

Приложение 5

ПРОЕКТ

Политика за организация и управление на информационната система и информационната сигурност, защита на информацията и данните на клиентите

Съдържание

1 Въведение	3
1.1.Цели	3
1.2 Обхват и предназначение	4
1.3 Принципи на информационната сигурност	4
1.4 Отговорности	5
1.5 Административни въпроси	6
2. Политика	6
2.1.Организация на Информационната система и сигурност в „Дис Трейдинг" ООД.....	6
2.2. Структурни звена и роли	6
3. Комуникации с надзорни и държавни институции	9
4.Сигурност при достъп на трети страни	9
5.Класификация, използване и управление на информационните активи	10
6.Физическа защита и контрол на средата.....	12
7. Управление на операциите и комуникациите	12
8. Контрол на достъпа	14
9. Управление на инциденти.....	18
10. Непрекъсваемост на бизнеса	18
11. Публикуване на политиките за сигурност.....	20
12.Дефиниции.....	20

1. Въведение

1.1 Цели

С непрекъснатото и динамично развитие на технологиите и глобализацията на финансовите услуги, рязко нараства честотата и формите на опитите за злоумишлено вмешателство и неправомерно придобиване и ползване на информация във финансовата сфера. Поради това, Дис Трейдинг ООД счита за изключително важно опазването на наличието, поверителността и целостта на информационната система, с оглед прякото ѝ влияние върху неговата дейност и мащаба на потенциалните неблагоприятни последици. Информационната сигурност е неотменен елемент от единната концепция за корпоративна сигурност, която дружеството прилага. Тя се изразява в защита на информацията от широк кръг събития, с цел гарантиране на непрекъсваемостта на бизнес процесите, минимизиране на операционния риск и нарастване на възвращаемостта от инвестициите. Настоящата „Политика за организация и управление на информационната система и сигурност“ (Политика) има за цел да дефинира минималните изисквания за поддържане на допустимо ниво на риск за дружеството по отношение на информационната система и сигурност, както и задълженията на мениджмънта и служителите за опазване на информационните активи на „Дис Трейдинг“ ООД и защита данните на клиентите.

С настоящата Политика ръководството на дружеството си поставя следните основни цели по отношение на информационната система и сигурност:

- осигуряване на съответствие с приложимото законодателство и договорените изисквания;
- осигуряване на непрекъсваемост на процесите при запазване на цялост и достъпност на информацията;
- минимизиране на рисковете за сигурност на информацията, причиняващи загуба или вреди на дружеството;
- осигуряване на необходимите ресурси за поддържане на Политиката и повишаване на нейната ефективност;
- информираност и обучение на служителите по отношение на информационната сигурност.

Документът дефинира нормативна рамка, с която следва да се съобразяват допълнителни правила и процедури, които касаят внедряването на конкретни контроли, свързани с информационната система и сигурност на „Дис Трейдинг“ ООД.

1.2 Обхват и предназначение

Аспектите на организация и управление на информационна система и сигурност обхващат:

- Дейността на ръководството по отношение на определянето на основните насоки и политика за управление на информационната система и сигурност, които да са в съответствие с изискванията на действащото законодателство, както и специфичните изисквания в платежната сфера;
- Организационните въпроси, включително въпросите, засягащи достъпа на трети лица;
- Класифициране и управление на активите и информационните потоци;
- Сигурността на персонала;
- Физическата сигурност и безопасното използване на оборудването;
- Управление на комуникациите;
- Контрол на достъпа до информационните потоци;
- Придобиване и поддържане на информационни масиви и системи;
- Управление на инциденти по информационна сигурност;
- Осигуряване на непрекъсваемост на процесите;
- Осигуряване на съответствие със законовите изисквания по отношение на сигурността;

Политиката е приложима към следните категории, наричани по-нататък „субекти“:

- Целият личен състав на дружеството (независимо от вида на трудовия договор);
- Трети страни;
- Всички други индивиди и/или групи, на които е гарантиран достъп до информационната система на дружеството.

1.3 Принципи на информационната сигурност

В Политиката за информационната система и сигурност на дружеството са заложили следните

основни принципи:

- Процесен подход – Управляваните събития се разглеждат, като процеси или като отделни етапи от процеси;

Системен подход – Нищо, което се прави по отношение на информационната система и сигурност, не е самоцелно и изолирано. Всички аспекти на информационната система и сигурност са взаимосвързани и са част от общата политика на дружеството

- Основаване върху анализа на риска – Управлението на информационната система е поставена на обективна основа. Анализът на риска се основава на метод, генериращ надеждни и повторими резултати;

- Целесъобразност – Изразходването на ресурси винаги подлежи на обосновка. Не се допуска разходите за защита да са по-високи от защитавания актив;

- Разделяне на права и задължения – Този принцип се прилага винаги, когато е необходимо да се генерира невъзможност от злоупотреба с права;

- Решаваща роля на ръководството на дружеството – Ръководството на дружеството отговаря в най-голяма степен за информационната система и сигурност и съзнателно я поема. Ролята на ръководството е решаваща за постигане на целите в политиката за информационна система и сигурност.

1.4 Отговорности

Всеки служител на „Дис Трейдинг“ ООД е длъжен да познава настоящия документ и да прилага в ежедневната си дейност залегналите в него принципи и изисквания. Спазването на правилата за информационната система и сигурност е задължително. Неспазването на изискванията на последната се разглежда като нарушение на сигурността.

Управителят и ръководител „Сигурност“ отговарят за спазването на Политиката в рамките на дружеството. Всички структурни единици на дружеството са потенциален обект на контрол, касаещ съблюдаването на клаузите на тази Политика.

Всички правила и процедури, имащи отношение към информационната система и сигурност на дружеството и свързани с настоящата Политика подлежат на преразглеждане и актуализация. Отговорност за поддържане актуалността на тези документи носи

дирекция „Информационни технологии“.

1.5 Административни въпроси

При неспазване на Политиката за информационна система и сигурност и произтичащите от нея нормативни документи на дружеството, административните въпроси ще бъдат третираны като „инциденти и злоупотреби с информационната система“. Служителите подлежат на административна отговорност в съответствие с разпоредбите на действащото в Република България законодателство, както и на финансови санкции в случаи на причинени на дружеството вреди. Горното не отменя съдебно преследване в случай на престъпно деяние от страна на служителите на дружеството. При тези обстоятелства дружеството съдейства на съответните органи за изясняване на обстоятелствата в рамките на Закона.

2. Политика

2.1 Организация на Информационната система и сигурност в структурата на „Дис Трейдинг“ ООД

Цел: Изграждане и поддръжка на ефективно работеща организация за управление на информационната система и сигурност, която обхваща всички звена и информационни ресурси на дружеството.

2.2. Структурни звена и роли

Общо събрание - Общото събрание представлява дружеството само в отношенията с Управителя и упражнява контрол върху дейността му. В изпълнение на това, то:

- одобрява Политиката за информационната система и сигурност;
- осигурява необходимите условия за осъществяване на контролни механизми относно информационната система и сигурност;
- запознава се с доклади от извършени проверки по информационната система и сигурност и предприетите от управителя мерки за отстраняване на идентифицираните в тях слабости.

Управител - Управителят управлява и представлява дружеството и във връзка с това демонстрира ангажираността на ръководството на дружеството по отношение на информационната система и сигурност като:

- участва в процеса на дефиниране на приемливите нива на риск за дружеството по отношение на

информационната система и сигурност;

- участва в процеса на периодичен преглед на политиката за информационна система и сигурност;
- одобрява вътрешно-нормативни документи, подчинени на Политиката за информационна система и сигурност;
- осигурява ясна насока и подкрепа за всички инициативи, свързани с информационната система и сигурност;
- отговаря за контрола върху цялостния аспект на информационната система и сигурност;
- одобрява делегирането на специфични функции и отговорности, свързани с информационната система и сигурност в организацията на дружеството;
- одобрява планове и програми за повишаване на информираността на служителите по отношение на сигурността;
- осигурява комуникирането на конкретните имплементации, свързани с информационната система и сигурност в организацията.
- приема планове и бюджети за обезпечаване на информационната система и сигурност;
- обезпечава дейността по информационна система и сигурност с необходимите човешки, финансови и материални ресурси;

Звено за информационни технологии - координира дейностите, свързани с управлението на информационната система и сигурност и обхваща съвместни действия на потребители, администратори, разработчици, вътрешен контрол, служители по сигурността в съответствие с нормативните изисквания. Дейността на звеното включва:

- отговаря за техническото управление и контрола над дейностите в дружеството, свързани с информационната система и сигурност;
- отговаря за изпълнението на мерките за осигуряване на наличието, целостта, автентичността и поверителността на всички данни и информацията, която директно и индиректно влияе на бизнес процесите в дружеството;
- определя стратегическите рамки за развитието на информационните системи по отношение и

информационната сигурност;

- отговаря за управлението, координиране и разработка на всички технически, физически, административни, организационни и оперативни задачи и мерки в пряка връзка с осигуряването на информационната система и сигурност, както и за спазването на всички вътрешни и външни регулации пряко свързани с нея;
- отговаря за предотвратяването, установяването и разследването на всякакъв вид инциденти - вътрешни и външни, свързани с информационната система и сигурност и които подлагат на риск дружеството, неговите служители и клиенти;
- дефинира изисквания към контролите за информационната система и сигурност в дружеството, оценява механизмите за контрол на информационната сигурност;
- изготвя и своевременно актуализира вътрешнобанковите нормативни регулации, свързана с въпроси, касаещи информационната сигурност;
- осигурява необходимото техническо съдействие за дейности на други звена, с цел посрещане на дефинираните изисквания към контролите за информационна система и сигурност;
- има контролни функции над всички операции, свързани с информационната сигурност.

Оперативният процес по организация и управление на информационните системи на дружеството се координира от ръководител „Информационни технологии“ подпомогнат и от ръководител „Сигурност“ (в сферите на неговите компетенции). Всички останали звена на имащи преки оперативни отговорности по въвеждане и поддръжка на контроли за сигурност, които нямат пряка връзка с информационната система се считат за допълнителни членове на организацията.

Независима оценка на информационната система и сигурност - Специализираната служба „Вътрешен контрол“ носи отговорността за дефиниране, планиране и извършване на независимо оценяване на процеса за прилагане на тази Политика.

Звено „Информационни технологии“ следва винаги да бъде информирано за резултатите от извършените проверки. Всички открити слабости, които водят до неприемливи нива на риск следва да бъдат обект на последващи действия за преодоляването им, като отговорност за това носи ръководител „Информационни технологии“. Цялостна оценка на риска по отношение на информационната сигурност на всички системи в дружеството следва да се извършва на всеки три години като се препоръчва участие на външен за дружеството одитор. За всички неприемливи нива

на риск следва да се предприемат мерки за снижаването им като отговорен за координиране на процес по оценка на риска и дефиниране на последващи действия е ръководител „Информационна технологии“.

3. Комуникации с надзорни и държавни институции

Служителите на „Информационни технологии“, чиито задължения са пряко свързани с обезпечаването на сигурността на информационната система в дружеството комуникират с надзорните и държавни органи по реда установен в съответните вътрешни регламенти.

4. Сигурност при достъп на трети страни

Достъпът на трети страни до информационната система подлежи на специален контрол. Трети страни, изискващи достъп до информационната система /ИС/ на дружеството трябва да са обвързани с договор, регламентиращ изискванията на Дис Трейдинг ООД към тях, по отношение на ИС. Преди окончателно да им бъде даден достъп, те трябва да подпишат декларация за спазване изискванията за работа с ИС и достъп на трети страни, а когато става въпрос за ключови данни, се подписва и декларация за опазване на професионална и търговска тайна.

5.Класификация, използване и управление на информационните активи

Цел: Постигане и поддържане на необходимото ниво на защита на информационните активи на „Дис Трейдинг " ООД.

Всички информационни активи на дружеството следва да бъдат описани и да имат назначени притежатели. За всеки информационен актив следва да има дефинирани защитни контроли и изисквания за тяхната поддръжка. Осъществяването на конкретен контрол може да бъде делегирано от притежателя на актива, но задължението за надлежното му опазване остава негова.

Класификация на информационните активи

Информационните активи се класифицират, като тази информация се съхранява в специална база данни, позволявайки по този начин подходящ мениджмънт и контрол, при спазване на изискванията за създаване, ползване, съхранение и унищожаване на информация, представляваща държавна и професионална тайна”.

Притежатели на информационните активи

Собственик на информацията и на материално-техническите ресурси е „Дис Трейдинг“ ООД. Отговорността за защита на информацията и поддържащите технически средства е възложена на оторизирани служители - „материално отговорни лица“ по смисъла на Кодекса на труда. Всички информационни активи следва да имат дефинирани собственици, които отговарят за съответните активи, съгласно конвенциите на ИС. Освен това те са задължени да:

- поддържат правилната класификация на информацията;
- извършват периодичен преглед и ревизия на ограниченията за достъп до информационния актив предвид действащите политики.

Информационната сигурност при персонала

Внедряват се контроли, за да се намали риска от човешки грешки, кражби, измами, нарушения или ползване на оборудването за зловредни цели. Там, където е необходимо, се включват в длъжностните характеристики на персонала - роли и отговорности по отношение на ИС. Те обхващат всички специфични отговорности за защита на определени активи и/или изпълнение на съответни процеси/действия, повишаващи сигурността на последните.

Изисквания, свързани с информационната система и сигурност при наемането на нови служители

За всяко работно място и позиция следва да има ясно дефинирана длъжностна характеристика, която определя точно съответните професионални задължения и отговорности, включително - очаквания и ангажименти, свързани с информационната система и сигурност.

Всички длъжностни характеристики се утвърждават от управителя и се съхраняват и поддържат актуални от звено „Нормативно съответствие“, в сътрудничество със съответният ръководител на звено. Изискванията на „Дис Трейдинг“ ООД към служителите относно достъпа и работата с информационните ресурси на дружеството, стандартите за професионална етика, професионална тайна и трудова дисциплина се определят и с Правилника за вътрешния трудов ред, индивидуалните трудови договори на служителите и други вътрешни регулаторни документи.

Изисквания, свързани с информационната сигурност по време на установени трудови правоотношения на служителите с дружеството.

Служителите се задължават да подпишат необходимите декларации за защита на конфиденциалност на информацията при постъпване на работа. Отговорност за предоставяне на

необходимият набор документи на постъпващите на работа в Банката лица носят Управителят и служителите от „Нормативно съответствие“. Звено „Информационни технологии" извършва периодичен контрол над подписаните от служителите декларации за конфиденциалност. „Информационни технологии " има право да инициира извършването на допълнителни проверки, които се фокусират върху определена област, служител или външни партньори на дружеството.

Обучение на служителите по въпроси, свързани с информационната система и сигурност

Нуждата от подходящо обучение се определя съгласно процедурата е от първостепенна важност. Звено „ИТ“, съгласувано с управителя определя начините за осведомяване на персонала и трети страни относно изискванията по информационната система и информационната сигурност.

Дисциплинарен процес

Всяко нарушение на действащите вътрешни регулации, свързани с информационната система и сигурност или нарушение на законовата рамка, в чийто контекст те оперират има правни последици. Процесът на санкциониране се извършва по дисциплинарен ред съгласно изискванията на Кодекса на труда по инициатива на ръководител „Информационни технологии". Всеки служител или мениджър забелязал събитие, което нарушава пряко или косвено Политиката за организация и управление на ИТ системата и информационната сигурност на дружеството следва да информира за това звено „Информационни технологии". Звено „Информационни технологии " провежда необходимите действия. Ако резултатът от разследването покаже недостатъчност на контролите за сигурност, „Информационни технологии " изготвя предложение за промяна на регулаторните процедури и въвеждане на допълнителни контроли, които да адресират конкретния проблем.

Изисквания, свързани с информационната сигурност при прекратяване на трудовите правоотношения на служителите с дружеството или при промяна на договорните условия

Ръководителите на структурни единици, звено „Информационни технологии" са отговорни за спазване на всички изисквания за сигурност при прекратяване на трудовите правоотношения със служители на дружеството, както и при промяна на служебните му задължения или позицията, която заема.

Връщане на активи

Всички служители, сътрудници и трети лица, които имат договорни отношения с дружеството са длъжни да върнат зачислените им активи при прекратяване на правоотношенията си с

дружеството, в това число всички информационни активи - софтуер, корпоративни документи, оборудване, мобилни компютърни устройства, мобилни телефони, кредитни карти, карти за достъп до помещения, сертификати, информация, съхранявана на електронни носители и др. Информационните активи намираща се върху оборудването с което е работил служителя принадлежи на дружеството и следва да се трансферира или архивира върху подходящи носители и да се предаде на прекия ръководител. Отговорност за инициране на този процес носи прекият ръководител на служителя.

Анулиране на права за достъп

При прекратяване на трудови правоотношения на служител се анулират всички права за достъп до информационните системи на дружеството. В случай, че служителят е част от група, на която са делегирани определени права за достъп, то той трябва да бъде изведен от тази група и всички членове на групата да се информират за неговото напускане, за да се елиминира възможността за косвен достъп до информация и ресурси. Правата за достъп следва да бъдат редуцирани или анулирани в зависимост от нивата на риск още преди служителят да напусне окончателно работното си място, което се иницира от съответния пряк ръководител.

6. Физическа защита и контрол на средата

Внедряват се контроли за избягване неоторизиран достъп до, влияние или повреда на информационните активи. Компютърните системи и мрежи се защитават чрез подходящи физически, технически или процедурни security-контроли. Файловете сървъри и машините, съхраняващи или обработващи данни с високо ниво на критичност и/или висока степен на чувствителност и наличност, трябва да са монтирани в помещения, физическият достъп до които се контролира. За общите изискванията за физическа сигурност и контрола над средата е отговорен ръководител „Сигурност”.

7. Управление на операциите и комуникациите

Внедряват се контроли, позволяващи коректна и сигурна работа на устройствата за обработка на информация.

7.1. Документирани работни процедури

Подготвя се и се поддържа документация (работни процедури) по създаването и конфигурирането на ИС, като се вземат предвид различията между отделните системни платформи. Чувствителната документация се съхранява и достъпва контролирано, на база подхода „необходимо да се знае”.

7.2 Разпределение на задълженията

Достъпът до критични системи и ключови данни и информация се гарантира само на база принципа „необходимо да се знае”.

За критичните системи се осигурява разделение на задълженията, касаещи работната среда. Пълен, неограничен по време достъп до реално работещи системи може да има само персонала, чиято роля и длъжност непременно го изисква. Идентифицират се чувствителните операции и се вземат мерки за прилагане на разделно-функционални контроли, където това е необходимо.

7.3. Промени в системите

Всяка промяна в „жива” критична система трябва строго да се придържа към съответния предварително дефиниран процес за контрол на измененията.

7.4. Тестове за нивото на сигурност

Критичните системи се подлагат на периодични тестове за ниво на сигурност.

7.5. Контроли срещу зловреден софтуер

Въвеждат се контроли, позволяващи проверка за появата на зловреден софтуер в средата на критичните системи.

7.6. Защита срещу вируси

За целите на антивирусната защита, за да се ограничи въвеждането и разпространението на компютърни вируси, както в рамките на дружеството, така и извън нея се внедрява и поддържа процедура „Защита срещу зловреден софтуер”.

7.7 Секюрити актуализации и други видове софтуерни доработки

Служителите на Дис Трейдинг ООД, които отговарят за ежедневното управление на системите са длъжни да осигурят прилагането на секюрити актуализации и други подобни софтуерни доработки.”

7.8. Резервни копия и архивиране

Създаването и поддържането на резервни копия и архиви на критични системи и данни се извършва в съответствие с процедурата "Непрекъсваемост на бизнес-процесите".

7.9 Работа с носители на данни. Съхранение. Повторно използване

Боравене с и съхранение на носителите

Носителите, съдържащи ключови данни се маркират, транспортират и съхраняват съгласно изискванията за „Класификация и защита на информацията”.

Повторна употреба и бракуване

Сменяемите магнитни или оптични информационни носители, съдържащи ключови данни, ако последните не са необходими, се използват повторно или бракуват чрез строго контролиран процес и в съответствие с изискванията за „Класификация и защита на информацията”. В случаите, когато се преотстъпва компютърна техника и/или носители, съдържащи ключови данни се прилага същата процедура с оглед на това горните данни да бъдат предварително и окончателно изтрети.

7.10 Обмяна на информация и софтуер

Използване и контрол на софтуера

Софтуерът се използва, управлява и контролира в съответствие със законовите норми. Всички основни софтуерни актуализации, базирани на вътрешни или външни разработки, които засягат критични системи се контролират и тестват с помощта на управляем процес, преди да бъдат приложени върху съответната жива система.

Ползване на Интернет

Дейностите, включващи ползване на Интернет се регламентират от процедурата "Използване на компютърните системи". Системите, осигуряващи външни услуги трябва да са подходящо защитени срещу атаки чрез съответни апаратно програмни средства. Необходимо е също така да се използват и съвременни IDS/IPS средства.

7.11 Ползване на криптография

Паролите за системна администрация и за управление на акаунтите трябва задължително да бъдат криптирани. Криптират се и електронните съобщения, съдържащи чувствителна или класифицирана информация. Тази процедура покрива също генерирането и използването на различни видове сертификати и електронни подписи.

8. Контрол на достъпа

8.1.Отговорности на потребителите

Субектите, използващи Интернет в рамките на компютърната система и/или мрежи трябва да спазват изискванията за използване на компютърните системи.

8.2.Изисквания за достъп до системите

8.2.1 Управление и администриране достъпа

_На субектите се предоставя специфичен достъп до ИТС на дружеството съответстващ на привилегиите, които са им дадени. Прилагат се формални инструкции, за гарантиране достъпа на потребителите, както до ИТС на дружеството, така и до външни услуги. Потребителските привилегии се одитират периодично, за да се осигури тяхната актуалност. Неизползваните (обездвижени) акаунти се закриват .

8.2.2 Отдалечен достъп

Въвеждат се контроли за управление на отдалечения достъп до ИТС на дружеството и съответните ключови данни в съответствие с изискванията за „Мобилна и отдалечена работа”.

8.2.3 Управление на привилегиите

Присвояването и използването на системни привилегии за всяка отделна компютърна платформа се ограничава и контролира на база „Контрол на достъпа и управление на акаунтите”.

8.2.4 Управление на паролите

Присвояването и използването на пароли се контролира в съответствие с изискванията за „Управление и използване на паролите”. В съгласие с горната процедура от потребителите се изисква да следват добрата практика при избора, ползването и управлението на техните пароли, както и да не оповестяват последните.

8.2.5 Оборудване без наблюдение

Потребителите на ИТС са отговорни за защитата на ключовите данни, като не оставят стационарните си компютри без наблюдение докато те са регистрирани в системата. При напускане на работното място за определен (макар и кратък) период от време потребителите са длъжни да прекратят своята сесия със съответната операционна/приложна система. Що се отнася до мобилното оборудване на тяхно разположение, то не трябва да бъде излагано на опасност от кражба. При офис-базираните системи, по възможност да се използват защитени с парола скрийн-

сейвъри и/или автоматични процедури за прекратяване на системните сесии, когато липсва трафик между клиента и системата.

8.3 Контрол на достъпа до мрежата

Ползването на мрежови услуги, свързаност към локална мрежа, както и на информационни системи, свързани с последната трябва да бъде в съответствие с изискванията за управление сигурността на мрежовия достъп.

8.4 Контрол на достъпа до операционни системи и приложения

Достъпът до операционните системи и приложния софтуер се контролира в съответствие с изискванията за контрол на достъпа и управление на акаунтите. Системни инструменти и обслужващи програми се съхраняват на места с повишена сигурност, като достъп до тях се позволява само на съответния обслужващ персонал, чиято длъжност предполага ползването им.

8.5. Анализ и документиране на изискванията за сигурност

ИТ звеното трябва да извършва оценка на риска, в съответствие с процедурата „Оценка на риска”, за да идентифицира изискванията по сигурността свързани със системите. В случай на закупуване на готови продукти задължително се преминава през процес на оценяване на контролите за сигурност, които те интегрират.

8.6. Обработка на данните

8.6.1 Проверка на входните данни

В процеса на работа трябва да се има предвид, че всички входни данни подлежат на контрол за автентичност и коректност на стойностите. За да се считат входните данни за валидни е необходимо като минимум да са изпълнени следните изисквания:

- потребителите, които подават входната информация да могат да бъдат идентифицирани;
- стойностите на входните полета да отговарят на очаквания тип (текст, цифри, дата и т.н.);
- чувствителните данни да не бъдат видими в чист вид, а маскирани;
- полетата, които са задължителни да бъдат попълнени;
- спазване на принципа на 4-те очи, съгласно приетата счетоводна методология.

8.6.2 Контрол на вътрешната обработка

Необходимо е спазването на установените изисквания за сигурност по отношение на обработката на данни с цел да се гарантира:

- цялост на данните в процеса на тяхното предаване през различни приложни интерфейси или комуникационни среди;
- наличен механизъм за възстановяване на старо копие на данни, които по погрешка са били редактирани
- контрол на процесите на обработка (механизъм за съпоставяне на данните преди обработка и след това);
- проверка на свързаните данни;
- наличие на процедура за валидиране на входните данни за всеки входен интерфейс;
- проверка за коректно изпълнение на автоматично стартирани процедури и елиминиране на възможността даден процес да продължи обработка в случай на възникване на грешка.

8.6.3 Контрол на изходните данни

Изходните данни следва да бъдат предоставяни според нивото на оторизация на съответния потребител, да бъдат достатъчни по смисъла на бизнес изискванията поставени към системата. Данните трябва да съдържат допълнителна информация, която да дава възможност на потребителя или следващата обработваща система да идентифицира случаи на некоректност, неточност, липси по отношение на данните и класификацията им.

8.6.4. Сигурност на системите, опериращи в реален режим

Изискванията за сигурността на всяка система, оперираща в реален режим следва да се съблюдават с особено внимание. По отношение на системните файлове трябва да се спазват следните изисквания:

- служителите от „Информационни технологии“ са отговорни за инсталиране на софтуера;
- разработчиците на системата нямат достъп за запис до нея;
- всички фази на пускане на системата в реален режим следва да бъдат документирани;

- преди влизане в експлоатация в реален режим се прави проверка за актуалност на наличната документация;

- преди влизане в експлоатация на нова версия на информационна система, потребителите ѝ следва да получат необходимия предварителен инструктаж за работа с промененото приложение.

9. Управление на инциденти

Всички събития, които ще се третират като „инциденти по сигурността” трябва да бъдат предварително дефинирани. Създават се също съответни инструкции, формализиращи процесите на разследване, контрол, управление и анализ на горните инциденти.

Всички явни или предполагаеми инциденти по сигурността се докладват на звена ИТ и Сигурност.

На компютри/устройства, участници в инциденти по сигурността извън мрежата се блокира мрежовия достъп и/или този до Интернет. Последващо възстановяване на достъпа се извършва само след като бъдат приложени съответните коригиращи мерки.

Всеки компютър/устройство, подлагащи на риск целостта на корпоративната мрежа се изключва от последната. Последващо възстановяване може да се предприеме само след като бъдат удовлетворени изискванията по горната инструкция.

10. Непрекъсваемост на бизнеса

Цел: „Дис Трейдинг ООД” подхожда с изключително внимание към въпросите, които касаят подsigуряване на информационните системи, така че да се гарантира непрекъсваемост на бизнес процеси на дружеството. Цел на дружеството е да разполага с информационни ресурси, които да му позволяват да функционира с максимално качество при оптимални времеви условия, имайки предвид широкия спектър на възможностите за възникване на технически проблеми, както и да минимизира всяка пряка или непряка щета, която би причинила нарушението на някой от бизнес процесите. В процеса на планирането с цел осигуряване на непрекъсваемостта на бизнеса се дефинират задачи по отношение на критичните процеси в дружеството, чието изпълнение следва да бъде гарантирано във времето и гарантиране на минимално време за прекъсване в случай на извънредни ситуации.

10.1 Бизнес анализ и оценка на риска

Бизнес анализът и оценката на риска се осъществяват в съответствие с процедурите „Оценка на риска” и „Непрекъсваемост на бизнес процесите” и с участието на собствениците на бизнес

ресурсите и процесите в дружеството. Оценката следва да обхваща всички бизнес процеси, а не само онези, които са свързани с информационните системи.

10.2. Стратегия и План за непрекъсваемост на бизнеса

На базата на оценката на риска и процедурата „Непрекъсваемост на бизнес процесите” се изготвят и поддържат „Стратегия за непрекъсваемост на бизнеса“, и „План за непрекъсваемост на бизнеса“. В процеса задължително участват всички бизнес звена според компетенциите си. Планът за непрекъсваемост на бизнеса и за действие в кризисни ситуации се одобрява от Управителя и се свежда до знанието на всички отговорни служители.

10.3 Тестване на плана за непрекъсваемост на бизнеса

Целите на тестовете са:

- да оценят адекватността му;
- да идентифицират пропуски;
- да идентифицират „тесните“ места в целия процес;
- да се прецени каква е вероятността за възникване на дефекти;
- да се изгради практика в служителите.

Целият „План за непрекъсваемост на бизнеса“ следва да се тества поне веднъж в годината. Периодът за тестване на всяка от процедурите за възстановяване се дефинира в самия план. Отговорност за провеждане на периодичното тестване на плана носи директора на дирекция ръководител „Информационни технологии“.

10.4 Съхранение на данните

Ключови данни не се съхраняват само на едно единствено място. В идеалния случай те се намират върху мрежов ресурс, така че да може да се копират/архивират с помощта на програмно-управляем процес. Където това не е възможно, данните трябва да бъдат обезпечени чрез регулярен backup процес в съответствие с процедурите „Непрекъсваемост на бизнес-процесите” и „Класификация и защита на информацията”. Носителите на backup-копията трябва да се съхраняват извън сградата на достатъчно разстояние от оригинала, така че да останат невредими в случай на сериозен инцидент или природно бедствие сполетели продукционната система.

10.5 Носители на backup-данни

Трябва да се прилага стриктно контролиран и напълно проследим процес за операции с горните носители. Това важи и за транспортирането и съхранението им, а също така и за възстановяването на информация, ползвайки тези носители, особено когато става въпрос за ключови данни .

11. Публикуване на политиките за сигурност

Политиката за информационна сигурност на дружеството подлежат на оповестяване. Служителите на дружеството следва да познават установените политики за сигурност. Специализирана служба „Вътрешен контрол” на дружеството, следва да извършва проверки дали служителите познават установените политики за информационна сигурност, като част от контрола на тези системи.

Дефиниции

Политика: цялостна позиция по организация и управление, формално изразена от ръководството на дружеството

Актив: всеки материален елемент, който има стойност за дружеството;

Данни: форма на представяне на информацията;

Информационна сигурност: защита на конфиденциалността, целостта и наличността на информацията;

Конфиденциалност: осигуряване на достъп до информация единствено и само на лица, които са изрично упълномощени да я ползват;

Цялост: характеристика на информацията, която указва, че тя е била модифицирана или е модифицирана само от упълномощени за това лица;

Наличност: свойство на информацията, което показва, че тя е достъпна за използване от упълномощените лица винаги, когато това е необходимо;

Автентичност: всяка информация се счита за автентична, ако нейният автор и фактът, че тя не е променяна от създаването си могат да бъдат категорично установени;

Заплаха: потенциална причина за инцидент, който може да доведе до щети за дружеството;

Уязвимост: слабост в актив или група от активи, които могат да станат предмет на заплаха;

Събитие, свързано с информационната сигурност: идентифицирана ситуация възникнала в следствие на нарушаване на Политиката за информационна сигурност, отпадане на контрол или неизвестно до момента събитие, което може да има връзка с информационната сигурност;

Инцидент: единично или серия от нежелани и неочаквани събития, които с голяма вероятност компрометират бизнес процесите и заплашват информационната сигурност;

Риск: комбинация от вероятността дадено събитие свързано с информационната сигурност да се случи и последиците от него;

Анализ на риска: систематично проучване с цел да се определят източниците на риск и да се оцени неговия размер;

Оценка на риска: цялостния процес по анализ на риска и идентифициране на неговите размери;

Контрол: всяко административно или техническо средство, което служи за минимизиране на някакъв вид риск;

Информационна система: комбинация от хардуер и софтуер, която има способност да обработва, предава, съхранява и т.н. данни;

Хардуер : физическите компоненти на информационните системи;

Софтуер: логическите компоненти на една информационна система;

Приложна система: програма, разработена със специална цел, която използва хардуерните възможности и възможностите на операционната система;

Потребител: лице, което е упълномощено с достъп до една или повече информационни системи с цел да изпълнява задълженията си;

Мрежа: връзка между два или повече компютъра с цел осигуряване на обмена на информация между отдалечените точки;

Защитна стена: компютърна технология (хардуерна и/или софтуерна), която физически и логически разделя една мрежа от друга и филтрира трафика между тях по определени правила;

Криптография: наука, чийто предмет са различните алгоритми, които стоят в основата на методите за осигуряване на конфиденциалността и автентичността на информацията в процеса на

предаването и/или съхранение;

Зловреден код: програма, която извършва нелегални операции без знанието на потребителя и която използва компютърните ресурси за да се само-възпроизвежда и/или разпространява;

Принцип на четирите очи: контролен механизъм, който изисква двама души за одобрение на дадено действие;

Разделяне на функциите: ограничителен достъп за осъществяване на специфични действия в някоя от банковите системи от страна на отделни звена - бизнес, риск, функционални;

ИТС: Информационни технологии и системи;

Субекти: Всички физически или юридически лица, имащи отношение към или попадащи в обсега на Политиката. В това число:

- Целият личен състав на дружеството (независимо от вида на трудовия договор);
- Трети страни;
- Всички други индивиди и/или групи, на които е гарантиран достъп до ИТС на дружеството;

Ключови данни: Данни, критични за функционирането на дружеството, чувствителни данни или такива, които дружеството е задължено от закона да поддържа, както и всички други данни, можещи да навредят на дружеството в случай, че бъдат откраднати или компрометирани;

Критични системи: Информационни системи, обработващи ключови данни;

Чувствителност: Мярка за важност, присвоявана на информацията за да се укаже нейната степен на поверителност;

Трети страни: Физически или юридически лица, обвързани с договорни отношения с Дис Трейдинг ООД с цел да извършването на услуги или други дейности в полза на дружеството;