**ОДОБРЯВАМ:**

**ИВАН МАРКОВ  
ГЛАВЕН СЕКРЕТАР НА   
МИНИСТЕРСТВО НА ТРАНСПОРТА, ИНФОРМАЦИОННИТЕ ТЕХНОЛОГИИ И СЪОБЩЕНИЯТА**

**ПОЛИТИКА ЗА СИСТЕМНО АДМИНИСТРИРАНЕ**

**И СИГУРНОСТ НА СЪРВЪРИ, ПЕРСОНАЛНИ КОМПЮТРИ И ЛОКАЛНА МРЕЖА,   
 ИЗПОЛЗВАНИ В МИНИСТЕРСТВО НА ТРАНСПОРТА, ИНФОРМАЦИОННИТЕ ТЕХНОЛОГИИ И СЪОБЩЕНИЯТА**

**Този документ е създаден съгласно настоящите възможности за информационно обслужване в Министерство на транспорта, информационните технологии и съобщенията и съгласно изискванията на клиентите. Той ще бъде актуализиран в зависимост от тенденциите за развитие и подобренията в областта на информационните технологии. Всички необходими промени ще бъдат осигурени от Дирекция Информационно обслужване и одобрени от Министъра на Транспорта.**

**Съдържание:**

[Въведение 4](#_Toc309044788)

[Управление на пароли. 5](#_Toc309044789)

[Управление на пароли на сървър. 5](#_Toc309044790)

[Управление на пароли на работна станция. 5](#_Toc309044791)

[Политика за предпазване от електронни вируси. 6](#_Toc309044792)

[Процедури за достъп, защита и използване на мрежата. 6](#_Toc309044793)

[Firewall. 6](#_Toc309044794)

[Достъп до Internet и Intranet. 7](#_Toc309044795)

[Електронна поща. 7](#_Toc309044796)

[Права на достъп до мрежови ресурси. 7](#_Toc309044797)

[Мерки, използвани за осигуряване на защита на счетоводна информация. 7](#_Toc309044798)

[Физическа сигурност. 8](#_Toc309044799)

[Физически достъп до сървърите. 8](#_Toc309044800)

[Физически достъп до работни станции. 8](#_Toc309044801)

[Използван софтуер. 8](#_Toc309044802)

[Съхранение на данни. 9](#_Toc309044803)

[Съхранение на данни на потребителите в папки на сървър. 9](#_Toc309044804)

[Съхранение на данни в обща директория. 9](#_Toc309044805)

[Непрекъсваемост на информационният процес и План за възстановяване в бедствени ситуации. 11](#_Toc309044806)

[Обща част. 11](#_Toc309044807)

[Критични ресурси. 11](#_Toc309044808)

[Необходимост от създаване на back-up и архивни файлове. 11](#_Toc309044809)

[Процедури за създаване на back-up, архив и възстановяване. 11](#_Toc309044810)

[Процедура за създаване на back-up. 12](#_Toc309044811)

[Създаване на back-up на информацията, локализирана на файловите сървъри. 12](#_Toc309044812)

[Създаване на back-up на информация от критични приложения и бази данни. 13](#_Toc309044813)

[Създаване на back-up от служителите на информация създадена от тях във файлове или бази данни на работните станции. 13](#_Toc309044814)

[Процедура за архивиране на данни. 13](#_Toc309044815)

[Процедура за възстановяване на данни. 14](#_Toc309044816)

[Поради срив в някоя от системите, например в резултат на повреда на твърдия диск/дискове, дисков контролер или друг системен компонент: 14](#_Toc309044817)

[Поради невнимание при работа с данните от страна на потребителя: 14](#_Toc309044818)

[Процедури за решаване на проблеми възникнали в информационни и комуникационни системи. 15](#_Toc309044819)

[Проблеми, свързани с услуги в мрежата. 15](#_Toc309044820)

[Проблеми, свързани с операционни системи на сървърите. 15](#_Toc309044821)

[Проблеми, свързани с комуникации в LAN. 16](#_Toc309044822)

[Проблеми, свързани с комуникации с външни мрежи. 16](#_Toc309044823)

[Проблеми, свързани с услуга или група услуги. 16](#_Toc309044824)

[Хардуерни проблеми. 16](#_Toc309044825)

[Дейности и критични ситуации причинени от бедствия и аварии. 17](#_Toc309044826)

[Основни положения. 17](#_Toc309044827)

[Стратегия за непрекъсваемост на информационните процеси. 17](#_Toc309044828)

[Описание на реализирания Disaster Recovery Center 18](#_Toc309044829)

[Известяване на екипът за възстановяване. 18](#_Toc309044830)

[Класификация на събитията. 19](#_Toc309044831)

[Първо ниво – локален проблем 19](#_Toc309044832)

[Второ ниво – проблеми с помещението на сървърите и/или основната сграда на МТИТС. 20](#_Toc309044833)

[Ресурси и дейности необходими за прилагането на Плана за непрекъснатост на информационните процеси 20](#_Toc309044834)

[Процедури за възстановяване на информационни процеси в случай на извънредна ситуация. 20](#_Toc309044835)

[Процедура за възобновяване на достъпа до файловите ресурси. 21](#_Toc309044836)

[Процедура за възобновяване на достъпа до електронна поща и Интернет портал 22](#_Toc309044837)

[Процедура за възобновяване на достъпа до информационната система за документооборот 24](#_Toc309044838)

# Въведение

Преди нов служител или външен потребител, който временно ще използва данни от локалната мрежа / одитор, служител от Камарата на счетоводителите, консултант и др./ да започне работа в Министерство на транспорта, информационните технологии и съобщенията, той трябва надлежно да бъде запознат със следната документация:

* Вътрешни правила за информационно осигуряване на потребителите в Министерство на транспорта, информационните технологии и съобщенията

Първоначални инструкции за употреба на оборудването, услугите и ресурсите се дават от представител на Дирекция Информационно обслужване. В случай на промяна на политиката за сигурност или промяна в ИТ инфраструктурата, потребителите ще бъдат уведомени своевременно от системните администратори.

Всеки потребител притежава профил - "акаунт" (валидно потребителско име и парола), чрез който се идентифицира в локалната мрежа на Министерство на транспорта, информационните технологии и съобщенията. Изискванията за сигурност на мрежата /предпазване от външни атаки, поддържане на firewall, създаване на потребителски профили, контрол на достъп до сървъри, инсталация на приложни програми, хардуерна поддръжка и др./ са от компетенцията и са отговорност на Дирекция Информационно обслужване.

Инсталацията и администрацията на софтуер закупен от други дирекции е под компетенцията на представителите на Дирекция Информационно обслужване. Инсталацията и администрацията на софтуер закупен от други дирекции могат да бъдат направени след писмена заповед от Главния Секретар до експертите от Дирекция Информационно обслужване. Заповедта трябва да бъде придружена от конкретни инструкции, описващи в детайли стъпките за инсталиране и администриране на софтуера, както и данни за контакт с представител, който може да осигури информация за софтуера в писмена форма.

Представителите на Дирекция Информационно обслужване могат да предлагат прилагането на нови мрежови услуги и приложения, и определен софтуер, както и подобряването на вече съществуващи мрежови услуги и приложения ако установят необходимост или имат възможност да подобрят работния процес. В този случай екипът трябва да подготви проект за изграждане, внедряване и подобрение на мрежовите услуги и приложения, в който е необходимо да бъдат засегнати следните въпроси:

* Описание на мрежовите услуги и приложения
* Причини, породили необходимостта от внедряването на нови услуги или за подобряването на вече съществуващи такива
* Предполагаеми срокове за изпълнение
* План за вероятните разходи, свързани с внедряването
* Специалистите отговорни за реализацията на проекта

1. Предложението трябва да бъде представено на Главния секретар.

2. Ако предложението бъде одобрено се стартира внедряването на услугите.

3. След приключване на внедряването на новата мрежова услуга или софтуер е необходимо да бъде изготвен доклад до Главния секретар.

**Процедура за системна сигурност и съхранение на данни.**

## Управление на пароли.

Изискванията за парола са наложени от т.н. Групова политика в Active Directory домейн.

### Управление на пароли на сървър.

Изисквания към паролите за работа със сървър

1. Паролата трябва да бъде с дължина най-малко от 9 символа.
2. Трябва да съдържа най-малко 2 букви, най-малко 2 цифри и най-малко 1 специален символ.
3. Не трябва да съдържа често използвани или лесни за отгатване думи като имена на приложения, системен софтуер или лична информация на системния администратор.
4. Трябва да бъде променяна всеки месец от системния администратор. (Валидност на паролата)

Настройка, промяна и съхранение на системните пароли

1. Настройката на нова системна парола трябва да бъде направена по време на инсталацията и конфигурирането на системния софтуер на сървъра – операционна система, мрежов софтуер, Data Base Control System или други сървърни приложения.
2. Забранено е публичното разгласяване на паролата или предоставянето й на други лица.
3. Системните пароли трябва да бъдат съхранени на 2 хартиени копия:

* в хартиен плик, който трябва да бъде поставен в метален сейф в архив на 5 етаж
* в хартиен плик, който трябва да бъде поставен в метален сейф, съхраняват от Директора на Дирекция Информационно обслужване

1. В случай на отсъствие на системния администратор или спешна необходимост от намеса, ръководителя на отдела може да даде разрешение за използването на системната парола. Ако Ръководителят на отдела отсъства, разрешение издава Директора на Дирекция Информационно обслужване или оторизирано от него лице.

### Управление на пароли на работна станция.

Потребителят трябва да използва предоставения му персонален компютър, периферни устройства и софтуер, съгласно предназначението им.

Изисквания към паролите за работа с работни станции

1. Паролата трябва да съдържа най-малко 5 символа и най-малко 2 цифри. Паролата не трябва да съдържа информация, свързана директно с потребителя /собствено име, фамилия, рожден ден и т.н./
2. Забранено е потребителя да предоставя потребителското си име и паролата на други служители или на неоторизирани лица.

Настройка, промяна и съхранение на системните пароли

1. След първоначалното зареждане на профила си, потребителя трябва да смени паролата си за достъп.
2. Потребителя трябва да сменя паролата си за достъп на всеки 6 месеца. (Валидност на паролата)
3. Забранено е да се използва парола идентична с някоя от последните 3 използвани от потребителя.

В случай на съмнителни събития, предполагащи разкриването на паролата от други лица, тя трябва да бъде променена незабавно, а експертите от Дирекция Информационно обслужване да бъдат уведомени.

## Политика за предпазване от електронни вируси.

Антивирусният софтуер се инсталира от системен администратор или експерт от Help Desk на всяка машина в Министерство на транспорта, информационните технологии и съобщенията, съгласно стандартната конфигурация на ИТ профилите. Пощенския и файловият сървър също са защитени от инсталиран антивирусен софтуер. Системният администратор уведомява потребителите за опасност от вируси чрез електронна поща.

Потребителите в локалната мрежа са длъжни да извършват проверка на всяко електронно съобщение, архивиращи медии и др. преди тяхното отваряне или копиране. В случай на индикация или съмнение за съществуването на инфектирани файлове, потребителите на локалната мрежа са длъжни да информират Дирекция Информационно обслужване. Служителите на Дирекцията са отговорни за обучението на потребителите в Министерство на транспорта, информационните технологии и съобщенията за проверка и предпазване от вируси.

Времеви интервали за актуализация на антивирусен софтуер:

* Работна станция – веднъж на всеки 3 часа.
* Пощенския и файлов сървър – веднъж на всеки 2 часа.

## Процедури за достъп, защита и използване на мрежата.

### Firewall.

Защитата чрез Firewall е внедрена в локалната мрежа на Министерството срещу неоторизиран достъп чрез Internet и националната ATM мрежа на Държавната администрация. Тази защита е конфигурирана така, че да осигури пълен достъп до почти всички Internet приложения и услуги, избрани от потребители от локалната мрежа на Министерство на транспорта, информационните технологии и съобщенията, но забранявайки достъп на външни потребители до ресурсите на локалната мрежа.

Защитата с Firewall е реализирана чрез Juniper Networks NetScreen-25, в която са интегрирани многобройни функции за сигурност – Stateful and Deep Inspection Firewall, IPSec VPN, антивирус и Web filtering.

### Достъп до Internet и Intranet.

Изходящият трафик до всички услуги е разрешен. Поради тази причина Firewall подсистемата, действаща на потребителските работни станции трябва да бъде допълнение към мерките за антивирусна защита и защита от външен достъп.

### Електронна поща.

Електронната поща се доставя до потребителя, чрез SMTP/POP3 протоколи. POP3 клиентите съхраняват получените електронни съобщения на Exchange server и в локалната пощенска кутия.

Антивирусният модул се стартира на пощенския сървър. Изходящите и входящите електронни съобщения се проверяват за вируси ако не са криптирани. Не съществува забрана за тяхното съдържание.

Antispam защитата се осигурява от antispam и антивирус софтуер Symantec Brightmail AntiSpam, който защитава от spam, вируси разпространени чрез електронна поща и др.

### Права на достъп до мрежови ресурси.

Мрежовият достъп до файлове и принтер ресурси са възможни благодарение на Microsoft file/print sharing. Всички потребители в Министерството са включени в домейн управляван от Активна Директория. Достъпът до всички ресурси се контролира от Активната Директория. Профилите на потребителите са защитени чрез парола и съответно достъпа до ресурсите е контролиран.

Файловите пространства са разделени на общи, групови и персонални. Достъпът до груповите пространства се извършва в зависимост от принадлежността на административната единица. Допълнителни права за достъп се формират след изискване на съответен ръководител. Вътрешен документ на Дирекция Информационно обслужване предоставя повече информация, касаеща този въпрос.

SAP притежава софтуерен инструмент за контрол на достъп.

## Мерки, използвани за осигуряване на защита на счетоводна информация.

Следните мерки за сигурност са използвани, за да се осигури протекция и цялостност на счетоводната информация в електронен вид:

|  |  |  |
| --- | --- | --- |
| **Предмет на контрол** | | **Предвидена мярка** |
| 1. Защита срещу неоторизиран достъп. | | Индивидуални пароли на потребителите, защитен екран с уникални пароли. |
| 2. Защита срещу неоторизирани промени /изтриване, добавяне, модификация на данни/ | | Наличие на файл с информация за извършен достъп до системата /logs/ и възможност за независимо разглеждане на този файл, предотвратяване на последващи промени чрез изискване на коригирани входящи данни ако е необходимо, не се позволява корекция на данни от предходни влизания |
| 3. Защита срещу външни атаки. | | Firewall и др. |
| 4. Предпазване от загуба на данни. | Регулярни /седмични/ back-up процедури, архивиращи устройства за реализиране на back-up, локализирани извън счетоводен отдел. Съхранение на направените архиви на сигурно място извън счетоводен отдел. |

## Физическа сигурност.

### Физически достъп до сървърите.

Физическият достъп до сървърите е ограничен. Само следните длъжностни лица имат право на достъп до помещенията със сървърите:

1. Министърът на Транспорта.
2. Главният Секретар.
3. Директорът на Дирекция Информационно обслужване.
4. Служители и системни администратори от Дирекция Информационно обслужване.
5. Служители, отговорни за поддръжката на оборудването, съгласно сключен договор за поддръжка.

Когато други служители на Министерство на транспорта, информационните технологии и съобщенията /електротехници, специалисти структурно окабеляване, телекомуникационни специалисти, работници по поддръжка и т.н./ трябва да влязат, за да изпълнят регулярни или обичайни задължения, трябва да получат разрешение от Директора на Дирекцията или от Главния Секретар.

Защитен екран, изискващ парола се активира при наличие на 10 минути без активност на мястото за контрол и/или администриране.

### Физически достъп до работни станции.

* Забранено е на потребителите да предоставят достъп на неоторизирани лица до работните им станции.
* Защитен екран, изискващ парола се активира при наличие на 20 минути без активност на работната станция.
* Преди да напусне работното място служителят трябва да заключи мрежовата сесия /чрез избиране на комбинацията от клавиши Ctrl+Alt+Del, избор на функция Lock computer (WorkStation)/ и в края на деня /преди напускане на работното място/ потребителя трябва да използва функцията Log Off.

## Използван софтуер.

Използват се различни софтуерни пакети - за счетоводство, въвеждане и извеждане на данни, за целите на Дирекция Информационно обслужване, специфични софтуерни продукти и т.н.

Въведените мерки за сигурност, осигуряват защита на информацията в електронна форма в зависимост от използвания софтуер. Мерките за сигурност са както следва:

* Персонални пароли за достъп на потребителите
* Използване на индивидуални Log in имена за достъп до софтуер и независим преглед на дневниковите файлове , предотвратяване на последващи промени, чрез изискване на коригирани входящи данни ако е необходимо, не позволява корекция на предишни данни за достъп

# Съхранение на данни.

## Съхранение на данни на потребителите в папки на сървър.

* Потребителите трябва да съхраняват всички документи, свързани с тяхната работа на мрежов сървър в създадена персонална директория (\\motdom\mt\home\\<User’s name>), за да бъде предотвратена загуба на данни.
* Потребителите от ИА ИСПА трябва да съхраняват всички документи, свързани със служебните им задължения на мрежов сървър в създадена персонална директория (\\motdom\mt\home\<User’s name>, за да бъде предотвратена загуба на данни.
* Всички документи и бази данни трябва да бъдат съхранявани на файлов сървър на Министерство на транспорта, информационните технологии и съобщенията. Ако потребител не може да съхранява информацията си на сървър /например софтуер, свързан с управлението на база данни не поддържа архивирането на създадени с него файлове на сървър/, трябва задължително да се изпълняват регулярни back-up процедури. Подобно архивиране трябва да бъде извършвано всяка седмица /в петък/ в специална директория на сървъра (\\motdom\mt\home\<User’s name>) или (\\motdom\mt\ISPA\users\<User’s name>)
* Ако съществува повече от един потребител, който има нужда от оторизиран достъп до документи/данни, те могат да бъдат изпращани чрез електронна поща, преносими дискове, хартиени носители и др.

## Съхранение на данни в обща директория.

По правило всички документи трябва да бъдат съхранявани в персонални папки на потребителите на сървъра. Общи директории трябва да бъдат използвани само в следните случаи:

* Когато е необходимо повече от един служител да работи със съответните документи
* Когато документите не са класифицирани като секретни и са информативни за останалите служители.

Във всички останали случаи е задължително да се използват персонални директории.

Ако част от служителите образуват Подгрупа с достъп до определени документи/данни, останалите потребители на главната Група не трябва да имат достъп до техните документи.

Всеки път, когато директорията на общата Група се използва от потребител, той трябва да се идентифицира.

Правото на достъп на потребителите може да бъде разделено на 3 степени:

1. Потребители, които нямат право на достъп до документите.
2. Потребители, които могат да четат, но не могат да променят документите.
3. Потребители, които могат да четат и да променят документите.

По правило всички публични документи трябва да бъдат поставени в папки, в които потребителите са с достъп от 2ра степен. За документи, класифицирани като секретни, всички потребители извън Подгрупата са с достъп от 1-ва степен. Правата за достъп до документите в Подгрупа трябва да бъдат дефинирани съгласно потребителите.

* Потребителите от Министерство на транспорта, информационните технологии и съобщенията ще използват за обмяна на данни, за информация и оперативна работа на сървъра директория (\\motdom\mt\Public\<User’s name>)
* Потребителите в ИА ИСПА ще използват за обмяна на данни, за информация и оперативна работа на сървъра директория (\\motdom\mt\ISPA\Public\<User’s name>)

# Непрекъсваемост на информационният процес и План за възстановяване в бедствени ситуации.

## Обща част.

Непрекъсваемостта на информационният процес и планирането й са определящи при възстановяване след аварийни ситуации. Степента, в която е ефективен планът варира в зависимост от характера на ситуацията.

## Критични ресурси.

Като критични точки в Министерство на транспорта, информационните технологии и съобщенията се определят следните приложения:

* Ajur5L
* Eventis R6
* Lotus Notes
* Софтуер за регистриране присъствие в МТИТС - Card Access
* Двата web сървъра (internet портал и intranet)

Като критични точки в ИА ИСПА на Министерство на транспорта, информационните технологии и съобщенията се определят следните приложения:

* Данните изготвяни и използвани в ИА ИСПА в електронен формат
* Хардуерът използван за съответното изпълнение на задачите в ИА ИСПА /работни станции, LAN, сървъри и т.н./

### Необходимост от създаване на back-up и архивни файлове.

За да се избегне каквато и да е загуба на информация и прекъсване на нормалния работен процес на цялото Министерство на транспорта, информационните технологии и съобщенията е необходимо да бъдат създавани back-up и архивни масиви на генерираната информация. Back-up файловете се използват за възстановяване на информация, загубена поради срив в системата или невнимание от страна на потребителите. Back-up файловете се създават за съхраняване на информация на сървърите, реализирано чрез огледални дискове, както и на информация на твърдите дискове на персоналните компютри на потребителите. Архивите се създават дневно, седмично или месечно в зависимост от ресурсите, предмет на архивиране.

## Процедури за създаване на back-up, архив и възстановяване.

Тези процедури се изпълняват от Системните администратори.

Носителите използвани за архивиране и създаване на back-up трябва да се съхраняват в металeн сейф в архивна стая на 13 етаж.

**Речник**

|  |  |
| --- | --- |
| Back-up | Дейност, свързана със създаването на копие на информацията, целяща оперативно възстановяване в случай на срив в системата |
| Archive | Дейност, свързана със създаването на копие на информацията, целяща дългосрочното й съхранение, съгласно изискванията на Министерство на транспорта, информационните технологии и съобщенията и другите държавни институции |
| Restore | Дейност, свързана с възстановяване на информация, на базата на по-рано създадени back-up копия |

### Процедура за създаване на back-up.

Тази процедура регулира действията, свързани със създаването и съхраняването на back-up на информацията в електронен вид (на сървърите) на Министерство на транспорта, информационните технологии и съобщенията, което ще възстанови дейността без загуба на данни, в случай на техническа повреда в хардуера, системния софтуер или при умишлено или неумишлено изтриване на данни.

|  |  |
| --- | --- |
| **Сървър** | **Вид на back-up информацията** |
| MTDC01 | Файлов сървър |
| MTFP01 | Файлов сървър, Postgres Database |
| MTWF01 | Lotus Domino server |
| MTDC02 | Файлов сървър, MS Exchange 2003 Server |

#### Създаване на back-up на информацията, локализирана на файловите сървъри.

* Всеки последен работен ден от седмицата, след приключване на работното време се извършва пълен back-up на информацията, намираща се на сървърите в стая 506 в Министерство на транспорта, информационните технологии и съобщенията;
* При необходимост от генерални промени на файловите сървъри – основна реконструкция на информация (промяна на местоположение на основни директории), преинсталация /upgrade на софтуер, когато съществува риск от загуба на данни е задължително да се правят допълнителни back-up операции.
* Архивиращите лентови устройства, използвани за създаването на back-up трябва да са с капацитет от над 200GB.
* Така направените back-up копия трябва да бъдат преместени и съхранени на подходящо огнеупорно място в стая, определена специално за тази цел в Министерство на транспорта, информационните технологии и съобщенията, различна от стаята, в която се помещават сървърите.
* Back-up копията се съхраняват не по-малко от 3 седмици след датата на тяхното създаване.
* Пълното архивиране извършено през четвъртата седмица се прави върху медията от първата седмица и т.н.
* Всички архивни носители трябва да бъдат прилежно надписани с етикети.

#### Създаване на back-up на информация от критични приложения и бази данни.

* Всеки последен работен ден от месеца се извършва автоматично пълно архивиране на системните файлове, базите от данни и критичните приложения, инсталирани на сървърите в стая 506 в Министерство на транспорта, информационните технологии и съобщенията.
* Всеки ден, в края на работното време, трябва да бъде направен back-up на новосъздадената информация (incremental backup), следващ за последно създадения – пълен или incremental.
* Back-up копия на данните използващи LOTUS Domino Server, Postgres Server трябва да се създават съгласно следната процедура:
  + Базите от данни трябва да бъдат съхранени във файлове, използвайки вътрешните процедури за архивиране на съответната база данни.
  + Получените файлове трябва да бъдат съхранени върху магнитен носител, следвайки процедурата за съхранение
* Back-up копията трябва да бъдат съхранявани един месец след датата на тяхното създаване. Трябва да се пазят заедно пълния back-up и приложени шест incremental back-up файла.
* Файловете се архивират на външен магнитен носител (дискети, CD и др.)

#### Създаване на back-up от служителите на информация създадена от тях във файлове или бази данни на работните станции.

* Всеки служител, използващ специфична база данни и създаващ потребителски файлове е задължен да създава обикновен back-up на новосъздадените от него документи/ данни след приключване на работа. Тези back-up файлове се съхраняват на сървъра (процедурата е описана в точка 3) и на външни магнитни носители (дискети, CD, когато работната станция позволява запис със CD-RW, и др.)
* В случай на необходимост от основна промяна на компютърната конфигурация или софтуер – преинсталация/ upgrade или съществува риск от загуба на информация се правят допълнителни back-up файлове.
* Така създадените Back-up файлове се съхраняват най-малко един месец след тяхното създаване.
* Магнитните носители е задължително да бъдат надписани като бъдат обозначени данни за вида на информацията, която е записана на тях и датата на създаването на back-up.

### Процедура за архивиране на данни.

Ако е необходимо да бъде извършено еднократно архивиране за дългосрочен период от време е в сила следната процедура:

* за архивиране на информация по-малка от 700MB трябва да бъде използван диск CD-R
* за архивиране на информация с размер по-голям от 700MB – 4.5 GB трябва да бъде използван диск DVD
* за архивиране на информация по-голяма от 4.5GB трябва да бъде използвано лентово архивиращо устройство

Всички архивни носители трябва да бъдат надписани. Етикетите трябва да съдържат следните атрибути:

* описание на съдържащата се информация
* дата на създаване на архива
* период на съхранение на архива
* име на служителят, който е изискал създаването на архива

Всички създадени архиви се регистрират в Архивен дневник с атрибутите на архива.

В случай на необходимост от регулярно архивиране на информация, например съгласно изискванията на Националния Архивен Фонд, се създават графици за архивиране, одобрени от Главния Секретар които съдържат следната информация:

* вид на информацията, която трябва да бъде архивирана
* периодичност на архивирането
* срок на съхранение на архивите
* място и условия за съхранение на архивите
* други

Носителите на back-up информация заедно с регистъра на архивите трябва да бъдат съхранявани в стая, определена от Министъра на Транспорта с контролиран достъп и обезопасена от бедствия и аварии /пожар, наводнения и др./.

### Процедура за възстановяване на данни.

Възстановяването на данни се извършва поради следните причини:

#### Поради срив в някоя от системите, например в резултат на повреда на твърдия диск/дискове, дисков контролер или друг системен компонент:

* Работната способност на системата се възстановява, използвайки back-up на операционната система и инсталираните приложения, или операционната система и необходимите приложения трябва да се преинсталират ако не могат да бъдат възстановени от back-up.
* Данните се възстановяват от последния back-up;
* Извършват се тестове за работната способност на системите;
* Възстановяването се регистрира в дневник на оператора, отразяващ: дата и час на възстановяването, системен администратор(и) извършил(и) възстановяването и резултати от тестването на системата.

#### Поради невнимание при работа с данните от страна на потребителя:

* Постъпва заявка от потребителя за възстановяване на данните. В случай на обща заявка (например възстановяване на директории на отдел или дирекция), заявката се прави от началника на съответното структурно звено като се описват действията довели до тази необходимост;
* Информацията се възстановява от последното копие, в което тя е актуална;
* Прави се проверка дали възстановените данни са актуални;
* Възстановяването на данните се регистрира в дневник на оператора, отразяващ следното: дата и час на възстановяването, системен администратор(и) извършил(и) възстановяването.

### Процедури за решаване на проблеми възникнали в информационни и комуникационни системи.

Процедурите се изпълняват от системните администратори и специални служители, отговарящи за поддръжката на оборудването в съответствие с договор за поддръжка.

#### Проблеми, свързани с услуги в мрежата.

Процедурата е както следва:

* Причината за прекъсване на услугата трябва да бъде установена;
* Проверява се дневника на събитията (Event Log) в сървъра, в който недействащата услуга е инсталирана;
* Проверяват се други журнални файлове (ако има такива), за да се намерят причините за проблема;
* Прави се опит да се отстрани причината за нефункционирането чрез:
* използване на личен опит и знания
* използване на знания съхранени в база данни
* търсене в мрежата (WEB)
* Ако е невъзможно да се възстанови работната способност на системата, се използва системният архив, само ако това не би нарушило работата на други мрежови услуги;
* Ако съществува причина за невъзможност да се възстанови работната способност на системата чрез архива, услугата се инсталира и конфигурира на друг сървър;
* Проблемът и извършените действия се описват.

#### Проблеми, свързани с операционни системи на сървърите.

Процедурата е както следва:

* Установява се причината за прекъсване на услугата;
* Проверява се дневника на събитията (Event Log) в сървъра, в който неопрериращата услуга е инсталирана;
* Проверяват се други журнални файлове (ако има такива), за да се намерят причините за проблема;
* Прави се опит да се отстрани причината за нефункционирането чрез:
* - използване на личен опит и знания
* - използване на знания съхранени в база данни
* - търсене в мрежата (WEB)
* Ако е невъзможно да се възстанови работната способност на операционната система, се използва системният архив само ако това не би нарушило работата на други мрежови услуги;
* Ако съществува причина за невъзможността да се възстанови работната способност на операционната система чрез архива, операционната система се преинсталира;
* Проблемът и извършените действия се описват.

#### Проблеми, свързани с комуникации в LAN.

Процедурата е както следва:

* Проблеми, свързани с изградената кабелна система - Structural Cable System (SCS);
* Проблемът се отнася на вниманието на фирмата - контрактор на SCS;
* Проблемът и предприетите действия се описват.
* Проблеми, свързани с активното мрежово оборудване - Active Network Equipment (ANE);
* Проблеми, свързани с конфигурацията на ANE – прави се преконфигурация;
* Хардуерни проблеми, свързани с ANE – сменя се с подобно устройство, след което повреденото устройство се преглежда в специализиран сервиз;
* Проблемът и извършените действия се описват.

#### Проблеми, свързани с комуникации с външни мрежи.

Процедурата е както следва:

* Проблеми, свързани с интернет трафик - проблемът се отнася на вниманието на системните администратори в Министерски съвет (МС);
* Проблеми, свързани с комуникационното оборудване - проблемът се отнася на вниманието на системните администратори в МС. Ако проблемът е от хардуерно естество, се отнася на вниманието на съответната служба (сервиз), след консултации с администраторите в МС.
* Проблемът и извършените действия се описват.

#### Проблеми, свързани с услуга или група услуги.

* Ако проблеми, свързани с услуга или група услуги, застрашава целостта на мрежата или правилното й функциониране, тези услуги се преустановяват до отстраняване на риска;
* Ако проблемите са причинени от потребител или група потребители, достъпът на този потребител или група потребители се прекъсва до отстраняване на риска;
* Проблемът и извършените действия се описват.

#### Хардуерни проблеми.

* Ако хардуерен проблем е свързан с компоненти и системи в гаранция – решаването на проблема се отнася на вниманието на фирмата за гаранционно обслужване;
* Ако хардуерен проблем е свързан с компоненти и системи след изтичане на гаранционния им срок – решаването на проблема се отнася на вниманието на съответната служба - сервиз;
* Проблемът и извършените действия се описват.

## Дейности и критични ситуации причинени от бедствия и аварии.

В случай на критични ситуации причинени от бедствия (пожар, наводнение и др.) в сградата на Министерство на транспорта, информационните технологии и съобщенията (МТИТС), следва да бъдат предприети мерки при спазване на съответните инструкции, правила и разпоредби в сила.

Критичните ситуации представени в този документ са свързани с:

* *Повреда на хардуера на сървърите и на работните станции;*
* *Повреда в работата на операционните системи;*
* *Прекъсване на главното електроподаване;*
* *Човешка намеса.*

които могат да доведат до загуба на данни и изваждане от строя на системата.

След решаване на проблема и осигуряване на достъп до информационните системи, се предприемат действия за възстановяване на тяхната работна способност.

### Основни положения.

При изготвянето на този план са направени следните предположения:

* Потребителите на информационните процеси са отговорни за спазването на този план;
* Back-up копията на цялостната информация се съхраняват на сигурно място, отделено от помещението, където се намира сървъра, за да се позволи навременното възстановяване при нужда;
* Служителите, които отговарят за прилагането на този план, разбират ролята си в изпълнението му и са способни да го изпълнят;
* Ръководството на МТИТС разбира и подкрепя действията по този план;
* Необходимото оборудване е налично и може да бъде използвано незабавно при нужда;

Копия от плана се съхраняват на местата, където той се изпълнява.

### Стратегия за непрекъсваемост на информационните процеси.

За да бъде осигурено непрекъсваемост на информационните процеси е избрана следната стратегия в рамките на този план:

**Трансфер на информационни процеси към сървърно помещение в сградата на „БДЖ” ЕАД намираща се на ул. Иван Вазов 3**

Този вариант се избира, когато се предполага, че извънредната ситуация е засегнала основната сграда на МТИТС и/или помещението, където се намира сървърите и никакви информационни услуги не могат да се осъществяват там. В този случай критичните информационни процеси се прехвърлят към сървърно помещение в сградата на „БДЖ” ЕАД намираща се на ул. Иван Вазов 3. Ключовите служители на МТИТС се инструктират и редовно се обучават, както са задължени да са на разположение за да участват в процеса на възстановяване.

#### Описание на реализирания Disaster Recovery Center

Disaster Recovery Center служи за резервиране на основните информационни услуги, необходими на Министерството на транспорта. Той представлява оборудване, инсталирано в 19-инчов комуникационен шкаф (rack), отделен само за тази цел. Шкафът се намира в сградата на БДЖ на ул. Иван Вазов 3. Резервирането на основните информационни услуги се изпълнява паралелно по два начина:

* Непрекъснат backup, реализиран по технологията Continuous data protection (CDP), съхраняващ текущо на резервните сървъри всяка промяна в данните на основните. Следят се данните в критичните приложения.
* Класически backup, реализиран на лентово устройство по определено разписание и схема.

В Disaster Recovery Center е инсталирано следното оборудване:

1. резервни сървъри за основните информационни услуги в МТИТС

Инсталирани са три резервни сървъра:

* + сървър за документооборот
  + файлов сървър
  + сървър за електронна поща

Всеки сървър има масив от 4 диска RAID 0+1 с обем 600 GB, което осигурява устойчивост срещу повреда на диск и много висока скорост на запис и четене. Предвидена е достатъчна процесорна мощност и оперативна памет за изпълнение на предвидените задачи.

1. надеждно резервирано захранване

Използвани са два UPS с мощност 1500VA/1000W с мощни допълнителни батерии (общо 4бр. 12V / 210Ah), осигуряващи между 15 и 20 часа автономна работа на центъра след прекъсване на ел. захранване.. Всеки от сървърите има по три захранващи блока и е свързан и към двата UPS. Това осигурява устойчивост срещу повреда на който и да е от компонентите на захранващата част.

1. комуникационна част

Мрежов комутатор (switch) 10/100/1000, към който са включени сървърите и оптичната линия до МТИТС Връзката със министерството на транспорта е осъществена по директна оптична линия.

### Известяване на екипът за възстановяване.

Тази част покрива следните стъпки от процеса: активиране на Плана за непрекъсваемост и известяване на членовете на възстановителния екип.

След като бъде информиран за възможно нарушение на работата, служителят веднага уведомява за това Главния секретар на МТИТС, който изпълнява ролята на координатор на Плана за непрекъсваемост. По възможност всички налични служители трябва да обсъдят заедно ситуацията и да постигнат съгласие при вземането на решение за това дали да активират тези процедури или да изчакат събирането на допълнителна информация, необходима за вземане на решение.

**Възстановителен екип в МТИТС**

| **Име** | **Длъжност** | **Телефон** | **Мобилен тел.** |
| --- | --- | --- | --- |
| Наталия Маникатова | Директор на дирекция „Информационно обслужване” | 9409766 |  |
| Галина Василева | Директор на дирекция „Координация на програми и проекти” | 9409421 |  |
| Юри Караманов | Главен специалист в дирекция „Информационно обслужване” | 9409695 |  |
| Стамен Хаджийски | Младши експерт в дирекция „Информационно обслужване” | 9409706 |  |
| Светлана Велкова | Главен специалист в дирекция „Информационно обслужване” | 9409856 |  |

Членовете на възстановителния екип следва да бъдат информирани и процедурата по възстановяването да започне. Ако някои от членовете на екипа не могат да бъдат уведомени своевременно, тогава се оставя съобщение на мобилния им телефон и той/тя е задължен(а) в момента, в който получи съобщението да се свърже с ръководителя на екипа или друг негов член, за да получи необходимата информация.

Всички членове на възстановителния екип следва да притежават копие от този план.

### Класификация на събитията.

Класификацията на събитията се извършва с цел да се избере стратегия, осигуряваща непрекъснатостта на информационните процеси в МТИТС. Събитията, които се класифицират са всички тези, които водят до прекъсване на информационните процеси в МТИТС. Те се категоризират въз основа на времето, необходимо за възстановяване на нормалното функциониране на информационните услуги в локалната мрежа на МТИТС.

#### Първо ниво – локален проблем

Това са събития, при които има прекъсване на информационните процеси в резултат на поява на локален проблем: хардуерен проблем, комуникационни проблеми, проблеми с електрозахранването и др., където пълното опериране може да бъде възстановено до 24 часа. На това ниво проблемите (подмяна на оборудване, превключване на захранването и др.) се отстраняват чрез прилагане на действията, описани в „Процедури за създаване на back-up, архивиране и възстановяване на данни”.

Проблемите от първо ниво не се разглеждат в този план.

#### Второ ниво – проблеми с помещението на сървърите и/или основната сграда на МТИТС.

Това са събития, при които проблемът не може да бъде разрешен на локално ниво или в рамките на един работен ден (пожар в помещението на сървъра, наводнение, заплаха от терористичен акт или др.). Това са събития, при които сградата на МТИТС не може да бъде използвана, например при земетресение, пожар, прекъсване на електрозахранването за повече от 24 часа и др. При събитие от това ниво, координаторът бива уведомен и се осъществява процедурата за активиране. След това се преминава към процедурите, описващи възстановяването на информационните услуги в помещенията на центъра за кризисно управление в МТИТС.

Процедурите, посочващи необходимите действия на второ ниво, са описани в точка 4.4.6.

### Ресурси и дейности необходими за прилагането на Плана за непрекъснатост на информационните процеси

Ресурсите и дейностите, които са жизнено важни за възстановяването на функционирането на информационните процеси в МТИТС са:

|  |  |  |
| --- | --- | --- |
| **Ресурси/дейности** | **Период (дата) за изпълнение/статус** | **Отговорен служител/длъжност** |
| Файлов Сървър | Пълна тревога | Юри Караманов  Стамен Хаджийски |
| Сървър за документооборот | Пълна тревога | Юри Караманов  Стамен Хаджийски |
| Комутатори | Пълна тревога | Юри Караманов  Стамен Хаджийски |
| \motdom\mt\ISPA\users |  | Юри Караманов |
| Електронна поща на служителите на дирекциите |  | Стамен Хаджийски |
| Ajur5L  Eventis R6  LotusNotes  Card Access  Интернет и интранет сайтове |  | Юри Караманов  Стамен Хаджийски  Светлана Велкова |

### Процедури за възстановяване на информационни процеси в случай на извънредна ситуация.

#### Процедура за възобновяване на достъпа до файловите ресурси.

**Събитие**:

* Невъзможност за опериране в основната сграда на МТИТС

**Оперативни предложения**:

* При ниво 2 – информационните процеси се прехвърлят към сървърно помещение в сградата на „БДЖ” ЕАД намираща се на ул. Иван Вазов 3.
* всички използвани network shares имат копия на двата сървъра, с еднакви имена и позволения.
* всеки от сървърите има две мрежови платки, от които едната е работна, а другата - резервна. Резервната платка се държи изключена от мрежата.
* всеки от сървърите е настроен с IP адреса и на другия, вписан на изключената платка

**Период за изпълнение на процедурата**:

* Неопределен

**Изпълняват се следните действия:**

|  | **Действие** | **Отговорен служител** | **Виж стр.** |
| --- | --- | --- | --- |
| 1 | Попълване на документ – Приложение 1 | Възстановителен екип | 26 |
| 2 | Класификация на събитията (виж т.4.4.4) | Възстановителен екип | 19 |
| 3 | Изпълнение на процедурите за активиране и уведомяване (виж т.4.4.3) | Възстановителен екип | 18 |
| 4 | Прилагане на процедура за възстановяване работата на информационните процеси в зависимост от нивото на проблема:  Второ ниво – в сървърно помещение в сградата на „БДЖ” ЕАД намираща се на ул. Иван Вазов 3.  Забележка 1: Описани са операции върху основния и резервния сървър. Ако основният е повреден, той се изключва, а операциите, предвидени върху него, се пропускат.  Забележка 2: Тази последователност разменя ролите на двата сървъра. Ако е необходимо да се върне началното положение, тя трябва да се повтори   * изключват се основните мрежови платки на сървърите * преименуват се двата сървъра, като всеки придобива името на другия * рестартират се двата сървъра * включват се резервните платки | Възстановителен екип |  |
| 5 | Докладване за извършените дейности | Възстановителен екип |  |
| 6 | Завършване на възстановителните дейности | Възстановителен екип |  |

**Важни компоненти, софтуер и хардуер:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Софтуер** | **Местонахождение** | **Лице за контакти** | **Телефон** |
| Server Windows 2003 | сървърно помещение в сградата на „БДЖ” ЕАД намираща се на ул. Иван Вазов 3 | Юри Караманов  Стамен Хаджийски | 9409695  9409706 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Хардуер** | **Местонахождение** | **Лице за контакти** | **Телефон** |
| Server x86; 2 GB RAM; 4х320 GB HDD; 10/100/1000 NIC | сървърно помещение в сградата на „БДЖ” ЕАД намираща се на ул. Иван Вазов 3 | Юри Караманов  Стамен Хаджийски | 9409695  9409706 |

#### Процедура за възобновяване на достъпа до електронна поща и Интернет портал

Тази част от плана описва процедурите, които се следват за възстановяване на работата на критични информационни процеси.

**Събитие**:

* Невъзможност за опериране в главната сграда на МТИТС

**Оперативни предложения**:

* Информационните процеси могат да се прехвърлят към сървърно помещение в сградата на „БДЖ” ЕАД намираща се на ул. Иван Вазов 3.
* По отношение на електронната поща
  + на резервния сървър се съхранява актуален архив на данните от основния и копие от всичките му настройки.
  + всеки от сървърите има две мрежови платки, от които едната е работна, а другата - резервна. Резервната платка се държи изключена от мрежата.
  + всеки от сървърите е настроен с IP адреса и на другия, вписан на изключената платка
  + на резервния сървър не е инсталиран Microsoft Exchange.
* По отношение на Интернет портал
  + на резервния файлов файлов сървър се съхранява актуален архив на данните, настройките и кода на Интернет портала
  + на резервния файлов сървър са инсталирани WWW, PHP и SQL сървърите, необходими за работата на Портала. Те се намират в неактивно състояние.

**Срок за изпълнение на процедурата**:

* Неопределен

**Изпълняват се следните действия:**

|  | **Действие** | **Отговорен служител** | **Виж стр.** |
| --- | --- | --- | --- |
| 1 | Попълване на документ – Приложение 1 | Възстановителен екип | 26 |
| 2 | Класификация на събитията (виж т.4.4.4) | Възстановителен екип | 19 |
| 3 | Изпълнение на процедурите за активиране и уведомяване (виж т.4.4.3) | Възстановителен екип | 18 |
| 4 | Прилагане на процедура за възстановяване работата на информационните процеси в зависимост от нивото на проблема:  Второ ниво – в сървърно помещение в сградата на „БДЖ” ЕАД намираща се на ул. Иван Вазов 3  За възстановяване на електронната поща   * изключват се основните мрежови платки на сървърите * инсталира се Microsoft Exchange на резервния сървър, с лиценза от основния * прилагат се съхранените настройки на Exchange * рестартира се резервния сървър * включва се резервната платка на резервния сървър   За възстановяване на Интернет портал   * активират се WWW, PHP и SQL на резервния файлов сървър * настройват се рутери, DNS и други мрежови компоненти, за да работи Интернет порталът от друг адрес в мрежата | Възстановителен екип |  |
| 5 | Докладване за извършените дейности | Възстановителен екип |  |
| 6 | Завършване на възстановителните дейности | Възстановителен екип |  |

**Важни компоненти, софтуер и хардуер**:

|  |  |  |  |
| --- | --- | --- | --- |
| **Софтуер** | **Местонахождение** | **Лице за контакти** | **Телефон** |
| Server Windows 2003  Web server, PHP и SQL server | сървърно помещение в сградата на „БДЖ” ЕАД намираща се на ул. Иван Вазов 3 | Юри Караманов  Стамен Хаджийски  Светлана Велкова | 9409695  9409706  9409856 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Хардуер** | **Местонахождение** | **Лице за контакти** | **Телефон** |
| Server x86; 4 GB RAM; 4х320 GB HDD - RAID 0+1; 10/100/1000 NIC | сървърно помещение в сградата на „БДЖ” ЕАД намираща се на ул. Иван Вазов 3 | Юри Караманов  Стамен Хаджийски | 9409695  9409706 |

Необходими ресурси:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ресурси** | **Брой** | **Срок** | **Местонахождение** | **Доставчик** |
| Хора | 3 | До 6 часа | сървърно помещение в сградата на „БДЖ” ЕАД намираща се на ул. Иван Вазов 3 | Министерство на транспорта, информационните технологии и съобщенията |
| Мобилни телефони | 2 |
| Преносими компютри | 2 |

#### Процедура за възобновяване на достъпа до информационната система за документооборот

Тази част от плана описва процедурите, които се следват за възстановяване на работата на критични информационни процеси.

**Събитие**:

* Невъзможност за опериране в главната сграда на МТИТС

**Оперативни предложения**:

* Информационните процеси могат да се прехвърлят към сървърно помещение в сградата на „БДЖ” ЕАД намираща се на ул. Иван Вазов 3.
* всички използвани бази данни имат реплики на двата сървъра, с еднакви имена.
* базите данни не са криптирани със средствата на Lotus Domino
* на всеки сървър (основен и резервен) има копие от ID файла и на другия сървър

**Срок за изпълнение на процедурата**:

* Неопределен

**Изпълняват се следните действия:**

|  | **Действие** | **Отговорен служител** | **Виж стр.** |
| --- | --- | --- | --- |
| 1 | Попълване на документ – Приложение 1 | Възстановителен екип | 26 |
| 2 | Класификация на събитията (виж т.4.4.4) | Възстановителен екип | 19 |
| 3 | Изпълнение на процедурите за активиране и уведомяване (виж т.4.4.3) | Възстановителен екип | 18 |
| 4 | Прилагане на процедура за възстановяване работата на информационните процеси в зависимост от нивото на проблема:  Второ ниво – в сървърно помещение в сградата на „БДЖ” ЕАД намираща се на ул. Иван Вазов 3  Забележка 1: Описани са операции върху основния и резервния сървър. Ако основният е повреден, той се изключва, а операциите, предвидени върху него, се пропускат.  Забележка 2: Тази последователност разменя ролите на двата сървъра. Ако е необходимо да се върне началното положение, тя трябва да се повтори   * спира се Domino Service и на двата сървъра * редактира се файлът C:\R6\Notes.ini на основния сървър. Променят се следните параметри:   KeyFile=backup.mtc.id  ServerKeyFile=backup.mtc.id   * редактира се файлът C:\R6\Notes.ini на резервния сървър. Променят се следните параметри:   KeyFile=workflow.mtc.id  ServerKeyFile=workflow.mtc.id   * изключват се основните мрежови платки на сървърите * включват се резервните платки * стартира се Domino Service и на двата сървъра | Възстановителен екип |  |
| 5 | Докладване за извършените дейности | Възстановителен екип |  |
| 6 | Завършване на възстановителните дейности | Възстановителен екип |  |

**Важни компоненти, софтуер и хардуер**:

|  |  |  |  |
| --- | --- | --- | --- |
| **Софтуер** | **Местонахождение** | **Лице за контакти** | **Телефон** |
| Server Windows 2003  Lotus Domino Server | сървърно помещение в сградата на „БДЖ” ЕАД намираща се на ул. Иван Вазов 3 | Юри Караманов  Стамен Хаджийски | 9409695  9409706 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Хардуер** | **Местонахождение** | **Лице за контакти** | **Телефон** |
| Server x86; 4 GB RAM; 4х320 GB HDD - RAID 0+1; 10/100/1000 NIC | сървърно помещение в сградата на „БДЖ” ЕАД намираща се на ул. Иван Вазов 3 | Юри Караманов  Стамен Хаджийски | 9409695  9409706 |

**Необходими ресурси:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ресурси** | **Брой** | **Срок** | **Местонахождение** | **Доставчик** |
| Хора | 1 | До 1 час | сървърно помещение в сградата на „БДЖ” ЕАД намираща се на ул. Иван Вазов 3 | Министерство на транспорта, информационните технологии и съобщенията,  Фирма „Envisimo” |
| Преносими компютри | 1 |

**ПРИЛОЖЕНИЕ 1**

**Контролен лист**

|  |  |
| --- | --- |
|  | **Дейност** |
| 1 | Прави се оценка на настъпилите събития преди да се вземе решение за активиране на плана в МТИТС. |
| 2 | При постъпване на сигнал за настъпило събитие:   * Отбелязва се името и времето на съобщението за настъпилото събитие; * Проверяват се всички източници, сигнализиращи за настъпило събитие (като противопожарни алармени инсталации) * Уведомяват се охраната / персонала по поддръжката * Когато се налага евакуация на сградата, се осигурява безопасност на данните * Когато се налага евакуация на сградата, се събира възстановителният екип: - при настъпване на събитието - сървърно помещение в сградата на „БДЖ” ЕАД намираща се на ул. Иван Вазов 3 * При наличие на наранени служители, се уведомяват службите за спешна помощ |
| 3 | Събира се информация за настъпилото събитие |
| 4 | * Какво е събитието?   + Проблем с работата на информационните услуги в някои дирекции   + Проблем с работата на информационните услуги в цялото Министерство   + Липса на достъп до информационните системи на МТИТС и ИА по програма ИСПА   + Обемът на използваните информационни услуги е нараснал или намалял драстично * Кои дирекции / информационни услуги са засегнати? * Функционират ли все още информационните системи? * Нормалното протичане на работните процеси зависи ли от нарушените информационни процеси? От какъв характер е това нарушение? |
| 5 | Описание и класификация на проблема |

**ПРИЛОЖЕНИЕ 2**

**Тестване на Плана за непрекъснатост на информационните процеси**

Тестването на ефективността на плана се провежда на всеки шест месеца по предложение на Координатора на плана, като решението за началото и обхвата на теста, контрола на провеждането, както и анализа на резултатите остават задължение на екипа по възстановяването.