**ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ**

**за**

***„*Изграждане на информационна инфраструктура на МРРБ и разработване**

**на електронни административни услуги”**

**По Обособена позиция № 4**:

***„Разработване и внедряване на софтуерна информационна система за управление и контрол на информационните активи“***

**На проектно предложение:** „МРРБ – ефективна, модерна и прозрачна приходна администрация в услуга на гражданите и бизнеса”

# Обща информация

Към настоящият момент управлението на информационните активи е съвместна или последователна работа на повече от една дирекция на Министерството на Регионалното Развитие и Благоустройството. Затруднената комуникация между отделните звена на администрацията е причина и за възможността от несъответствия и грешки, което от своя страна води до затрудняване при идентифицирането на активите, които ще попаднат в обхвата на приложение на Системата за управление на качеството и информационната сигурност (СУКИС) и собствениците на тези активи. С внедряването на информационната система тези проблеми ще бъдат напълно разрешени. Също така, ще се изпълнят изискванията на Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност. С изграждането на системата ще се постигне устойчивост по отношение на работата със СУКИС.

# Цел на проекта и очаквани резултати

Софтуерната информационна система за управление и контрол на информационните активи е предназначена да осигури лесно управление и прецизен контрол на ИТ инфраструктурата в МРРБ по отношение на наличните информационни активи.

Общата цел на проекта е чрез изграждането и внедряването на тази система да бъде подобрено качеството на предоставяните административни услуги към гражданите, тъй като тя ще подпомогне процеса при класификация, управление и контрол на информационните активи, поддържането на инвентарни списъци, отговарящи на изискванията на Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност.

Специфичните цели са свързани с:

* улеснено инсталиране и управление на софтуер;
* централизирано управление на софтуерните обновявания;
* централизиран мониторинг на ресурсите на сървърите, информационните масиви и системите за управление на бази данни;
* поддържане на база данни с наличен и инсталиран софтуер и хардуер. Проследяване на промените по инсталациите на софтуер и хардуер.

Като резултат от реализиране на целите по проекта ще се увеличи ефективността на процесите в организацията, като ще се усъвършенстват съществуващите процедури във връзка с предоставянето на по-качествени услуги.

# Описание на проектните дейности

В обхвата на проекта изпълнителя трябва да разработи и внедри информационна система за управление и контрол на информационните активи, отговаряща на изискванията на Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност.

Дейностите по разработването и внедряването трябва да преминат през следните етапи:

1. **Етапи за внедряването на информационна система за управление и контрол на информационните активи**

* **Етап 1** Анализ на съществуващото положение – съществуващи информационни системи в МРРБ, прилагани технологии, бази данни и тяхното използване в отделите и структурите на МРРБ както и за обмен на данни с други администрации. Анализ на съществуващите информационни системи по отношение на изискванията за Информационна сигурност, на достъпност, автентичност, цялосност и конфиденциалност на съхраняваните или предаваните данни.
* **Етап 2** Проучване на използваните стандарти за връзка с външни системи и препоръки за тяхното оптимизиране и стандартизиране съгласно изискванията на „НАРЕДБА за общите изисквания за оперативна съвместимост и информационна сигурност”. Класификация на видовете електронни документи и данни обменяни между администрациите.
* **Етап 3** Анализ на съществуващите политики за информационна сигурност в МРРБ по отношение на:а) мрежа; б) системи; в) приложения; г) информация съобразно изискванията на Наредбата за информационна съвместимост.
* **Етап 4** Идентификация и оценка на рисковите фактори при информационната сигурност за системите в МРРБ. Разработване на механизми за контрол и въздействие върху рисковете.
* **Етап 5** Препоръки за промени в информационните системи в МРРБ по отношение структура, формати и използвани информационни технологии при съхраняване и обмен на информация в МРРБ, както и с други администрации.
* **Етап 6** Проектиране на системата за управление и контрол на информационните активи в МРРБ - централизиран достъп до логовете, алармени събития при опити за неправомерен достъп до информация, мониторинг на ресурсите на сървърите, информационните масиви и системите за управление на бази данни.
* **Етап 7** Проектиране на Регистър на използваните стандарти при информационните системи в МРРБ съгласно изискванията на чл. 57 от Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност.
* **Етап 8** Реализация на системата и регистъра.
* **Етап 9** Пилотно внедряване и зареждане на регистъра с данни.
* **Етап 10** Обучение на администраторите, операторите и вътрешните одитори за работа със системата и регистъра и поддържане в съответствие на системата с изискванията на Наредбата - до 5 човека в група (общо 5 групи), общо 5 дни обучение по групи: общо 25 човека.
* **Етап 11** Анализ на съответствието и Сертификация за оперативна съвместимост и информационна сигурност съгласно изискванията на Наредбата за оперативна съвместимост и информационна сигурност и извършеното по дейности 4, 5, 8 и 9. Препоръки за бъдещо развитие.

1. **Класификация, контрол и управление на информационните активи**

4.1. Картите на наличните информационни ресурси в МРРБ трябва да определят еднозначно:

а) конкретен служител за кои информационни ресурси (компютри, устройства, софтуерни продукти/системи, бази данни и др.) отговаря;

б) конкретен софтуерен продукт/информационна система и/или коя база от данни на кои компютри и устройства се използват.

4.2. Инвентарните списъци за наличните информационни ресурси в МРРБ трябва да включват:

а) за хардуерни устройства (без бързо амортизируемите, като мишки, клавиатури и други подобни) минималният набор от данни, които трябва да се поддържат, включва:

- сериен номер;

- фабричен номер;

- модел;

- описание на основните технически параметри (процесор/честота, размер на паметта и вид/тип, модел на диска и размер, захранване - мощност и модел/тип, списък на аксесоарите към устройството и др.);

- дата на придобиване;

- дата на пускане в експлоатация;

- дата на извеждане от употреба;

- дата на продажба/бракуване/даряване;

- местоположение на устройството;

- име на служителя, отговарящ за функциониране на устройството;

- име/имена на служителя/служителите, ползващ/ползващи устройството;

- дати на обслужване и ремонт на устройството;

- описание на извършеното обслужване/ремонт;

- с кои устройства е свързано това устройство;

- работата на кои устройства зависи от правилното функциониране на това устройство;

- правилното функциониране на това устройство от работата на кои устройства зависи;

- кои работни процеси обслужва това устройство;

б) за софтуерни продукти минималният набор от данни, които трябва да се поддържат, включва:

- име на продукта;

- версия на продукта;

- списък на минималните изисквания към хардуера за нормална работа на продукта;

- дата на придобиване;

- дата на инсталиране и настройка;

- дата, от която започва да тече лицензът за ползване на продукта;

- машина/машини, на която/които е инсталиран продуктът;

- дата на извеждане от употреба;

- дата на изтичане на лиценза за ползване на продукта;

- дата, на която са извършени промени в настройки или в самия продукт;

- описание на извършените промени;

- име на служителя, инсталирал продукта;

- име на служителя, извършил настройките;

- име на служителя, извършил промените;

- име на файла, в който се пази състоянието преди промените;

- кои работни процеси обслужва този софтуерен продукт;

- работата на кои софтуерни продукти зависи от правилното функциониране на този софтуерен продукт;

- правилното функциониране на този софтуерен продукт от работата на кои софтуерни продукти зависи.

4.3. Всички информационни системи, които се въвеждат в експлоатация в администрациите, трябва да се съпровождат с подробна документация за:

а) всички функции на клиента, приложението и базите данни;

б) административните средства за достъп и настройка;

в) схеми на базите данни с подробно описание на таблиците и връзките;

г) контролите при въвеждане и обмен на данни;

д) контролите при обработката и резултатите от обработката;

е) приложението с всички модули, "use cases", UML схеми и интерфейси.

4.4. Инсталирането и настройката на нови софтуерни и хардуерни продукти да се планира и всички лица, използващи засегнатите ресурси, да се уведомяват не по малко от 3 дни преди извършване на инсталацията или настройката.

4.5. Преди извършване на инсталация да се направят резервни копия на софтуера, файловете и базите данни, като се разработи и "roll back" план.

4.6. Инсталирането, настройката и поддръжката на нови софтуерни и хардуерни продукти да се извършват в периоди с минимално натоварване на съответните ресурси.

4.7. Преди инсталиране в оперативно действащите системи на нови софтуерни и хардуерни продукти те да се тестват в тестова среда максимално близка до реалните работни условия.

4.8. Служителите в администрациите носят материална отговорност за мобилните устройства, които са им предоставени за ползване. Мобилните устройства се получават от служителите, които ги използват, срещу подпис върху документ, съдържащ пълното описание на мобилното устройство и инсталирания софтуер.

4.9. Услугите по активен анализ на защитеността на системата (активни скенери на защитеността) позволяват да се открият и отстранят недостатъци в системата за защита на информационните активи, преди от тях да са се възползвали злонамерени лица.

1. **Действия при мониторинг на събитията и инцидентите в информационните системи на администрациите**

5.1. При съхраняването на информация за събития и инциденти, свързани с информационните системи на администрациите, трябва да се създават следните записи:  
а) дата и време на настъпване на събитието;  
б) уникален идентификатор на ползвателя - инициатор на действието;  
в) тип на събитието;  
г) резултат от събитието;  
д) източник на събитието;  
е) списък на засегнатите обекти;  
ж) описание на измененията в системата за защита, произтекли от събитието.   
5.2. Ръководителите на администрациите трябва да определят точни процедури за мониторинг на използването на системата, с които да осигурят изпълнението само на регламентирани процеси от страна на ползвателите. Процедурите за мониторинг трябва осигуряват:  
а) реалистична оценка и мерки за управление на риска;  
б) проследяване на изключения или ненормално поведение на ползватели за определен период;  
в) осигуряване на записи както на успешните, така и на отказаните опити за достъп в системата.  
5.3. За осигуряване на точност и пълнота на записите на логовете, които могат да се използват за разследване на неправомерни действия или за нуждите на ангажиране на съдебни доказателства, ръководителите на ведомствата трябва да осигурят поддържането на единно време в информационните системи съгласно Наредбата за електронните административни услуги, приета с Постановление № 107 на Министерския съвет от 2008 г. (ДВ, бр. 48 от 2008 г.).

1. **Възможностите за конфигурационно управление на бази данни на системата трябва да:**

* моделира цялото обкръжение включващо мрежи, сървъри, виртуална среда и софтуерни приложения;
* съпоставя ИТ елементи, данни и информация в нормализиран вид;
* предоставя възможност за логическо и физическо групиране;
* взима данните чрез автоматично откриване, уеб API интерфейси, XML импорт/експорт и ръчно въвеждане;

1. **Системата трябва да следи наличността като:**

* поддържа ICMP response тестване;
* поддържа SNMP response тестване;
* поддържа тестване на TCP/IP услуги като HTTP,SMTP, FTP, DNS, DHCP, WINS, NetBIOS и други;
* поддържа тестване на специфични TCP/IP портове с изследване по regular expression, състояние като – отворен, затворен, филтриран;
* поддържа тестване на портлети;
* използва синтетични транзакции за тестване на наличността на уеб сайтове;
* тества специфично поведение симулирайки потребителски действия;
* тества наличност на услуги в Windows като Active Directory,IIS, Sharepoint, Exchange, Terminal Services, Apache Tomcat;
* тества за наличност на процеси Windows/Linux/Unix;
* тества мрежата за наличност и корелативно свързване;
* поддържа мониторинг на бази данни Oracle, MySQL,MS SQL и PostgreSQL;
* поддържа мониторинг на мейл услуги;
* предефинира набори за мониторинг на хардуерното състояние за HP, Dell, SUN/Oracle/, Cisco, IronPort, Siemens, Juniper;
* провежда мониторинг на виртуални инфраструктури базирани на Vmware vSphere, Microsoft Hyper-V, Oracle VM.

1. **Системата трябва да предоставя инвентаризация и следене чрез:**

* автоматично откриване на IP базирани устройства;
* поддръжка на иконно представяне на откритите устройства и да организира по класове, групи, системи и местоположение;
* следене на детайли за конфигурацията на устройствата като интерфейси, ОС, услуги, процеси, софтуер и други;
* автоматично сканиране и откриване на VMware vSphere Microsoft Hyper-V инфраструктура;
* използване на IP адресната схема;
* автоматично логване на промени чрез автоматичното и ръчно откриване.

1. **Системата трябва да следи производителността като:**

* следи основни параметри като памет, процесор, диск, мрежа, температура;
* планирано да събира данни от SNMP OID стойности;
* безагентно следи основните параметри на операционните системи;
* безагентно следи Java application servers и Java виртуални машини използвайки JMX;
* предоставя голяма база от предварително въведени MIB-ове и възможност за добавяне;
* поддържа собствени скриптове за събиране на данни за производителността;
* предоставя възможност за поставяне на няколко гранични стойности по нива на специфични метрики;
* предоставя възможност за генериране на събития/аларми базирано на гранични стойности;
* графично изобразява тенденциите през изминало време – часово, дневно, седмично, месечно и годишно.

1. Системата трябва да управлява събития, следи дневници и аларми като:

* събира събития от различни източници, мониторинг на наличност, производителност syslog източници, SNMP трапове, Windows Event Log;
* автоматизирано известява за събитие по e-mail, FTP, HTTP, SNMP Trap, DB Alert-и;
* създава частни събития чрез XML-RPC интерфейс;
* обработва специфични за приложенията текстови логове чрез части скриптове;
* предоставя възможност за създаване на поддържала за обработка на събития през GUI интерфейс;
* автоматично рестартира услуги по различни критерии, приоритети и спазвайки шаблон за зависимост на услугите;
* автоматични действия като следене и само-рестартиране на LEAKAGE процеси;
* автоматично почиства дисковото пространство по предефиниране критерии, освобождаване на памет, изпълнение на частно дефинирани команди;
* поддържа автоматично запускане на съхранени процедури в база данни;
* поддържа автоматична класификация на събития, приоритизация на събития и дедуплициране;
* поддържа автоматична връзка от тип начало-край;
* предоставя възможност за приемане на дадено събитие от оператор;
* поддържа автоматично и ръчно архивиране;
* предоставя възможност за визуализация както на текущите събития, така и на архиви.

1. Системата трябва да се интегрира с:

* Web Services API's (XML-RPC и REST);
* XML import/export;
* Python Scripting Shell;
* Google Maps, чрез портлет.

1. Функционалността на системата за отчитане и доклади трябва да осигурява:

* изпратени по електронната поща отчети с вградена графика и изображения;
* стандартни и частни графики дефинирани използвайки RDD Graphing Language;
* отчети които включват частни селекции на индивидуални графики;
* мултиграфичен отчет, който включва комбинации от различни елементи на различни устройства;
* автоматично генериране на графични и таблични отчети за изминало време – часово, дневно, седмично, месечно и годишно.

1. Системата трябва да поддържа още:

* сигурен уеб базиран портал и конзоли;
* достъп базиран на роли;
* частни работни екрани с различни събития;
* частни работни екрани които обобщават данни от събития по бизнес системи и значимост;
* AJAX-Enabled потребителски и администраторски уеб интерфейси и портлети;
* частична drag & drop функционалност.

1. Административните функции на системата трябва да:

* предоставят потребителски определени вътрешни събития;
* позволяват на потребителите да сменят съобщения и аларми така че да спомагат бизнес нуждите;
* определят групи;
* поддържат групиране за събиране на поддържала за няколко потребителя на едно място;
* предоставят възможност за лесно създаване на шаблони за следене на различни производители.

1. Системата трябва да поддържа следния набор от бази данни

* Oracle, MySQL, MS SQL, PostgreSQL.

1. Системата трябва да работи с уеб базиран графичен интерфейс на браузъри

* Internet Explorer, Firefox, Google Chrome, Opera, Safari.

1. Системата трябва да има възможност за работа върху следните виртуализационни платформи и приложни сървъри:

* Microsoft Hyper-V;
* Microsoft Sharepoint.

1. Системата трябва да работи има възможност за работа върху следните уеб сървъри:

* Apache Web Server;
* Microsoft IIS;
* Web (HTTP) Transactions.

1. Системата трябва да поддържа следното оборудване за справяне с непредвидени ситуации:

* Powerware UPS;
* HP Temperature Sensors;
* APC UPS PowerNet.

1. Системата трябва да е съвместима с мрежово оборудване:

* Cisco, HP, Dell, 3COM, IronPort, Brocade JUNIPER.

1. Системата трябва да поддържа хардуер, сториджи и библиотеки на:

* HP, Dell, SUN, Oracle.

1. Системата трябва да работи със следните протоколи:

* DIG, DNS, Generic Printer Monitor, NNTP, NTP;
* RPC, HTTP, SMTP, FTP, DHCP, NetBIOS, SSH;
* RSH, Telnet, RDP, LDAP, LDAPS.

Навсякъде, където е споменат модел, източник, процес, търговска марка или др. следва да се счита „или еквивалентен“.

Неразделна част от техническата спецификация са общите технически изисквания за изпълнение на обществената поръчка от документацията за участие.

Гаранционна поддръжка – минимум 12 месеца.

Срок за изпълнение – до 5 месеца от сключване на договор.

**Изисквания за прототип на СОФТУЕРНА ИНФОРМАЦИОННА СИСТЕМА ЗА УПРАВЛЕНИЕ И КОНТРОЛ НА ИНФОРМАЦИОННИТЕ АКТИВИ**

**Въведение**

*Цел и обхват*

В този раздел се дава кратко описание на *Прототип на* **СОФТУЕРНА ИНФОРМАЦИОННА СИСТЕМА ЗА УПРАВЛЕНИЕ И КОНТРОЛ НА ИНФОРМАЦИОННИТЕ АКТИВИ** (наричана по-долу Системата), неговата цел и обхват.

*Резюме*

В този раздел се дава описание от гледна точка за управленската перспектива и преглед на рамката, в която концептуалният дизайн на Системата е създаден. Ако е необходимо, трябва да се включи информация, разгледана в следващите секции в резюмето.

* *Преглед на Системата*. В този раздел се описва системата в повествователна форма, като не се използват технически термини. Той трябва да представи на високо ниво архитектурна диаграма на Системата, показваща, ако е приложимо, разделянето на подсистеми. Предоставя се на високо ниво контекстна диаграма за системата. Позовете се на *Техническото задание за Системата,* за да се направи разпределяне на функционалните изисквания към различни части от дизайна на системата.
* *Ограничения в дизайна*. В този раздел се описват всякакви ограничения в дизайна на Системата (справка на всички анализи за размяна, проведени като използване на ресурсите в сравнение с производителността, или конфликти с други системи) и включване на всякакви предположения, направени от екипа при разработването на дизайна на Системата.
* *Бъдещи непредвидени случаи*. В този раздел се описват всички обстоятелства (непредвидени случаи), които биха могли да възникнат в дизайна на Системата, и които могат да променят посоката на развитие (изграждане). Възможностите включват липсата на договори за интерфейс с външни организации или нестабилна архитектури в момента на създаване на този документ. Адресиране на евентуални алтернативни планове.

**Архитектура на Системата**

В този раздел се описва архитектурата на системата и/ или подсистемата.

*Архитектура на хардуера на Системата*

В този раздел се описва цялостната хардуерна система и организацията. Включва списък на хардуерните компоненти (с кратко описание на всеки елемент) и диаграми, показващи връзки между компонентите. Ако е необходимо, се използват подраздели за адресиране на всяка подсистема.

*Архитектура на софтуера на Системата*

В този раздел се описва цялостната софтуерна система и организацията. Включва списък на софтуерни модули (това може да включва функции, подпрограми, или класове), компютърни езици и инструменти за софтуерен инженеринг, подпомагащи компютърното програмиране (с кратко описание на функцията на всяка позиция). Трябва да се използват структурирани организационни диаграми/ обектно-ориентирани диаграми, които показват различни нива на сегментацията надолу до най-ниското ниво. Всички детайли на диаграмите трябва да имат поредни номера и имена. Включване на описание, което разширява и подобрява разбирането на функционалното разпределение. Ако е необходимо, трябва да се използват подраздели за адресиране на всеки модул.

*Забележка*: Диаграмите трябва да препокриват диаграмите на потоците данни от Техническото задание, осигуряващи физическите процеси и потоците данни, свързани с логическите процес от Техническото задание и потока данни.

**Дизайн на файлове и база от данни**

Предоставя се изчерпателен речник за данни показващ елементите на данните: име, тип, дължина, източник, правила за валидиране, поддръжка (способност за създаване, четене, актуализиране и изтриване), складове от данни, изходи, псевдоними и описание.

* *Система за управление на СУБД файлове*. В този секция се разкрива окончателния дизайн на СУБД файлове и включва следната информация, ако е подходящо (виж речника на данните):

(1) Рафиниран логически модел; предоставящ нормализирани оформления на таблица, диаграми за отношенията на обектите, както и друга логическа информация за проекта;

(2) Физическо описание на схемите на СУБД, под-схеми, записи, редове, таблици, размери на страницата за съхранение и др.;

(3) Методи за достъп (например индексирани, чрез набор, последователен, произволен достъп, сортирани подчертани област и т.н.);

(4) Приблизителна оценка на СУБД размера на файла или обем на данни в рамките на файла и страниците с данни, включително и претоварване, произтичащо от методите за достъп и свободното пространство;

(5) Определяне на честотата на актуализацията на таблиците на базата данни, изгледи, файлове, области, записи, множества, и страници с данни;

* *Система за управление на не-СУБД* *файлове*. В тази секция се осигурява детайлно описание на всички не-СУБД файлове и включва изчерпателно описание на използването на всеки файл - включително ако файлът се използва за въвеждане (вход), извеждане (изход), или и двете, ако този файл е временен файл; индикация на кои модули четат и пишат във файла и т.н.; и файлови структури (виж речника на данните). При необходимост, структурата на информацията за файла следва да:

(1) Идентифицира структурите на запис, ключове или индекси на запис, както и справочни елементи на данните в рамките на записите;

(2) Определи дължината на записа (фиксирана или максимално променлива дължина) и блокиращи фактори;

(3) Определяне на метода за достъп до файла - например, индекс на резултата, виртуална последователност, случаен достъп и др.;

(4) Приблизителна оценка на размера на файла или обем на данните в рамките на файла, включително и претоварване в резултат на методите за достъп до файла.

**Интерфейс човек-машина**

В този раздел се предоставя подробен проект на системните и подсистемите входове и изходи, свързани към потребител/ оператор. Всяка допълнителна информация може да се добавят към този раздел и може да бъде организирана според това каква структура представя по най-добрия начин проектите на операторския вход и изхода. В зависимост от конкретния характер на проекта, може да бъде подходящо да се повтарят тези раздели за дизайна на системата и на ниво модули. Допълнителна информация може да бъде добавена към подразделите, ако предложените списъци са недостатъчни, за да се опишат входовете и изходите на проекта.

*Входове*

В тази секция е описана входната медия, използвана от оператора за предоставяне на информация за системата; показва препокриването на потоците от данни на високо ниво, описани в раздел *Преглед на системата*. Например, екрани за въвеждане на данни, оптични тип четци, бар код скенери и др. Ако е необходимо, входния тип записи, структури на файлове и структури на бази данни, предоставени в раздел *Дизайн на файлове и база от данни*, могат да бъдат посочени. Включване на определения на елементи на данните, или отнасяне до речника на данните.

Предоставяне на оформлението на всички входни екрани за данни или графичния потребителски интерфейс (ГПИ). Предоставяне на графичното представяне на всеки интерфейс. Определяне на всички елементи на данните, свързани с всеки екран или ГПИ, или позоваване на речника на данните.

Този раздел трябва да съдържа критерии за редактиране на елементите на данните, включително и конкретни стойности, област от ценности, задължителни/опционални, буквено-цифрови стойности и дължина. Също така адресиране на контрол за въвеждане на данни за предотвратяване на неспазване на редактирането.

Обсъждане на разни съобщения, свързани с входовете на оператора, включително и описание на всички ограничения за достъп или съображения за сигурност;

*Резултати (изходи)*

В този раздел се описва дизайнът на изхода на системата по отношение на потребител/ оператор; показват препокриването на потоците от данни на високо ниво, описани в раздел Преглед на системата. Изходите на системата включват доклади, данни, екрани и ГПИ, резултати от питане и т.н. Изходните файлове са описани в раздел *Дизайн на файлове и базата от данни* и могат да бъдат съотнесени към този раздел. Следното трябва да се предостави, ако е необходимо:

* Установяване на кодове и имена за доклади и екрани за показване на данни;
* Описание на съдържанията на доклад и екран (предоставяне на графично представяне на оформлението и определяне на всички елементи на данни, свързани с оформлението или препратка съм речника на данните);
* Описание на целта на резултата, включително и идентификация на първичните потребители. Доклад за изискванията за разпределяне, ако има такива (включително честотата на периодични отчети);
* Описание на всички ограничения за достъп или съображения за сигурност.

**Контроли за интегритета на Системата**

Чувствителните системи за *автоматизирана обработката на данните* използват информация, чиято загуба, злоупотреба, промяна или неоторизиран достъп до тази информация би могло да засегне националните интереси, провеждане на правителствена програма, или личния живот на физическите лица.

От разработчиците на чувствителни системи се изисква да разработят спецификации за следните минимални нива на контрол:

* Вътрешна сигурност за ограничаване достъпа до критични елементи на данните;
* Одитни процедури, които да отговарят за контрол, отчетност, както и изисквания за период на задържане за оперативни и управленски доклади;
* Одитни следи за приложението за динамичен одит за достъп до и възстановяване на определени критични данни;
* Използване или изискване на стандартни таблици за валидиране на полетата на данните;
* Процеси за проверка на допълнения, заличавания или актуализации на критични данни;
* Способност за идентифициране на цялата одитна информация чрез използване на потребителската идентификация, идентификация на работно място, дата, време, както и достъп до данни.