TLP: WHITE NOI-001-PO

ПОЛИТИКА

ПО МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

ИСТОРИЯ НА ВЕРСИИТЕ

Версия	*Заповед №/дата*	*Описание на промените*	*Утвърдил*
1	***№1016-40-630/18.12.2015*** г.	Начална редакция	Весела Караиванова Подуправител на НОИ
2	***№1016-40-317/18.03.2021*** г.	Привеждане в съответствие с НМИМИС	Ивайло Иванов Управител на НОИ
3	***№1016-40-1012/ 17.09.2021 г.***	Актуализация на документа	Ивайло Иванов Управител на НОИ

ПРЕДНАЗНАЧЕНИЕ

Документът е предназначен да изрази официално намеренията и насоките за информационната сигурност в Националния осигурителен институт.

С Политиката по мрежова и информационна сигурност Националния осигурителен институт цели да се приобщи към основните ценности и принципи, постановени в *Насоките за сигурността на информационните системи и мрежи - Към култура на сигурност на Организацията за икономическо сътрудничество и развитие*.

- **Осведоменост**

Персоналът, осигурените лица, осигурителите, доставчиците, подизпълнителите и всички останали участници в обмена на информация следва да са наясно с необходимостта от сигурност на информационните системи и мрежи и да допринасят за повишаване на сигурността.

- **Отговорност**

Всички участници в информационния обмен са отговорни за сигурността на информационните системи и мрежи.

- **Реакция**

Всички участници в информационния обмен трябва да действат своевременно и да си сътрудничат за предотвратяване, разкриване и реагиране на инциденти по сигурността.

- **Оценка на риска**

Рисковете за информационната сигурност следва да бъдат оценявани.

- **Проектиране и внедряване на сигурността**

Сигурността следва да бъде включвана като съществен елемент в информационните системи и мрежи.

- **Управление на сигурността**

Сигурността следва да бъде постигана чрез прилагането на цялостен подход за управление.

- **Преоценка**

Сигурността на информационните системи и мрежи следва да бъде преразглеждана и преоценявана минимум веднъж годишно, като при необходимост бъдат внасяни изменения в Политиката, процедурите, практиките и мерките.

Реализирането на тази *Политика* е от особена важност за осигуряването на правилното и непрекъсваемото осъществяване на предлаганите и предоставяните информационни услуги.

С *Политиката NOI-001-PO по мрежова и информационна сигурност* Националният осигурителен институт цели да постигне:

- защита на информацията от неразрешен достъп;
- запазване на поверителността на информацията;
- недопускане разкриване на информация на неоправомощени лица, дори в следствие на небрежност или на случайна грешка;
- запазване на информацията непокътната от неразрешени промени;
- предоставяне на информацията на оправомощените лица винаги, когато им потрябва;
- по-точно спазване на нормативната уредба;
- разработване, прилагане и практическа проверка на плановете за непрекъсваемост на сигурността;

- обучение по информационната сигурност на всички участници в информационния обмен;
- документиране и проучване на всяко съмнение за нарушение на информационната сигурност.

ПРИЛОЖИМОСТ

Документът се прилага в целия *Обхват* NOI-004-SC на Системата за управление сигурността на информацията (СУСИ) в Националния осигурителен институт.

С тази *Политика* Националния осигурителен институт изразява своята решимост за въвеждане на цялостна система за предпазване на информацията и свързаните с нея активи от всякакви заплахи, както външни така и вътрешни, независимо от това дали са нарочни или неволни, в Централното управление и в Териториалните поделения на Националния осигурителен институт, както и навсякъде другаде, където се намира информация и свързаните с нея активи на Националния осигурителен институт.

Целият персонал на Националния осигурителен институт е отговорен за прилагането на тази *Политика* в ежедневната си работа.

Висшето ръководство се ангажира да осигурява необходимите ресурси и ще подпомага усилията на всеки участник в информационния обмен за постигането на тази *Политика*.

ТЕРМИНИ И СЪКРАЩЕНИЯ

Термин	***Описание***
Политика	намеренията и насоките на една организация, които са официално изразени от нейното висше ръководство
Организация	лице или група хора, които имат свои функции с отговорности, правомощия и взаимоотношения за постигане на своите цели
Висше ръководство	лице или група от хора, които насочват и контролират една организация на най-високо равнище

СЪДЪРЖАНИЕ

1 ОСНОВНИ НАПРАВЛЕНИЯ

Основните направления на информационната сигурност, в които тази *Политика* ще търси реализация са:

- предпазване на информацията, явяваща се собственост на осигурените лица, осигурителите или на други трети лица;
- предпазване на личните данни;
- предпазване на информационните активи на Националния осигурителен институт;
- осигуряване на доверие сред всички заинтересовани страни за надеждността на управлението на информацията.

1.1 Стратегически и оперативни цели за мрежова и информационна сигурност

Стратегическите цели на НОИ за мрежова и информационна сигурност са обвързани със стратегическа цел 2 от стратегията за развитие на Националния осигурителен институт а именно „Повишаване на организационната ефективност и информационната сигурност“.

Подходът и дейностите за постигане на целта са свързани с:

- Усъвършенстване на информационната и технологична среда в НОИ;
- Осигуряване на надеждна защита на качеството на информацията и интегритета на данните;
- Осигуряване на надеждна защита на достъпа, качеството и интегритета на данните в Информационните системи на НОИ, съобразно нормативните изисквания;
- Осигуряване на резервираност на информационната система и план за непрекъсваемост.

2 ЗАДАЧИ

Управителят на НОИ организира изпълнението на следните задачи:

- Определяне на информацията и свързаните с нея активи, техните уязвимости и заплахите, на които те могат да бъдат изложени и точното оценяване на рисковете;
- Осигуряване на съответствие спрямо изискванията на:
  - Конституцията, законите, наредбите към тях и другите приложими нормативни актове;
  - сключените договорености с трети страни и приетите изисквания към информационната сигурност;
  - всички вътрешни правила на Националния осигурителен институт;
  - международните стандарти от фамилията ISO/IEC27xxx.
- Приемане на цели за информационна сигурност, в които да залегнат основните критерии за приемливост при оценяване на рисковете;
- Управление на рисковете за информационната сигурност в установените граници на приемливост;

- Контрол на дейността на Националния осигурителен институт с цел прилагането на тази *Политика* и регулярното отчитане на състоянието и изпълнението ѝ в хода на прегледа на СУСИ.

3 ОТГОВОРНОСТИ

Управителят на НОИ реализира тази *Политика* чрез въвеждане и прилагане на необходимите правила, които се документират в *Правилата*, *Процедурите*, *Правилниците, Инструкциите, Заповедите* и другите вътрешни актове на Националния осигурителен институт.

Пълномощията и отговорностите на управленските органи и позиции за определяне на политиките (цялостните намерения и насоки на дейност) на Националния осигурителен институт, насочени към осигуряване и поддържане на информационната сигурност, в съответствие с изискванията на изпълняваните дейности, стандарта ISO/IEC 27001 и приложимите законови и други нормативни актове са регламентирани в съответните процедури и включват:

- **Съвет по информационна сигурност** – изпълнява главната функция по ръководството и контрола на СУСИ във Ведомството.
- **Отговорници по информационна сигурност (ОИС) -** отговарят всички служители, контрагенти и други заинтересовани лица, да бъдат напълно информирани по отношение на задълженията и отговорностите, включени в процедурите и инструкциите по отношение на информационната сигурност. Организират провеждането и документирането на периодичните проверки и тестове за сигурност на системите. Докладват на Прегледите от ръководството за състоянието на информационната сигурност в организацията.
- **Директори на дирекции -** носят отговорност по отношение на данните и другите информационни ресурси, използвани при дейностите, които се осъществяват под тяхното наблюдение и контрол, за да се гарантира, че те са адекватно защитени, а също така се спазват приложимите указания, процедури и механизми при изпълнението на съответните дейности. Притежават правомощия за инициатива за промени по отношение на действащата СУСИ в организацията.
- **Системни администратори** – отговарят за инсталацията, конфигурацията и администрирането на инфраструктурата на публични ключове, както и за

регистрацията и създаването на удостоверения; отговарят за ежедневната работа на системата за издаване на удостоверения, като извършват редовно процедури по архивиране, създаване на резервни копия на информация и възстановяване информационни системи.

- **Всички служители** - служителите, вкл. временно наетите, посетителите, доставчици и подизпълнители, са длъжни да спазват указанията, процедурите и механизмите за информационна сигурност и активно да участват в опазването на информационните активи/ресурси на НОИ. Те не трябва да имат достъп и да боравят с информационните активи без да имат съответните пълномощия и са длъжни да докладват за нарушения по отношение на сигурността на отговорните лица.

Всички участници в информационния обмен са длъжни:

- да спазват правилата, указани в документацията на СУСИ и другите вътрешни актове на Националния осигурителен институт;
- да съдействат с личен принос за осъществяването на тази *Политика*;
- да докладват за наблюдавани слабости в информационната сигурност.

По всички въпроси относно тази *Политика* заинтересованите лица следва да се обръщат към Управителя, чиито разяснения и указания са задължителни за спазване при осъществяване на информационния обмен с Националния осигурителен институт.

4 ПОЛИТИКА ПО МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

За осъществяването на тази *Политика* са разработени и се прилагат регламенти, включващи:

4.1 Оценка на риска

Оценката на риска се прилага за всеки актив на организацията или извън нея, обхванат от споразумение с трета страна. Оценката на риска се прилага към цялата информационна система и включва приложения, сървъри, мрежата, и всеки процес или процедура чрез които системата се администрира и/или поддържа. Във Ведомството е разработена Стратегия за оценка на риска.

4.2 Вътрешна организация на информационната сигурност

Висшето ръководство на НОИ е разработило, внедрило и прилага политики за координиране на цялата дейност в организацията по внедряването и поддържането на мерките за защита.

4.3 Управление на активите

Ръководството на НОИ е разработило, утвърдило и приложило регламенти, отнасящи се до всички служители, отговорни лица, включително и персонал на трети страни и се прилага по отношение на цялото информационно оборудване, собственост или използвано от Националния осигурителен институт.

Регламентът за използване на активите цели не да налага ограничения, противоречащи на установената ведомствена култура на откритост и доверие, а да защитава служителите на НОИ, всички контрагенти и заинтересовани страни, както и самата Организация от незаконни и увреждащи действия, извършени предумишлено или несъзнателно.

4.4 Управление на човешките ресурси

Човешките ресурси са основен елемент от дейностите, свързани с управление на информационната сигурност. В НОИ са разработени и въведени регламенти, насочени към осъзнаване на необходимостта от осигуряване на информационната сигурност чрез адекватно дефиниране на отговорности и обучение.

4.5 Управление на физическата сигурност и сигурност на заобикалящата среда

В Националния осигурителен институт са разработени и въведени регламенти, насочени към защита на средствата за обработка и съхранение на информацията чрез определяне на граници на физическа сигурност и организация на зони за сигурност.

4.6 Контрол на достъпа

Въведените в НОИ регламенти за контрол на достъпа са базирани на принципите „необходимо да знае” или „необходимо да се ограничи”, „всеки достъп, който не е изрично разрешен е забранен” и минимизиране на привилегиите.

4.7 Разработване, внедряване и поддържане на информационните системи

Въведените регламенти за разработване, внедряване, изменение и поддържане на информационните системи са базирани на принципа на превантивната оценка на риска от измененията, включително ъпгрейд на съществуващи и внедряване на нови елементи от

системата, разделение на средата за изпитване от действащата информационна система и планирана поддръжка на цялата информационна система.

4.8 Управление на инциденти и подобряване на мрежовата и информационната сигурност

С цел намаляване на риска и произтичащите от появата на инциденти разходи, Ведомството е разработило и внедрило подходящи мерки за управление на инциденти, насочени към разработване и внедряване на правила, процедури и средства за ефективно третиране на слабостите и пробивите, свързани с информационната сигурност. Мерките обхващат непрекъснато наблюдение, реагиране, оценяване, подобряване и цялостно управление на слабостите и инцидентите.

4.9 Осигуряване на непрекъснатостта на процесите

Ръководството на НОИ разбира необходимостта от планиране непрекъснатостта на процесите. То осъзнава, че има значителен риск за неговите критични системи при потенциални и неочаквани разрушителни събития. Увеличаващото се развитие на процеси, базирани на технологии и силната зависимост от информационните технологии е основание за създаване на план за непрекъснатост на работа.