**ПОЛИТИКА**

**ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ**

В съответствие с изискванията на

Наредба за минималните изисквания за мрежова и информационна сигурност

**УТВЪРДИЛ,**

**Изпълнителен директор на ИАСАС: ................................**

**/инж. Бистра Павловска/**

Версия 1

Влиза в сила от ......................... г.

Автор на документа: КОНСЕХО ЕООД

**СЪДЪРЖАНИЕ**

[I. ИЗПОЛЗВАНИ ТЕРМИНИ, ОПРЕДЕЛЕНИЯ И СЪКРАЩЕНИЯ 3](#_Toc56687226)

[II. СПИСЪК НА ФОРМУЛЯРИТЕ КЪМ ПОЛИТИКАТА ЗА МИС 3](#_Toc56687227)

[III. ОБЩА ИНФОРМАЦИЯ ЗА АГЕНЦИЯТА 3](#_Toc56687228)

[IV. СИСТЕМА ЗА УПРАВЛЕНИЕ НА МРЕЖОВАТА И ИНФОРМАЦИОННА СИГУРНОСТ 5](#_Toc56687229)

[V. РАЗПРЕДЕЛЕНИЕ НА РОЛИ И ОТГОВОРНОСТИ (чл. 3 от НМИМИС) 5](#_Toc56687230)

[5.1. Висше ръководство 5](#_Toc56687231)

[5.2. Служител по мрежова и информационна сигурност (СМИС) 5](#_Toc56687232)

[5.3. Задължения на собствениците на активи (отговорниците за активи) 6](#_Toc56687233)

[5.4. Задължения на всички служители и външни лица 6](#_Toc56687234)

[VI. ПОЛИТИКА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ (чл. 4 от НМИМИС) 7](#_Toc56687235)

[VII. ДОКУМЕНТИРАНА ИНФОРМАЦИЯ (чл. 5 от НМИМИС) 8](#_Toc56687236)

[7.1. Управление на документираната информация (Политика за мрежова и информационна сигурност, Процедури, Специфични политики, Планове за непрекъсваемост и формуляри) 8](#_Toc56687237)

[7.2. Достъп до документацията 11](#_Toc56687238)

[7.3. Управление на документираната информация с външен произход 11](#_Toc56687239)

[7.4. Дейности, свързани с управление на документираната информация, съхранявана като доказателство за съответствия (записи) 11](#_Toc56687240)

[VIII. УПРАВЛЕНИЕ НА РИСКА ЗА МРЕЖОВАТА И ИНФОРМАЦИОННА СИГУРНОСТ (чл. 7 от НМИМИС) 12](#_Toc56687241)

[IX. УПРАВЛЕНИЕ НА ИНФОРМАЦИОННИТЕ АКТИВИ (чл. 8 от НМИМИС) 13](#_Toc56687242)

[9.1. Управление на жизнения цикъл на информационните активи 13](#_Toc56687243)

[9.2. Опис на информационните активи 13](#_Toc56687244)

[X. РЕСУРСИ 13](#_Toc56687245)

[10.1. Общи положения 13](#_Toc56687246)

[10.2. Човешки ресурси (чл. 9 от НМИМИС) 14](#_Toc56687247)

[10.3. Инфраструктура и оборудване, физически достъп (чл. 21, ал. 1 и чл. 26 от НМИМИС) 16](#_Toc56687248)

[XI. ИЗПЪЛНЕНИЕ НА ДЕЙНОСТИ ПО МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ 17](#_Toc56687249)

[11.1. Планиране на дейности и контрол 17](#_Toc56687250)

[11.2. Анализиране, оценяване и въздействие върху риска за мрежовата и информационна сигурност 17](#_Toc56687251)

[XII. ОЦЕНЯВАНЕ НА РАБОТНИТЕ ХАРАКТЕРИСТИКИ 17](#_Toc56687252)

[12.1. Наблюдение и контрол 17](#_Toc56687253)

[12.2. Вътрешни и външни одити, проверки, анкети (чл. 35, чл. 36 и чл. 37 от НМИМИС) 18](#_Toc56687254)

[XIII. ДЕЙСТВИЯ ЗА ПОДОБРЯВАНЕ 20](#_Toc56687255)

[13.1. Несъответствие и коригиращо действие 20](#_Toc56687256)

[ТАБЛИЦА С НАПРАВЕНИТЕ ИЗМЕНЕНИЯ 20](#_Toc56687257)

## I. ИЗПОЛЗВАНИ ТЕРМИНИ, ОПРЕДЕЛЕНИЯ И СЪКРАЩЕНИЯ

Термините и определенията, използвани в настоящата Политика за мрежова и информационна сигурност, са съгласно са съгласно БДС EN ISO/IEC 27000:2020 "Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Общ преглед и речник (ISO/IEC 27000:2018)", БДС EN ISO/IEC 27001:2017 "Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Изисквания" (ISO/IEC 27001:2013), Закон за киберсигурността и Наредба за минималните изисквания за мрежова и информационна сигурност.

Използвани съкращения:

1. НМИМИС – Наредба за минималните изисквания за мрежова и информационна сигурност;
2. СУМИС – Система за управление на мрежовата и информационната сигурност;
3. МИС – Мрежова и информационна сигурност;
4. ПМИС – Политика за мрежова и информационна сигурност;
5. СМИС – Служител по мрежова и информационна сигурност;
6. СА – Системен администратор.

## II. СПИСЪК НА ФОРМУЛЯРИТЕ КЪМ ПОЛИТИКАТА ЗА МИС

|  |  |
| --- | --- |
| ФПМИС 0.1 | Доклад за състоянието на мрежовата и информационна сигурност |
| ФПМИС 0.2 | Опис на информационните активи |
| ФПМИС 0.3 | Декларация за спазване на задълженията по мрежова и информационна сигурност |
| ФПМИС 0.4 | График за провеждане на обучения (инструктажи) по мрежова и информационна сигурност |
| ФПМИС 0.5 | Протокол от проведено обучение (инструктаж) по мрежова и информационна сигурност |

## III. ОБЩА ИНФОРМАЦИЯ ЗА АГЕНЦИЯТА

* 1. **ПРЕДСТАВЯНЕ**

Изпълнителна агенция по сортоизпитване, апробация и семеконтрол (ИАСАС, Агенцията) е второстепенен разпоредител с бюджетни средства към Министерство на земеделието, храните и горите, създадена с ПМС № 203 от 10 ноември 1999 г.

Агенцията извършва дейностите, предвидени в Закона за закрила на новите сортове растения и породи животни, Закона за посевния и посадъчен материал (ЗППМ), сертифицира и контролира производството на хмел и продукти от хмел в съответствие с правото на Европейския съюз (Регламенти 1850/2006/ЕС и 1234/2007/ЕС) и е контролен органа по чл. 115 от Закона за генетично модифицираните организми.

Агенцията е национален орган по отношение прилагането на схемите за семена на Организацията за икономическо сътрудничество и развитие (OECD).

По Закона за закрила на новите сортове растения и породи животни агенцията извършва експертиза по същество за различимост, хомогенност и стабилност на новите сортове растения въз основа на която Патентно ведомство издава сертификат за правна закрила.

За да отговори на очакванията на клиентите за предоставяне на административни услуги, при спазване на най-високи професионални стандарти, агенцията е акредитирана и има реално действащи системи за качество по ISO стандарт 9001:2015, и по стандарта на Международната асоциация на семетестващите лаборатории /ISTA/. Агенцията е оправомощена от Службата на Общността за сортовете растения (CPVO) да извършва експертиза от нейно име за различимост, хомогенност и стабилност на нови сортове, за предоставяне на правна закрила в Европейския съюз.

* 1. **АДРЕС:**
* гр. София 1113, бул. "Цариградско шосе" № 125, бл. 1.
	1. **ОРГАНИЗАЦИОННА СТРУКТУРА**

Организационната структура на Изпълнителна агенция по сортоизпитване, апробация и семеконтрол е представена и поддържана в актуално състояние на интернет страницата на ведомството: ([https://iasas.government.bg/](https://iasas.government.bg/%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B0/)).

## IV. СИСТЕМА ЗА УПРАВЛЕНИЕ НА МРЕЖОВАТА И ИНФОРМАЦИОННА СИГУРНОСТ

Изпълнителна агенция по сортоизпитване, апробация и семеконтрол е създала, приложила, поддържа и постоянно подобрява Система за управление на мрежовата и информационната сигурност съгласно изискванията на Наредба за минималните изисквания за мрежова и информационна сигурност.

Дейностите по създаване, документиране, внедряване, поддържане и подобряване на СУМИС са задължение и се извършват от всички длъжностни лица в агенцията. Основната отговорност за правилното функциониране на системата за управление се носи от Изпълнителния директор, служителя по мрежова и информационна сигурност и дирекция "Административно и финансово обслужване" (АФО).

## V. РАЗПРЕДЕЛЕНИЕ НА РОЛИ И ОТГОВОРНОСТИ (чл. 3 от НМИМИС)

Организационната структура на ИАСАС илюстрира управленската структура и функционалните връзки при организирането на дейностите.

### 5.1. Висше ръководство

Висшето ръководство на ИАСАС в лицето на Изпълнителния директор е ангажирано със Системата за управление на мрежовата и информационна сигурност като:

* носи пряка отговорност за мрежовата и информационната сигурност на ИАСАС, включително и за дейности, които Агенцията възлага на трети страни;
* създава условия за прилагане на комплексна система от мерки за управлението на мрежовата и информационната сигурност по смисъла на международен стандарт ISO/IEC 27001:2013;
* осигурява наличието на ресурсите, необходими за СУМИС;
* упражнява контрол чрез организиране на одити и годишни прегледи на мрежовата и информационна сигурност;
* определя, документира и налага отговорностите, свързани с развитието, поддръжката и експлоатацията на информационните и комуникационните системи;
* определя със заповед служител(и), отговарящ(и) за мрежовата и информационната сигурност;
* насърчава подобряването на СУМИС.

### 5.2. Служител по мрежова и информационна сигурност (СМИС)

Служителят по мрежова и информационна сигурност е на пряко подчинение на Изпълнителния директор и осъществява функции, свързани с организирането, управлението и прилагането на мерки за мрежова и информационна сигурност в ИАСАС.

Ръководството на ИАСАС е делегирало следните функции и отговорности на СМИС:

* Ръководи дейностите, свързани с постигане на високо ниво на мрежова и информационна сигурност, и целите, заложени в политиката на ведомството;
* Участва в изготвянето на политиките и документираната информация;
* Следи за спазването на вътрешните правила, регламентирани в документите от СУМИС, и прилагането на законите, подзаконовите нормативни актове, стандартите, политиките и правилата за мрежовата и информационната сигурност;
* Консултира ръководството на ИАСАС във връзка с информационната сигурност;
* Ръководи периодичните оценки на рисковете за мрежовата и информационната сигурност;
* Периодично (не по-малко от веднъж в годината) изготвя доклади за състоянието на мрежовата и информационната сигурност в Изпълнителна агенция по сортоизпитване, апробация и семеконтрол и ги представя на ръководството;
* Координира обученията, свързани с мрежовата и информационната сигурност;
* Организира проверки за актуалността на плановете за справяне с инцидентите и плановете за непрекъсваемост (ПЛН 6-1). Анализира резултатите от тях и организира изменение на плановете, ако е необходимо;
* Поддържа връзки с други администрации, организации и експерти, работещи в областта на информационната сигурност;
* Следи за акуратното водене на регистъра на инцидентите (Ф 6-1.2);
* Уведомява за инциденти съответния секторен екип за реагиране на инциденти с компютърната сигурност в съответствие с изискването на чл. 31, ал. 1 НМИМИС и П 6-1 "Управление на инциденти по мрежова и информационна сигурност";
* Организира анализ на инцидентите с мрежовата и информационната сигурност за откриване на причините за тях и предприемане на мерки за отстраняването им с цел намаляване на еднотипните инциденти и намаляване на загубите от тях;
* Следи за актуализиране на използвания софтуер и фърмуер.
* Следи за появата на нови киберзаплахи (вируси, зловреден код, спам, атаки и др.) и предлага адекватни мерки за противодействие.
* Организира тестове за откриване на уязвимости в информационните и комуникационните системи и предлага мерки за отстраняването им;
* Организира и сътрудничи при провеждането на одити, проверки и анкети и при изпращането на резултатите от тях на съответния национален компетентен орган;
* Предлага санкции за лицата, нарушили мерките за мрежовата и информационната сигурност.

### 5.3. Задължения на собствениците на активи (отговорниците за активи)

Собственици на активите по смисъла на ISO/IEC 27001:2013 (отговорните лица за активите по смисъла на чл. 8, ал. 2, т. 9 от НМИМИС) са лицата, отговорни за жизнения цикъл на съответния актив, които не притежават непременно правата на собственост върху актива. Собствениците на активи са длъжни да:

* гарантират, че активите, на които са собственици, са описани (ФПМИС 0.2 "Опис на информационните активи");
* извършват подходяща класификация и предпазване на тези активи;
* преглеждат периодично класификацията на активите;
* предлагат подходящи механизми за защита и контрол;
* разрешават достъп до тези активи в съответствие с класификацията на информацията;
* наблюдават съответствието при прилагането на определените механизми за контрол за съответните активи;
* осигуряват правилно обработване, когато активът бъде изтрит и унищожен;
* информират Служителя по мрежова и информационна сигурност/ Системен администратор за всякакви инциденти и нарушаване на активите, свързани с мрежовата и информационна сигурност.

### 5.4. Задължения на всички служители и външни лица

* всички служители на ИАСАС и външните лица (на граждански договор, консултанти, изпълнители по договор, временни работници и посетители) са длъжни да прилагат Политиката за мрежова и информационна сигурност в съответствие с извършваната от тях работа;
* всички служители са отговорни за сигурността на поверената им информация. При назначаване на работа, всеки служител подлежи на обучение по мрежова и информационна сигурност и се задължава да изпълнява изискванията на Системата за управление на мрежовата и информационна сигурност.

Всеки служител, който не изпълнява или нарушава изискванията на СУМИС, може да бъде предмет на дисциплинарно наказание като напр. прекратяване на трудовия договор и/или съдебно преследване.

* всички служители са длъжни да информират СМИС/ СА при инциденти и нарушаване на активите, свързани със сигурността на информацията;
* всички служители са длъжни да участват активно в непрекъснатото развитие и усъвършенстване на СУМИС в ИАСАС.

Отговорностите, пълномощията и компетентностите на служителите във ведомството са отразени в длъжностни характеристики и в трудово-договорните/служебните правоотношения между тях и ръководството на ИАСАС.

Длъжностните характеристики определят границите и характерните особености на работното място, трудовите задължения на служителя, изискванията на заеманата длъжност и условията на работа.

## VI. ПОЛИТИКА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ (чл. 4 от НМИМИС)

Основната цел на управлението на мрежовата и информационна сигурност в ИАСАС е да се осигури наличността, интегритета и конфиденциалността на информацията, собственост на учреждението, на други ведомства/държавни институции и на контрагенти на ИАСАС, както и да се осигури непрекъсваемост на процесите по време на всички дейности, които се извършват.

Настоящата Политика за мрежова и информационна сигурност гарантира, че:

* са определени рисковете за мрежовата и информационна сигурност, собствениците на тези рискове и защитата от вътрешни, външни, предумишлени и случайни заплахи;
* са взети предвид стратегическите цели на ИАСАС за мрежовата и информационната сигурност, както и подходът за постигането им в съответствие с общите стратегически и оперативни цели, нормативните и договорните изисквания;
* е осигурена и се поддържа конфиденциалността, наличността и интегритета на информацията;
* информацията е предпазена от неоторизиран достъп;
* критериите за оценяване на рисковете, както и нивото на приемлив риск, са определени и спрямо тях се оценява вероятността от възникване на заплахи, както и тежестта на тяхното въздействие за активите на Агенцията;
* нормативните и вътрешноорганизационните изисквания по мрежова и информационна сигурност са определени и се изпълняват;
* са разработени процедури и специфични политики за изпълнение на ПМИС, включващи мерки за защита от зловреден софтуер, защита от неоторизиран достъп, управление на инциденти, взаимоотношения с трети страни и др.;
* е осигурено обучение по управление мрежовата и информационната сигурност за всички служители;
* ПМИС има отношение към всички съответни процедури и специфични политики за сигурност на информационните и комуникационните системи, като напр. П 6-2 "Управление на рисковете за мрежовата и информационната сигурност", СП 6-3 "Използване на криптографски механизми", СП 6-9 "Класификация на информацията" и др., които са неразделна част от СУМИС (виж Ф 1-1.1 "Списък на документите от Системата за управление");
* всички съществуващи и потенциални пробиви ще бъдат съобщавани на Изпълнителния директор на Агенцията и ще бъдат щателно разследвани.

Изпълнителният директор и СМИС са отговорни за внедряването и поддържането на Политиката за мрежова и информационна сигурност и поемат ангажимент за непрекъснато подобряване на Системата за управление на мрежовата и информационна сигурност.

 При необходимост Политиката за мрежова и информационна сигурност се предоставя и на външни заинтересовани страни.

 Чрез Политиката за мрежова и информационна сигурност Изпълнителният директор на ИАСАС декларира личното си участие и отговорност за изпълнение на изискванията относно защитата на всички информационни и комуникационни активи от вътрешни, външни, предумишлени и случайни заплахи, но също така и по отношение на осигуряване на непрекъсваемост на дейността.

Одобрената Политика за мрежова и информационна сигурност се поддържа като част от документираната информация на системата за управление на мрежовата и информационна сигурност на Агенцията.

Цел на ИАСАС е основните дейности да отговарят на международните и национални нормативни изисквания и стандарти, както и на очакванията за сигурност на информацията на заинтересованите страни.

Документите от СУМИС и Политиката за мрежова и информационна сигурност се поддържат актуални, като се преразглеждат и оценяват минимум веднъж годишно и при необходимост се актуализират.

## VII. ДОКУМЕНТИРАНА ИНФОРМАЦИЯ (чл. 5 от НМИМИС)

Документираната информация на ИАСАС за мрежовата и информационна сигурност обхваща настоящата Политика за мрежова и информационна сигурност, Процедури, Специфични политики, Планове за действия, формуляри, информацията с външен произход и всякаква друга документирана информация (записи в свободен формат), съхранявана като доказателства за съответствие. Целта на разработената документирана информация е да намали загубите от инциденти чрез намаляване на времето за реагиране и за разрешаване, както и намаляване на вероятността от възникване на инциденти, породени от човешки грешки.

Политиката за мрежова и информационна сигурност на ИАСАС описва системата за управление при осъществяване на дейностите и процесите по отношение на мрежовата и информационна сигурност. Освен това тя служи за демонстриране на действащата система пред заинтересовани страни в съответствие с изискванията на НМИМИС.

По-долу е описан редът, по който се управлява документираната информация от СУМИС.

### 7.1. Управление на документираната информация (Политика за мрежова и информационна сигурност, Процедури, Специфични политики, Планове за непрекъсваемост и формуляри)

Етапите при създаването и въвеждането в действие на документите са:

* Разработване;
* Утвърждаване;
* Разпространение;
* Съхранение и архивиране;
* Преглед и поддръжка;
* Изменение.

**7.1.1. Разработване**

Разработената документирана информация в ИАСАС включва:

* Опис на информационните активи – ФПМИС 0.2;
* Схема на свързаност – ФСП 6-11.1 "Схема на свързаност";
* Логическа схема на информационните потоци – включена във ФСП 6-11.1;
* Документация на структурната кабелна система;
* Техническа, експлоатационна и потребителска документация на информационните и комуникационните системи и техните компоненти;
* Специфични политики/ Процедури за всяка дейност, свързана с администрирането, експлоатацията и поддръжката на хардуер и софтуер – документация от СУМИС;
* Специфични политики/ Процедури за служителите, указващи правата и задълженията им като потребители на услугите, предоставяни чрез информационните и комуникационните системи като използване на персонални компютри, достъп до ресурсите на корпоративната мрежа, генериране и съхранение на паролите, достъп до интернет, работа с електронна поща, резервиране и архивиране на информация, използване на преносими записващи устройства и т.н. – документация от СУМИС).

Документите от СУМИС се идентифицират по следния начин:

* Заглавие, версия, дата на издаване/утвърждаване, автор на документа;
* Всяка процедура носи буквен индекс "П" и пореден номер.
	+ Пример: Първа процедура от СУМИС се означава П 6-1.
* Всяка специфична политика носи буквен индекс "СП" и пореден номер.
	+ Пример: СП 6-8 е осма по ред политика от СУМИС.
* Формулярът носи буквен индекс "Ф", като:
	+ за произхождащите от ПМИС: ФПМИС
		- Пример: ФПМИС 0.2 – втори формуляр към Политиката за МИС;
	+ за произхождащите от процедура (П): Ф
		- Пример: Ф 6-1.3 – трети формуляр към първа процедура от СМИС;
	+ за произхождащите от специфична политика (СП): ФСП
		- Пример: ФСП 6-5.2 – втори формуляр към пета специфична политика;
	+ за произхождащите от плановете за непрекъсваемост (ПЛН): ФПЛН
		- Пример: ФПЛН 6-1.2 – втори формуляр към планове за непрекъсваемост от СУМИС.

Документите от СУМИС се описват във Ф 1-1.1 "Списък на документите от Системата за управление".

Документите се разработват от СМИС или от външен консултант, чрез възлагане с договор.

СМИС съгласува разработените документи с други заинтересовани служители в ИАСАС.

При наличие на забележки, документите се доработват и отново се представят за съгласуване до постигане на съгласие.

**7.1.2. Утвърждаване**

Изпълнителният директор на ИАСАС утвърждава документите от СУМИС или отказва мотивирано внедряването им. Одобрените и утвърдени документи се класифицират съгласно СП 6-9 "Класификация на информацията".

**7.1.3. Разпространение**

Служителите на ИАСАС ползват за четене Политиката за мрежова и информационна сигурност, Процедурите, Специфичните политики и формулярите на хартиен носител и в електронна среда. В електронна среда документацията е разпространена сред служителите посредством вътрешно споделено пространство (споделена директория) и при установени правила, гарантиращи невъзможността за внасяне на изменения от неоторизирани служители.

Предоставянето на Политиката за мрежова и информационна сигурност, както и на останалите документи от СУМИС на трети (външни за агенцията) лица става с разрешение на Изпълнителния директор на ИАСАС.

**7.1.4. Съхранение и архивиране**

Съхранението и архивирането на документите от СУМИС, както и на други електронни документи се осъществява съгласно приложимите нормативни изисквания и установените правила на Изпълнителна агенция по сортоизпитване, апробация и семеконтрол.

**7.1.5. Преглед и поддръжка**

Документите от СУМИС се поддържат в актуално състояние, преглеждат се за адекватност от СМИС минимум веднъж годишно и се обновяват при необходимост.

Необходимост от извършване на преглед и оценка на приложимостта на документите от СУМИС може да настъпи вследствие на:

* Открито несъответствие между описанието на дейност или процес в документ от системата и реалното му изпълнение;
* Промяна в начина на изпълнение на дейността или процеса, обект на документа;
* Промяна на нормативни изисквания;
* Други.

Предложението за извършване на преглед и оценка може да бъде направено от всеки служител на ИАСАС.

**7.1.6. Изменение**

Изменения в документите се правят:

* при промяна в процесите на управление на мрежовата и информационна сигурност или в отговорностите;
* при промяна в номера и/или наименованието, в съдържанието на ПМИС, процедура, специфична политика или на номера и/или наименованието на формуляр; при включване на нов или отпадане на формуляр;
* в резултат на предложения от одити, проверки и цялостен преглед на Системата за управление на мрежовата и информационна сигурност;
* при изменения на нормативни документи, при промяна в структурата, функциите или наименованието на Изпълнителна агенция по сортоизпитване, апробация и семеконтрол.

Предложение за изменение на документи може да постъпи от всеки служител на Агенцията. Изменението или отменянето на документ се осъществява със заповед на Изпълнителния директор на ИАСАС.

Пътят на разглеждане на предложенията, решението за изменение, неговото разработване, утвърждаване, архивиране и разпространение е както при разработката на документите от СУМИС.

Измененията в основните документи от СУМИС и Ф 1-1.1 "Списък на документите от СУ", с изключение на формулярите, се маркират в жълто. При последващо изменение новопромененият текст се маркира в жълто, а от текста на предишните изменения се отстранява маркирането. При промяна на версията променените текстове не се маркират.

Всички промени на документите от СУМИС (ПМИС, процедури и специфични политики) и техните актуални версии се отразяват в "Таблица на направените изменения", която е неразделна част от всеки документ.

Измененият документ се разпространява по реда за утвърждаване на нов документ.

### 7.2. Достъп до документацията

Документацията от Системата за управление на мрежовата и информационна сигурност на ИАСАС е достъпна до служители и външни лица на хартиен и електронен носител. В електронна среда тя е разпространена чрез вътрешно споделено пространство (споделена директория).

Информацията, доказваща по неоспорим начин изпълнението на изискванията на НМИМИС, се поддържа в актуално състояние. Тя е достъпна (по смисъла на чл. 5, ал. 4, т. 2 от НМИМИС) само за:

* лица, които е необходимо да я ползват при изпълнение на служебните си задължения по силата на трудови, служебни или договорни отношения;
* представители на съответните национални компетентни органи съгласно чл. 16, ал. 5 от Закона за киберсигурност;
* други организации, оправомощени с нормативен акт или договорни отношения.

### 7.3. Управление на документираната информация с външен произход

Документите с външен произход, необходими за планирането и функционирането на СУМИС, се определят от Изпълнителния директор на ИАСАС.

В ИАСАС се използват следните категории външни документи:

1. **нормативни документи**

Юрисконсулт регистрира националното приложимо законодателство, национални и международни технически стандарти (БДС ИСО) и директно приложимото право на ЕО във Ф 1-1.4 "Регистър документи с външен произход". Разпространението на регистъра е в електронна среда, в уеб базирана интернет система, достъпен за всички служители.

Юрисконсулт носи отговорност за актуалността на Ф 1-1.4.

При промяна отразява измененията във Ф 1-1.4 в жълт цвят.

### 7.4. Дейности, свързани с управление на документираната информация, съхранявана като доказателство за съответствия (записи)

За удостоверяване и проследяване съответствието, както и за ефективно управление на Системата за управление на мрежовата и информационна сигурност, в ИАСАС се генерират записи. Записите периодично се проверяват и анализират, за да може да се предприемат своевременно коригиращи действия.

Записите се създават на хартиен или електронен носител.

Изисквания към записите:

* записите съдържат информация, удостоверяваща пряко или косвено съответствието;
* записите са четливи, чисти, лесни за идентифициране, възстановими, съхранявани на места, осигуряващи подходящи условия за предпазване от повреждане и загубване и достъпни за ползване от служителите на Агенцията.

Записите се идентифицират посредством един или няколко от следните начини за идентификация:

* наименованието и/или логото на ИАСАС;
* наименованието на документа;
* индексация, ако е налична;
* името на служителя, който го издава (съставя);
* името и подписа на служителя, който ги утвърждава (ако е приложимо);
* дейността, процеса и др., за които се отнасят;
* дата на издаване (съставяне).

Записите се съхраняват на оперативно ниво, на хартиен и електронен носител при условия, предотвратяващи увреждането, похабяването и загубването им.

Унищожаване на записи на хартиен носител се допуска само след изтичане на установения срок за съхранение (вътрешно или нормативно определен срок). Унищожаването се извършва под контрола на Изпълнителния директор на ИАСАС или упълномощено от него лице.

Контролът за правилното съставяне и състояние на записите се извършва при одитите за ефикасно функциониране на СУМИС.

## VIII. УПРАВЛЕНИЕ НА РИСКА ЗА МРЕЖОВАТА И ИНФОРМАЦИОННА СИГУРНОСТ (чл. 7 от НМИМИС)

Основна задача за успешното функциониране на Системата за управление на мрежовата и информационна сигурност е правилното определяне на рисковете, свързани с мрежовата и информационна сигурност.

Определянето на рисковете и начините за тяхното управление има превантивен характер и е от изключително значение за:

* създаване на увереност, че СУМИС е способна да постига желаните резултати по отношение на мрежовата и информационна сигурност;
* предотвратяване и намаляване на нежеланите въздействия;
* постигане на непрекъснато подобрение на нивото на мрежовата и информационна сигурност.

Рисковете периодично се наблюдават, анализират и оценяват с цел избор на подходящи мерки за овладяването им.

Третирането на рисковете включва избирането на едно или повече действия за овладяването им и прилагане на тези действия.

Действията за третиране на риска могат да включват следното:

* избягване – процесът да бъде променен така, че рискът да бъде избегнат;
* споделяне – изнасяне на идентифицирания риск към външна организация (аутсорсинг или застраховане);
* намаляване (смекчаване)/ограничаване – ако рискът не може да бъде избегнат, се разработва алтернатива – стъпки, които ще сведат до минимум щетите в случай на рисково събитие;
* приемане – когато няма какво да се предприеме в отговор на риска, единствената възможност, която остава, е той да бъде осъзнат и приет.

С цел да се регламентира процесът по анализиране, оценяване, овладяване и управление на рисковете, свързани с мрежовата и информационна сигурност, ИАСАС създава и утвърждава П 6-2 "Управление на рисковете за мрежовата и информационната сигурност", в която определя реда, компетенциите, отговорностите, както и методиката за определяне и оценяване на рисковете.

## IX. УПРАВЛЕНИЕ НА ИНФОРМАЦИОННИТЕ АКТИВИ (чл. 8 от НМИМИС)

### 9.1. Управление на жизнения цикъл на информационните активи

Въз основа на ISO 55000:2014 ("Управление на активите. Общ преглед, принципи и терминология"), активите се дефинират по следния начин: "Активът е предмет, вещ или обект, който има потенциална или действителна стойност за организацията".

Процесът е регламентиран в П 6-3 "Управление на жизнения цикъл на информационните и комуникационните системи и техните компоненти".

### 9.2. Опис на информационните активи

Служителят по мрежова и информационна сигурност идентифицира активите, изискващи защита, по целесъобразност и ги регистрира във ФПМИС 0.2 "Опис на информационните активи".

В описа се документират следните типове активи:

* + - информационни системи;
		- комуникационни системи;
		- хардуерни устройства, с които са реализирани информационните и комуникационните системи;
		- фърмуерът на тези устройства;
		- софтуери, с които са реализирани информационните и комуникационните системи;
		- бази данни, включително лични данни по смисъла на GDPR;
		- записи за събитията (логове, журнали);
		- документация (експлоатационна и потребителска);
		- поддържащи системи (електрозахранващи, климатични);
		- системи за контрол на физическия достъп и на околната среда;
		- процеси/дейности, свързани с управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
		- документация на тези процеси и дейности;
		- служители, имащи отговорности към управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
		- външни организации, имащи отношение към управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
		- друго;

## X. РЕСУРСИ

### 10.1. Общи положения

При определяне на необходимите за СУМИС ресурси, следва да се имат предвид:

* възможностите и ограниченията на наличните ресурси;
* необходимостта от използване на външни доставчици (изпълнители).

За реализиране на целите за мрежова и информационна сигурност от решаващо значение е определянето и осигуряването на ресурси, включващи:

* човешки ресурси – служители с необходимата квалификация, знания и умения за заеманата от тях позиция;
* инфраструктура – работни помещения, оборудване, софтуер, информационни и комуникационни технологии и други, необходими за изпълнение на процесите;
* заобикаляща среда – осигуряваща възможност за ефективна работа на служителите и за нормално функциониране на процесите и оборудването;
* информация, знания и опит – интелектуална собственост, ръководства, инструкции, средства за комуникация и други данни, използвани като източници за получаване на информация и непрекъснато развитие на професионалната информираност за служителите, данни за несъответствия и решения по тях, стандарти за управление, литературни източници на информация и др.

### 10.2. Човешки ресурси (чл. 9 от НМИМИС)

Правилата за управление и сигурност на човешките ресурси, както и дисциплинарен процес за лицата, които са извършили нарушение по отношение на изискванията за МИС, са регламентирани в П 2-1 Осигуряване на ресурсите. Обучение, познания и компетентност.

10.2.1. Общи положения

За намаляване на риска от инциденти с мрежовата и информационна сигурност, умишлено или неумишлено предизвикани от служителите, Изпълнителна агенция по сортоизпитване, апробация и семеконтрол гарантира чрез своята СУМИС, че служителите, имащи отношение към процесите и дейностите, свързани с информационната сигурност, са с подходящата квалификация, знания и умения за изпълнение на отговорностите си. Ръководството на ИАСАС определя изисквания към компетентността на всички служители (квалификация, стаж, професионален опит и др.), необходими за изпълнение на функциите и задачите в агенцията, в техните длъжностни характеристики.

Всеки новопостъпил се запознава с длъжностната си характеристика, подписва трудов договор/договор за служебни правоотношения и "Декларация за спазване на задълженията по мрежова и информационна сигурност" (ФПМИС 0.3) и преминава през начален инструктаж за условията на работа в ИАСАС. Изпитателният срок на служителите, назначени по служебно правоотношение, е регламентиран в чл. 12 от Закона за държавния служител, а на служителите по трудово правоотношение – в чл. 70 от Кодекса на труда.

На новопостъпилия служител се осигурява право на достъп до документацията от СУМИС.

На служителя се провежда въвеждащо обучение от СМИС, на което му се представят изискванията, разписани в документите от СУМИС, извършва се първоначален инструктаж за повишаване на вниманието по отношение на мрежовата и информационната сигурност, както и приложимите за конкретната позиция изисквания. Въвеждащото обучение се документира във Ф 2-1.1 "Програма за обучение на нов служител".

10.2.2. Предоставяне/връщане на материални активи/права за достъп на служителя

Предоставянето на права за достъп до информационните и комуникационни системи на ИАСАС се осъществява по реда на СП 6-4 "Управление на достъпите и автентикацията" и след подадени от прекия ръководител на служителя формуляр Ф 6-4.4 "Заявка за предоставяне/ промяна/ прекратяване на достъп". След одобрение от страна на СМИС се пристъпва към предоставянето на необходимите за работа достъпи/активи.

При промяна/прекратяване поради нова длъжност или напускане, излишните активи се връщат, а правата се деактивират, като се прави запис в Ф 6-4.4 "Заявка за предоставяне/ промяна/ прекратяване на достъп" за съответния служител.

Всички предоставени на служителя активи в случай на напускане следва да бъдат върнати от същия, а всички права – деактивирани от Системен администратор (след одобрение от СМИС) не по-късно от последния работен ден на напускащия. Само след връщане на всички материални активи, служителят може да бъде освободен.

10.2.3. Обучение на служителите

Изпълнителна агенция по сортоизпитване, апробация и семеконтрол създава условия и осигурява ресурси за непрекъснато повишаване компетентността на служителите си.

Въз основа необходимостта от поддържане и повишаване квалификацията на служителите по отношение на мрежовата и информационна сигурност в съответствие с използваната техника и технологии, всяка година се планират и провеждат подходящи обучения на всички служители, както и периодични инструктажи на служителите за повишаване на вниманието им по отношение на мрежовата и информационната сигурност. Периодичните инструктажи се осъществяват по утвърден график (ФПМИС 0.4 "График за провеждане на обучения (инструктажи) по мрежова и информационна сигурност") и се документират по начин, гарантиращ проследимост, във ФПМИС 0.5 "Протокол от проведено обучение (инструктаж) по мрежова и информационна сигурност".

* **Вътрешни обучения и инструктажи**

За лектори се ползват СМИС, СА или други опитни служители от ИАСАС, или външни специалисти.

Лекторът подготвя програма/график за обучението, където определя:

* + Начална дата и продължителност на обучението/инструктажа;
	+ Темата на обучението/инструктажа;
	+ Участниците в обучението;
	+ Начин за приключване на обучението – тест, изпит, събеседване и т.н.
* **Външни обучения**

Документите, удостоверяващи провеждането на обучение като протоколи, сертификати, удостоверения и т.н. се съхраняват в ИАСАС във вид на документирана информация. Желателно е този вид информация да се съхранявана като копие и в личното досие на обучавания служител с цел ведомството да представи във всеки един момент доказателства за компетентността му.

10.2.4. Дисциплинарен процес

За всеки служител на Изпълнителна агенция по сортоизпитване, апробация и семеконтрол, извършил/позволил да се извърши пробив в сигурността на информацията, се изпълнява дисциплинарен процес съгласно установените норми в Закон за държавния служител, Кодекса на труда и приложимите вътрешноведомствени правила.

Всеки служител е длъжен да подаде сигнал до СМИС за забелязан пробив/ инцидент, касаещ мрежовата и информационната сигурност на ИАСАС.

За всеки получен сигнал за пробив в мрежовата и информационна сигурност или нарушение на специфичните политики, процедури и вътрешни правила се извършва разследване на обстоятелствата относно:

* Установяване на виновността на служителя;
* Вид и тежест на пробива;
* Влиянието на пробива върху активите;
* Дали нарушението е за първи път или се повтаря;
* Дали нарушителят е бил подходящо обучен;
* Други обстоятелства.

Дисциплинарният процес гарантира, че е постигнато разбиране и съгласие от страна на служителите по отношение на важността от спазването на внедрената СУМИС, както и последствията от несъобразяването с нейните изисквания.

При установяване на виновност на лицето, веднага се предприемат следните мерки в съответствие с нарушението:

* Преустановяване на свободен физически достъп до сградата или определени помещения;
* Преустановяване на съответния достъп в компютърната мрежа;
* Отнемане на съответните привилегии и активи (ако се налага).
* Предприемане на коригиращи действия за останалите служители, доставчици и външни страни;
* Процедира се по реда на нормативната уредба за дисциплинарно нарушение.

### 10.3. Инфраструктура и оборудване, физически достъп (чл. 21, ал. 1 и чл. 26 от НМИМИС)

**10.3.1. Общи положения**

Наличното информационно и комуникационно оборудване/активи на ИАСАС е съвременно и подходящо за осигуряване на дейността и вътрешните ИТ услуги. Използваното оборудване включва: сървъри, мрежови устройства, компютърна техника и др. За намаляване на риска от неоторизиран достъп, устройствата са разположени в зони, които са физически и логически защитени в съответствие с класификацията на информацията, с която работят.

Изпълнителна агенция по сортоизпитване, апробация и семеконтрол осигурява физическа защита на информационните си активи чрез прилагане на адекватни мерки срещу заплахи от неоторизиран достъп до тях (описани в СП 6-7 "Физическа сигурност на информационните активи"). Мерките за защита са съобразени с нормативните актове, включват защита от пожар, наводнение, химическа и физическа промяна на въздуха и гарантират наличността, интегритета и конфиденциалността на информационните активи.

За да се гарантира ефикасността на приложените мерки за сигурност, отговорни лица от Агенцията извършват подходящо наблюдение и контрол върху тях.

**10.3.2. Ред за осигуряване на оборудване**

Необходимостта от закупуване на информационно и комуникационно оборудване/активи се определя в зависимост от наличието и състоянието на съществуващото такова, изискванията на дейностите, както и контрол на характеристиките на вътрешните ИТ услуги.

**10.3.3. Поддържане на оборудването**

Поддържането на информационното и комуникационно оборудване се извършва съгласно техническата му документация.

Отговорник за поддръжката на оборудването е Системният администратор, като в изпълнение на тези дейности може да бъде подпомаган и от други специалисти на ИАСАС или външни доставчици. При необходимост от ремонт, същият се извършва от отговорните лица или от външна организация по конкретно договаряне.

За намаляване на риска от инциденти, предизвикани от технически повреди, Системният администратор:

* осигурява климатико-механичните условия, указани от производителя;
* осъществява наблюдение на параметрите на условията по предходната точка;
* планира и провежда регулярна техническа профилактика на устройствата.

## XI. ИЗПЪЛНЕНИЕ НА ДЕЙНОСТИ ПО МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

### 11.1. Планиране на дейности и контрол

В Агенцията е разработена и внедрена Система за управление на базата на изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност. Системата за управление на мрежовата и информационна сигурност запазва достъпността, интегритета и конфиденциалността на информацията чрез прилагане на процес за управление на риска и дава увереност на заинтересованите страни, че рисковете се управляват по подходящ начин.

Във връзка с естеството на извършваната дейност, в ИАСАС е от съществено значение управлението на сигурността с цел предотвратяване загубата и изтичането на информация, както и за осигуряване на непрекъснатост на процесите.

Агенцията планира, внедрява и контролира процесите, необходими за отговаряне на изискванията за мрежовата и информационната сигурност, водейки се от одобрената от Изпълнителния директор документация от СУМИС.

### 11.2. Анализиране, оценяване и въздействие върху риска за мрежовата и информационна сигурност

Изпълнителна агенция по сортоизпитване, апробация и семеконтрол определя реда, компетенциите, отговорностите, както и методиката за оценяване на рисковете, свързани с мрежовата и информационна сигурност във ведомството.

Агенцията планира, внедрява и контролира процесите, необходими за анализиране, оценяване и въздействие върху риска за мрежовата и информационна сигурност в съответствие с изискванията на одобрената от Изпълнителния директор П 6-2 "Управление на рисковете за мрежовата и информационната сигурност". Оценяване на рисковете се извършва минимум веднъж годишно или при необходимост (напр. при осъществяване на съществени изменения) от СМИС и се документира във Ф 6-2.1 "Регистър на рисковете". При установени нива на риска над допустимата стойност (съгласно утвърдената Методология за оценяване на рисковете), СМИС изготвя "План за намаляване на неприемливите рискове", който е неразделна част от Ф 6-2.1.

## XII. ОЦЕНЯВАНЕ НА РАБОТНИТЕ ХАРАКТЕРИСТИКИ

### 12.1. Наблюдение и контрол

**12.1.1. Общи положения**

В настоящата точка се регламентира редът и отговорностите на служителите на ИАСАС за осъществяване на дейностите по наблюдение и контрол, необходими за осигуряване на съответствие на процесите за извършване на дейността с изискванията на НМИМИС.

В Агенцията се извършва периодично наблюдение и контрол на определени в документите от СУМИС параметри.

В документите от СУМИС за отделните дейности (процеси) са определени механизмите за планиране, проследяване на протичането и контрола на процесите, необходими за осигуряване на съответствие със заложените изисквания, както и подобряване на тяхната резултатност и на СУМИС.

**12.1.2. Дефиниране на параметрите, подлежащи на наблюдение и контрол**

СМИС обобщава процесите и мерките за контрол, свързани с управление на мрежовата и информационна сигурност, които подлежат на наблюдение и изготвя Ф 4-1.1 "План за наблюдение и измерване", който се утвърждава от Изпълнителния директор.

Определянето на обектите и дейностите по наблюдение и контрол на управлението на мрежовата и информационна сигурност е вследствие на извършеното анализиране и оценяване на риска и изпълнението на "План за намаляване на неприемливите рискове" (част от Ф 6-2.1 "Регистър на рисковете").

За осигуряване на валидни резултати за целите на анализа и оценяването, определените методи за наблюдение и контрол се документират във Ф 4-1.1 "План за наблюдение и измерване".

Обектите и методите на наблюдение и контрол се избират така, че да се осигури:

* че са взети предвид анализираните и оценени рискове за мрежовата и информационна сигурност;
* че избраните мерки за контрол са в състояние да постигнат очаквания контрол върху риска/опасността, за които са предназначени;
* че мерките на организацията за непрекъснатост на дейността остават ефикасни, съответстват на предназначението си и са актуални.

Резултатите от наблюдението се отразяват във Ф 4-1.2 "Контролен лист" или в друг документ от СУМИС от СМИС или от външна организация, наета да извършва наблюдение.

**12.1.3. Анализ на данните и оценяване на резултатите**

Данните, събрани при наблюдението и упражнения контрол, се обобщават, анализират и оценяват при периодичност, определена във Ф 4-1.1 "План за наблюдение и измерване", но минимум веднъж годишно.

Получените при анализа резултати се използват от СМИС за оценяване на:

* резултатността и ефикасността на СУМИС;
* ефикасността на внедреното планиране;
* ефикасността на предприетите действия за овладяване на рисковете;
* необходимостта от подобряване на СУМИС.

Ф 4-1.1 "План за наблюдение и измерване" се преразглежда и при необходимост се актуализира от СМИС.

### 12.2. Вътрешни и външни одити, проверки, анкети (чл. 35, чл. 36 и чл. 37 от НМИМИС)

**12.2.1. Вътрешни одити на Системата за управление на мрежовата и информационна сигурност**

Вътрешните одити в Изпълнителна агенция по сортоизпитване, апробация и семеконтрол са предназначени за:

* преглед и проверка на мрежовата и информационна сигурност;
* преглед и проверка на адекватността на предприетите мерки;
* определянето на степента на съответствие на СУМИС с изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност;
* предприемане на действия за подобряване на нивото на защита на мрежовата и информационна сигурност.

Вътрешните одити се извършват от служители на агенцията, компетентни да извършват тези дейности, или от привлечени за целта външни специалисти.

Вътрешен одит по мрежова и информационна сигурност се извършва минимум един път в годината, като резултатите от него се документират в доклад, класифициран с TLP-AMBER.

Вътрешните одити се извършват съгласно регламентираните правила в П 4-2 "Вътрешни одити".

Съгласно чл. 16, ал. 5 от Закона за киберсигурност ИАСАС следва да предоставя, при поискване, резултатите от извършените одити на съответния национален компетентен орган – като информация, необходима за оценка на мрежовата и информационната си сигурност и/или като доказателство за ефективно изпълнение на препоръките и изискванията, касаещи мрежовата и информационната сигурност.

**12.2.2. Външен одит от втора страна**

Одит от Втора страна се извършва от организация/заинтересована страна, за да се оцени възможността на ИАСАС да удовлетворява определени изисквания за мрежова и информационна сигурност.

Целта е да се събере необходимата информация за СУМИС, за да се гарантира, че определените и декларирани от ИАСАС изисквания по отношение на мрежовата и информационна сигурност се изпълняват и ще продължават да се изпълняват.

Обхватът и дълбочината на одита от втора страна зависят от предназначението на оценката и от това дали тя ще служи за първоначално одобрение или има надзорно-инспекционна цел. Външният одит се извършва или от екип на заинтересованата страна, или от външна организация (с компетентни експерти), или се работи в смесен екип.

Външният одит от втора страна се планира според предназначението на оценката – кои обекти се одитират, с какъв метод, от кого, какво сътрудничество е нужно. Резултатите от одита се представят чрез доклад, който съдържа констатации, оценки и препоръки (или предписания), съгласно плана за одит.

**12.2.3. Външен одит от трета страна**

Одит от трета страна се извършва за определяне на степента на съответствие на Системата за управление на мрежовата и информационна сигурност на ИАСАС с критериите на одита (които може да са нормативни и стандартизационни изисквания, изисквания на СУМИС или др. специфични изисквания и цели на ръководството на учреждението).

Одитът от трета страна се изпълнява с цел сертифициране на ИАСАС за съответствие с действащи национални, европейски и/или международни стандарти и/или нормативни изисквания. Провежда се от квалифицирани одитори от избрана сертифицираща организация, притежаваща валидна акредитация.

Провеждането на всеки одит от трета страна се извършва съобразно предварително получен план от сертифициращата организация. В съответствие с плана, Изпълнителният директор издава заповед за провеждане на одита от трета страна. В заповедта се уточняват звената/ дирекциите/ отделите, които подлежат на проверка, периодите, времетраенето, придружаващите външните одитори лица, като към нея се прилага и планът за провеждане на одита.

След всеки одит от трета страна, в ИАСАС се изготвя доклад за резултатите от външния одит.

В случаите на констатирани несъответствия от одити от трета страна, се процедира съгласно указанията и препоръките на организацията, констатирала несъответствието (контролен орган, сертифицираща организация).

**12.2.4.** **Проверките** се осъществяват от председателя на Държавна агенция "Електронно управление" на основание чл. 12, т. 6 от Закона за киберсигурност. Те се извършват съгласно стандарт БДС EN ISO 19011 "Указания за извършване на одит на системи за управление", стандарт БДС EN ISO/IEC 17020 "Оценяване на съответствието" и НМИМИС. Докладът с резултатите от проверката и оценено съответствие с одобрената методика за извършване на оценка на мрежовата и информационната сигурност се класифицира с TLP-AMBER.

**12.2.5. Анкетите** се извършват от националните компетентни органи на основание Закона за киберсигурност и имат за цел да съберат информация по конкретно изискване от НМИМИС. Попълнените анкети са с класификация TLP-AMBER.

## XIII. ДЕЙСТВИЯ ЗА ПОДОБРЯВАНЕ

### 13.1. Несъответствие и коригиращо действие

Подобряването на нивото на защита на мрежовата и информационна сигурност в ИАСАС се постига чрез осъществяването на целенасочени коригиращи действия.

Документирането, изпълнението и анализът на коригиращите действия се осъществява от СМИС/друго определено за целта отговорно лице. Контролът на тези действия се осъществява от ръководни служители в Агенцията (Изпълнителен директор, упълномощени от него служители).

Необходимостта от провеждане на коригиращи действия може да възникне от:

* констатирани несъответствия спрямо изискванията на НМИМИС или на документите от СУМИС, установени и докладвани от служители на агенцията;
* вътрешни и/или външни одити, проверки;
* наблюдение и контрол на процесите;
* взаимоотношения с други ведомства, доставчици и трети страни;
* предписания/санкции от страна на контролни органи;
* други.

В резултат на регистрираното несъответствие, при необходимост и по решение на ръководството на ИАСАС, се извършва актуализация на оценените рискове и се разглежда възможността за внасяне на промени в Системата за управление на мрежовата и информационна сигурност.

Редът за управление на несъответствия и извършване на корекции и коригиращи действия е описан по-подробно в П 4-3 "Корекции и коригиращи действия".

## ТАБЛИЦА С НАПРАВЕНИТЕ ИЗМЕНЕНИЯ

| **Версия №** | **Дата** | **Страница №** | **Същност на изменението** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |