагат се единствено на утвърдени доставчици на услуги с подписан SLA и рамков договор;
- Параметрите на разработване се обсъждат на работна среща и се утвърждават с Техническо задание от Доставчика;
- Техническото задание се утвърждава от Изпълнителен директор;
- Разработването и тестването на софтуера се извършват извън инфраструктурата на "ДЖИ ПИ ГРУП" АД;
- Тестването не се извършва с реални данни на "ДЖИ ПИ ГРУП" АД;
- "ДЖИ ПИ ГРУП" АД не разполага с достъп до кода на разработения софтуер и всяка желана промяна се съгласува с Доставчика.

Ръководството на "ДЖИ ПИ ГРУП" АД ЕООД декларира своята пълна ангажираност в процесите на развитие, поддържане и усъвършенстване на СУИС.