ПРАВИЛА
за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност

Глава първа

ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Настоящите правила определят минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методите за управление на риска за тяхната сигурност.

(2) Настоящите правила определят критериите за определяне на въздействието като значително на инциденти, свързани със сигурността на обществените електронни съобщителни мрежи и услуги, както и изискваната информация, формата и начина за уведомяване на Комисията за регулиране на съобщенията, наричана по-нататък „комисията“, за инцидентите, свързани със сигурността, които са оказали значително въздействие върху функционирането на мрежите или услугите.

Чл. 2. Правилата се прилагат спрямо следните обществени електронни съобщителни мрежи:

1. фиксирани мрежи;
2. мобилни мрежи;
3. мрежи за разпространение на радио- и телевизионни програми.

Чл. 3. Правилата се прилагат спрямо следните обществени електронни съобщителни услуги:

1. мобилна гласова услуга;
2. мобилен достъп до интернет;
3. фиксирана гласова услуга;
4. фиксиран достъп до интернет;
5. междуличностна съобщителна услуга без номер;
6. услуги за разпространение на радио- и телевизионни програми;
7. услуги, при които се използва комуникация Машина – Машина;
8. други услуги за пренос на сигнали.

Чл. 4. (1) По отношение на междуличностните съобщителни услуги без номера настоящите правила се прилагат спрямо доставчика на съответната услуга. Разпоредбите на настоящите правила, които се отнасят до междуличностните съобщителни услуги без номера, не се прилагат към предприятията, предоставящи обществените електронни съобщителни мрежи, чрез които се предоставят услугите.

(2) Изискванията на правилата към услугите, при които се използва комуникация Машина – Машина, се отнасят до предприятията, предоставящи съответната услуга.

Чл. 5. Правилата се прилагат при предоставяне на електронните съобщителни мрежи или услуги, като изискванията за сигурност се планират на етапа на проектирането им.

Глава втора

МЕТОДИ ЗА УПРАВЛЕНИЕ НА РИСКА

Раздел I

Оценка на риска

Чл. 6. (1) Предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, изготвят оценка на риска за сигурността на предоставяните от тях мрежи или услуги.

(2) Оценката на риска се документира, като се определят потенциалните заплахи за обществените електронни съобщителни мрежи и/или услуги, вероятността за реализиране на дадена заплаха и отговорностите на лицата, извършващи оценката.

Чл. 7. (1) При извършване оценката на риска предприятията изготвят пълен списък с активи на предприятието, в това число активи на „трети страни“, които при компрометиране или отпадане могат да предизвикат инцидент, свързан със сигурността на мрежата и/или услугата.

(2) При изготвянето на списъка с активите на мрежите и/или услугите се отчитат системите и процесите, необходими за предоставянето на електронните съобщителни мрежи и/или услуги.

(3) При изготвяне на списък с активите се включват всички служители на предприятието, доставчиците и потребителите на „трети страни“, които имат ключови роли при предоставянето на електронните съобщителни мрежи и/или услуги.

(4) При изготвяне на списъка с активите като „трети страни“ се отчитат всички страни, с които предприятието взаимодейства при предоставянето на електронните съобщителни мрежи и/или услуги.

(5) Под „трети страни“ не се разбират ползватели на услугите и държавни или регулаторни органи.

Чл. 8. Въз основа на оценката на риска се определя нивото на сигурност, на което обществените електронни съобщителни мрежи или услуги трябва да издържат.

Раздел II

Технически и организационни мерки за намаляване на риска

Чл. 9. Предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, изготвят план за намаляване на риска, който да включва най-малко технически и организационни мерки за намаляване на риска, срок за прилагане на мерките и отговорните лица.

Чл. 10. (1) При избора на подходящи технически и организационни мерки за сигурност, в зависимост от нивото на сигурност, предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, използват приложение № 1. Предприятията могат да прилагат и мерки за сигурност в допълнение към посочените в приложение № 1.

(2) Техническите и организационни мерки за сигурност в приложение № 1 са групирани на три нива на сигурност, като всяко следващо ниво на сигурност включва изискванията на предходното.

Чл. 11. (1) Предприятията, предоставящи обществени мобилни електронни съобщителни мрежи, предприемат минимум трето ниво на сигурност от приложение № 1.

(2) Предприятията, предоставящи обществени фиксирани мрежи и/или мрежи за разпространение на радио- и телевизионни програми, предприемат минимум първо ниво на сигурност от приложение № 1.

Чл. 12. (1) Предприятията, предоставящи обществени електронни съобщителни услуги по чл. 3, т. 1, 2 и 7, предприемат като минимум трето ниво на сигурност от приложение № 1.

(2) Предприятията, предоставящи обществени електронни съобщителни услуги по чл. 3, т. 3, 4 и 6 с над 50 000 ползватели, предприемат минимум трето ниво на сигурност от приложение № 1.

(3) Предприятията, предоставящи обществени електронни съобщителни услуги по чл. 3, т. 3, 4 и 6 с по-малко от 50 000 ползватели, предприемат като минимум първо ниво на сигурност от приложение № 1.

(4) Предприятията, предоставящи обществени електронни съобщителни услуги съгласно чл. 3, т. 5, приемат всички подходящи мерки от приложение № 1. Неподходящи за тях са мерките, свързани с обществените електронни съобщителни мрежи, чрез които се предоставят услугите.

Чл. 13. (1) При сключване на договор с „трети страни“ – доставчици на оборудване и управлявани услуги, предприятията, предоставящи обществени мобилни електронни съобщителни мрежи и/или обществени електронни съобщителни услуги по чл. 3, т. 1, 2 и 7:

1. трябва да предвидят подходящи изисквания за сигурност за:

а) гарантиране на качеството на предлаганите продукти и услуги;

б) оперативна съвместимост на предлаганите продукти и съответствието им с приложими международни стандарти;

в) сигурност на информацията; изисквания, свързани с достъпа на представители на доставчиците на оборудване и управлявани услуги до информация и активи на предприятието;

г) адекватни мерки за защита на личните данни;

д) последици при неспазване на изискванията за сигурност на информацията;

е) условия за гаранционна и/или възложена извънгаранционна поддръжка, включително по отношение на актуализациите на програмите за осигуряване на сигурността на мрежата;

ж) за взаимодействие в случай на възникване на инцидент, който най-малко включва: контактни точки, начин за докладване, време за реакция, време за възстановяване на работата, условия за затваряне на инцидент;

2. трябва да отчетат в най-голяма степен възможността да предвидят подходящи изисквания за сигурност за:

а) обхват на контрола на „трети страни“ върху информацията на предприятието за доказване, че третата страна също прилага адекватни мерки за сигурност, включително клаузи за доказването на прилагането на тези мерки чрез документи и/или провеждане на одити;

б) наличие на център/екип за поддръжка на услуги и/или продукти на територията на страна/държава – членка на ЕС, с оглед ескалиране на проблеми на ниво доставчик;

в) за прозрачност на веригата на доставките; третата страна трябва да е способна да докаже произхода на предлагания ресурс/услуга и неговата сигурност;

г) отговорност при неспазване на договорените срокове, количество и/или качество на стоката или услугата, което може да създаде съществен риск за постигане на целите на сигурността;

д) осигуряване на информация за извършването на редовни одити и оценка на риска на веригата на доставки.

(2) Предприятието определя служител, отговарящ за спазване на изискванията по ал. 1 и параметрите на нивото на обслужване.

(3) Предприятието изготвя и прилага мерки за отстраняване на последиците в случай на неспазване на уговорените дейности и клаузи с „третата страна“.

(4) Предприятията по ал. 1 предвиждат парични санкции и когато е приложимо, разваляне на договорите при неизпълнение на договорни задължения от „трети страни“ – доставчици на оборудване, когато би могло да доведе до неизпълнение на задължения по настоящите правила.

Раздел III
Одити

Чл. 14. (1) Одитът на сигурността е периодичен или след възникване на инцидент.

(2) Одитът на сигурността може да е вътрешен, извършен от квалифициран независим орган или от друг компетентен орган.

(3) Одитът на сигурността се извършва с преглед на документи и с разговор с отговорните служители.

Чл. 15. Всяко предприятие, предоставящо обществени електронни съобщителни мрежи и/или услуги, е длъжно да извършва поне вътрешен периодичен одит на всеки три години.

Чл. 16. При извършване на одит за съответствие на техническите и организационни мерки от приложение № 1 се използва колона „доказателства за изпълнение“ от същото приложение.

Чл. 17. (1) След възникване на инцидент със значително въздействие се извършва вътрешна проверка или вътрешен одит за установяване причините за възникване на инцидента.

(2) След анализ на причините предприятието предприема мерки за намаляване на риска.

Чл. 18. (1) Резултатите от вътрешната проверка могат да се изискат от комисията.

(2) Предприетите мерки от предприятията в изпълнение на този раздел не изключват упражняването на правомощията на комисията по чл. 243в от Закона за електронните съобщения.

Глава трета

ИНЦИДЕНТИ, СВЪРЗАНИ СЪС СИГУРНОСТТА

Раздел I

Общи положения

Чл. 19. Инцидентите, свързани със сигурността, са всички инциденти, които компрометират наличността, автентичността, целостта или поверителността на мрежите и услугите, на съхранените, пренесените или обработените данни или на свързаните услуги, които тези електронни съобщителни мрежи или услуги предоставят или до които осигуряват достъп.

Чл. 20. Причините за възникване на инциденти, свързани със сигурността, са:

1. човешка грешка – инциденти, причинени от служители на предприятието, включително вследствие на неправилна конфигурация или неправилно разполагане на техническото оборудване, платформи, програмни продукти, архиви и бази данни и неправилно прилагане на процедурите по управление на технически ресурси и инциденти;

2. повреди в техническото оборудване и програмните продукти;

3. природни бедствия – включва тежки климатични условия, наводнения, пожари, земетресения, свлачища и др.;

4. злонамерени атаки – придобиване на неоторизиран физически или логически достъп до мрежи, системи, приложения, данни или други информационни ресурси от лица или програмни продукти, което може да е резултат на целенасочени вътрешни или външни атаки;

5. външни причини – включва човешки грешки, неправилно прилагане на процедури и повреди, причинени от „трети страни“.

Раздел II

Инцидент, оказал значително въздействие

Чл. 21. Инцидентите, оказали значително въздействие, които предприятията, предоставящи обществени електронни съобщителни мрежи или услуги, докладват в изпълнение на чл. 243б, ал. 1 от ЗЕС, отговарят на един или няколко количествени и/или качествени критерии.

Чл. 22. (1) Количествените критерии за инциденти, свързани с наличността на услугите, чието въздействие изпълнява едновременно „продължителност на инцидента“ и „брой ползватели, засегнати от инцидента“, са определени съгласно приложение № 2.

(2) Инциденти са и тези, при които продължителността на инцидента и броят на засегнатите ползватели не достигат заложените в приложение № 2 критерии, но при неколкократно повторение в рамките на 30 дни сумарната продължителност и общият брой на засегнатите ползватели оказват въздействие, определено в приложение № 2.

Чл. 23. Количественият критерий за инцидент, свързан с автентичността, целостта или поверителността, е съгласно приложение № 2.

Чл. 24. Качествени критерии за инциденти:

1. инцидентът е трансграничен;

2. инцидентът обхваща площ на една административна област;

3. инцидентът обхваща цялата територия на гр. София;

4. инцидентът обхваща труднодостъпни райони;

5. инцидентът засяга функционирането на мрежите и/или услугите на няколко предприятия;

6. инцидентът засяга достъпа към единния европейски номер за спешни повиквания 112 и/или националните номера за спешни повиквания;

7. инцидентът засяга системите за предупреждение на населението.

Раздел III

Информация, форма и начин за уведомяване

Чл. 25. Информацията и формата за уведомяване за инциденти са определени в приложение № 3.

Чл. 26. (1) Първоначалното уведомление се подава до 24 часа след възникване на инцидент.

(2) При първоначалното уведомяване не е необходимо да се подава пълната информация за въздействие на инцидента.

Чл. 27. (1) Окончателното уведомление се подава след приключване на инцидента, свързан със сигурността.

(2) В случай че в рамките на 24 часа след възникване инцидентът е приключил, предприятието може да изпрати едно уведомление с попълнена пълната информация за инцидента.

ДОПЪЛНИТЕЛНА РАЗПОРЕДБА

§ 1. По смисъла на тези правила:

1. „Автентичност“ е свойството на данните (трафични и за ползвателите на услугата), че са тези, за които се представят.

2. „Актив“ – всяко нещо, което има стойност за предприятието, като:

а) физически, например сгради, оборудване, електрическо захранване и др.;

б) програмни продукти, в това число инсталирани на оборудването, програми за наблюдение и управление на мрежите и/или услугите;

в) данни – например регистри, бази данни;

г) услуги – предоставяните от предприятието услуги и на свързаните услуги;

д) персонал и неговата квалификация, умения и опит, и

е) нематериални ценности като например репутация на предприятието.

3. „Наличност“ е свойството на електронните съобщителни мрежи или услуги за достъпност и използваемост при поискване.

4. „Ниво на сигурност“ – способността на електронните съобщителни мрежи и/или услуги да издържат при определено ниво на действия, които компрометират наличността, автентичността, целостта или поверителността на тези мрежи и услуги, на съхранените, пренесените или обработените данни или на свързаните услуги, които

тези електронни съобщителни мрежи или услуги предоставят или до които осигуряват достъп.

5. „Поверителност“ е свойството на данните (трафични и за ползвателите на услугата) да не стават достъпни или да не се разкриват от неоторизирани лица, системи, процеси.

6. „Цялост“ е свойството на данните (трафични и за ползвателите на услугата) за точност и пълнота.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 2. Настоящите правила са приети с Решение № 162 от 19.05.2022 г. на Комисията за регулиране на съобщенията на основание чл. 243, ал. 3, изр. първо от Закона за електронните съобщения.

§ 3. Разпоредбите на глава втора влизат в сила една година след обнародване на настоящите правила.

§ 4. Раздел II и приложение № 1 към чл. 8, ал. 2 от Общите изисквания при осъществяване на обществени електронни съобщения се отменят (ДВ, бр. 108 от 2021 г.).

Приложение № 1 към чл. 10, ал. 1

Технически и организационни мерки за сигурност

Област на сигурност 1: Управление и ръководене на риска

Цел на сигурност 01: Политика за сигурност на информацията

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Задаване на високо ниво на политика за сигурност, насочена към сигурността на мрежите и услугите. б) Информиране на ключовия персонал за политиката за сигурност.	1. Документирана политика за сигурност, включително за мрежи и услуги по обхват, критични активи, които ги поддържат, и цели за сигурност. 2. Ключовият персонал е запознат с политиката за сигурност и нейните цели (интервю).
2	в) Задаване на подробни политики за сигурността на информацията за критични активи и бизнес процеси. г) Запознаване на целия персонал относно политиката за сигурност и какво означава тя за тяхната работа. д) Преглед на политиката за сигурност след инциденти.	3. Документирани политики за сигурността на информацията, одобрени от ръководството, включително приложими законови и регулаторни разпоредби, достъпни за персонала. 4. Персоналът е наясно с политиката за сигурност на информацията и какво означава тя за тяхната работа (интервю). 5. Преглед на коментарите или регистрите на промените на политиката.
3	е) Периодичен преглед на политиката за сигурност на информацията и вземане предвид на нарушенията, изключенията,	6. Политиките за информационна сигурност са актуални и одобрени от висшето ръководство.

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
	предишни инциденти и тестове/тренировки, и инциденти, засягащи други (подобни) доставчици в сектора.	7. Регистри на изключенията от политиката, одобрени от съответните роли. 8. Документиране на процеса на преглед, като се вземат предвид промените и миналите инциденти.

Област на сигурност 1: Управление и ръководене на риска
Цел на сигурност 02: Управление и ръководене на риска

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Изготвяне на списък с основните рискове за мрежите и услугите, отчитайки основните заплахи за критичните активи. б) Запознаване на ключовия персонал с основните рискове и начините за намаляването им.	1. Списък на основните рискове, описани на високо ниво, включително на основните заплахи и тяхното потенциално въздействие върху сигурността на мрежите и услугите. 2. Ключовият персонал знае основните рискове (интервю).
2	в) Създаване на методология и/или инструменти за управление на риска, базирани на индустриални стандарти. г) Уверение, че ключовият персонал използва методологията и инструментите за управление на риска. д) Преглед на оценките на риска след промени и инциденти. е) Уверение, че остатъчните рискове са приети от ръководството.	3. Документирани методология и/или инструменти за управление на риска. 4. Насоки за персонала за оценка на рисковете. 5. Списък с рисковете и доказателства за актуализации/прегледи. 6. Преглед на коментари или регистрите на промените за оценка на риска. 7. Одобрение на остатъчните рискове от ръководството.
3	ж) Преглед на методологията и/или инструментите за управление на риска, като се вземат предвид промени и минали инциденти.	8. Документация за процеса на преглед и актуализации на методологията и/или инструментите за управление на риска.

Област на сигурност 1: Управление и ръководене на риска
Цел на сигурност 03: Роли и отговорности по сигурността

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Разпределение на ролите и отговорностите по сигурността на персонала.	1. Списък с ролите по сигурността (служител по сигурността на информацията, длъжностно лице по защита на данните, ръководител по непрекъснатостта на дейностите и т.н.), кой ги

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
	б) Уверение, че ролите по сигурността са достъпни в случай на инцидент.	заема и данни за контакт.
2	в) Персоналът е назначен официално на длъжност, свързана с роля по сигурността. г) Уведомяване на персонала за ролите по сигурността в организацията и кога трябва да бъдат потърсени.	2. Списък на назначенията (главен служител по сигурността на информацията, длъжностно лице по защита на данните и т.н.) и описание на отговорностите и задачите за ролите по сигурността (главен служител по сигурността на информацията, длъжностно лице по защита на данните и т.н.). 3. Материали за персонала за осведоменост/разпространение, обясняващи ролите по сигурността и кога/как те трябва да бъдат потърсени.
3	д) Структурата на ролите и отговорностите по сигурността редовно се преразглеждат и преработват въз основа на промени и/или минали инциденти.	4. Актуална документация за структурата на назначенията и отговорностите на ролите по сигурността. 5. Документация за процеса на преглед, като се вземат предвид промените и миналите инциденти.

Област на сигурност 1: Управление и ръководене на риска

Цел на сигурност 04: Сигурност на зависимост от трети страни

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Включване на изисквания за сигурност в договорите с трети страни, включително за конфиденциалност и сигурен трансфер на информация.	1. Изрични изисквания за сигурност в договорите с трети страни, доставящи IT продукти и услуги, изнесени бизнес процеси, информационен център, кол центрове, взаимно свързване, споделени съоръжения и т.н.
2	б) Задаване на политика по сигурността за договори с трети страни. в) Уверение, че всички доставки на/поръчки на услуги/продукти от трети страни следват политиката. г) Преглед на политиката по сигурността за трети страни след инциденти или промени. д) Изискване за специфични стандарти за сигурност в процесите на трети страни	2. Документирана политика по сигурността за договори с трети страни. 3. Списък на договорите с трети страни. 4. Договорите за услуги на трети лица съдържат изисквания за сигурност в съответствие с политиката по сигурността за доставка.

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
	доставчици по време на доставката. е) Намаляване на остатъчните рискове, които не се разглеждат от третата страна.	5. Преглед на коментарите или промените в регистрите на политиката. 6. Договорите с доставчици на оборудване съдържат изисквания за спазване на добрите практики за сигурност и индустриални стандарти. 7. Остатъчните рискове, произтичащи от зависимост от трети страни, са изброени и намалени.
3	ж) Проследяване на инциденти на сигурността, свързани или причинени от трети страни. з) Периодичен преглед и актуализиране на политиката за сигурност за трети страни на редовни интервали, като се отчитат минали инциденти, промени и т.н.	8. Списък на инциденти на сигурността, свързани със или причинени от ангажимент с трети страни. 9. Документация на процеса на преглед на политиката.

Област на сигурност 2: Сигурност на човешките ресурси
Цел на сигурност 05: Проверка на миналото

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Проверка на професионалните препоръки на ключовия персонал (системни администратори, служители по сигурността, охрана и др.).	1. Документиране на проверките на професионалните препоръки за ключов персонал.
2	б) Извършване на проверки/филтриране за ключовия персонал, когато е необходимо и законово разрешено. в) Създаване на политика и процедура за проверка на миналото.	2. Политика и процедура за проверки/филтриране. 3. Насоки за персонала относно това кога/как да се извършват проверки.
3	г) Преглед и актуализиране на политиката/процедурите за проверка на миналото и проверки на препоръките на редовни интервали, като вземете предвид промените и миналите инциденти.	4. Преглед на коментарите или регистрите на промените на политиката/процедурите.

Област на сигурност 2: Сигурност на човешките ресурси
Цел на сигурност 06: Знания и обучения по сигурност

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Осигуряване на подходящо обучение и материали по въпросите на сигурността на ключовия персонал.	1. Ключовият персонал е преминал обучения и има достатъчно познания по сигурността (интервю).
2	б) Изпълнение на програма за обучение, като се провери, че ключовият персонал разполага с достатъчно и актуални познания за сигурността. в) Организиране на обучения и сесии за осведоменост на персонала по теми за сигурността, важни за организацията.	2. Персоналът участва в сесии за осведоменост по теми за сигурността. 3. Документирана програма за обучение за умения в сферата на сигурността, включително цели за различните роли и как да бъдат постигнати (например чрез обучение, повишаване на осведомеността и др.).
3	г) Периодичен преглед и актуализиране на програмата за обучение, като се отчитат промените и миналите инциденти. д) Проверка на знанията по сигурността на персонала.	4. Актуализирана програма за осведоменост и обучение по сигурността. 5. Резултати от тестове на знанията по сигурността на персонала. 6. Преглед на коментарите или регистрите на промените за програмата.

Област на сигурност 2: Сигурност на човешките ресурси

Цел на сигурност 07: Промяна на персонала

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) След промени в персонала да се отнемат правата за достъп, пропуск, оборудването и т.н., ако вече не са необходими или допустими. б) Информиране и обучаване на новия персонал за действащите политики и процедури.	1. Доказателства, че промените в персонала са последвани от отнемане на права за достъп, пропуск, оборудване и др. 2. Доказателства, че новите служители са били инструктирани и обучени в действащите политики и процедури.
2	в) Прилагане на политика/процедури за промени в персонала, като се взема предвид своевременното отнемане на права за достъп, пропуски и оборудване. г) Прилагане на политика/процедури за образоване и обучение на персонала в нови роли.	3. Документиране на процеса за промени в персонала, включително отговорности за ръководене на промените, описание на правата за достъп и притежание на активи по роли, процедури за инструктаж и обучение на персонала за нови роли. 4. Доказателство, че промените на персонала са извършени в съответствие с процеса и че правата за достъп са

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
		актуализирани своевременно (например контролни списъци).
3	д) Периодична проверка дали политиката/процедурите са ефективни. е) Преглед и оценка на политиката/процедурите за промени на персонала, като се вземат предвид промените или минали инциденти.	5. Доказателства за проверки на правата за достъп и т.н. 6. Актуални политика/процедури за управление на промените на персонала. 7. Преглед на коментарите или регистрите на промените.

Област на сигурност 2: Сигурност на човешките ресурси

Цел на сигурност 08: Справяне с нарушенията

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Персоналът да се държи отговорен за инциденти, свързани със сигурността, причинени от нарушения на политиките, например чрез трудовия договор.	1. Правила за персонала, включително отговорности, кодекс за поведение, нарушения на политики и други, възможно като част от трудови договори.
2	б) Създаване на процедури за нарушения на политиките от персонала.	2. Документация на процедурите, включително видове нарушения, които могат да бъдат предмет на дисциплинарни действия, и какви дисциплинарни действия могат да бъдат предприети.
3	в) Периодичен преглед и актуализиране на дисциплинарния процес въз основа на промени и минали инциденти.	3. Преглед на коментарите или регистрите на промените.

Област на сигурност 3: Сигурност на системите и съоръженията

Цел на сигурност 09: Физическа сигурност и сигурност на средата

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Предотвратяване на неоторизиран физически достъп до съоръжения и инфраструктура и създаване на адекватен контрол на средата за защита на активите на доставчика срещу неоторизиран достъп, кражба с взлом, пожар, наводнения и др.	1. Основно внедряване на мерки за физическа сигурност и контрол на средата, като ключалки на врати и шкафове, аларми за взлом, пожароизвестители, пожарогасители и др.
2	б) Внедряване на политика за мерки за физическа сигурност и контрол на средата.	2. Документирана политика за мерки за физическа сигурност и контрол на средата, включително описание на

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
	в) Внедряване на стандарти за физически контрол и контрол на средата. г) Прилагане на засилен контрол за физически достъп до критични активи.	съоръженията и системите. 3. Физически контрол и контрол на средата, като електронен контрол на входа и достъпа за одит, сегментиране на пространствата според нивата на упълномощаване, автоматизирани пожарогасители с халокарбонови газове и др. 4. Политиката включва списъци с критични активи и засилен физически контрол за достъп до тези активи.
3	д) Периодична оценка на ефективността на физическия контрол и контрола на средата. е) Преглед и актуализация на политиката относно мерките за физическа сигурност и контрол на средата, като се вземат предвид промените и миналите инциденти.	5. Актуална политика за мерки за физическа сигурност и контрол на средата. 6. Документация за оценка на контрола на средата, преглед на коментарите или регистрите на промените.

Област на сигурност 3: Сигурност на системите и съоръженията

Цел на сигурност 10: Сигурност на доставките

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Осигуряване на сигурност на критичните доставки.	1. Сигурността на критичните доставки е защитена по основен начин, например налично е резервно захранване и/или резервно гориво.
2	б) Прилагане на политика за сигурност на критичните доставки. в) Прилагане на индустриални стандарти за мерките за сигурност, за защита на критични доставки и поддържащи съоръжения (напр. пасивно охлаждане, автоматично рестартиране след прекъсване на захранването, акумулаторно резервно захранване, дизелови генератори, резервно гориво и др.).	2. Документирана политика за защита на критичните доставки, като електрическа енергия, гориво и други, описваща различни видове доставки и мерки за сигурност, защитаващи доставките. 3. Доказателство за индустриални стандартизирани мерки за защита на сигурността на критичните доставки.
3	г) Прилагане на най-съвременни мерки за сигурност за защита на критични доставки (като активно охлаждане, UP,	4. Доказателства за съвременни мерки за защита на сигурността на

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
	паралелно работещи генератори, Споразумение за ниво на обслужване (SLA) с компании за доставка на гориво, резервирано охлаждане и системи за резервно захранване). д) Регулярен преглед и актуализиране на политиката и процедурите за осигуряване на критични доставки, като се вземат предвид промените и миналите инциденти.	критични доставки. 5. Актуализирана политика за осигуряване на критичните доставки и спомагателни съоръжения, преглед на коментари и/или регистрите на промените.

Област на сигурност 3: Сигурност на системите и съоръженията

Цел на сигурност 11: Контрол на достъпа до мрежови и информационни системи

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Потребителите и системите имат уникални идентификатори и се удостоверяват преди достъп до услуги или системи. б) Прилагане на логически механизъм за контрол на достъпа за мрежови и информационни системи, за да се позволи само упълномощен достъп.	1. Регистрите за достъп показват уникални идентификатори за потребители и системи, когато им е предоставен или отказан достъп. 2. Преглед на методите за автентикация и контрол на достъпа за системи и потребители.
2	в) Прилагане на политика за защита на достъпа до мрежови и информационни системи, отнасящи се до например роли, права, отговорности и процедури за присвояване и отнемане на права за достъп. г) Избор на подходящи механизми за удостоверяване в зависимост от вида на достъпа. д) Наблюдението на достъпа до мрежови и информационни системи да има процес за одобряване на изключения и регистриране на нарушения на достъпа. е) Подсилване на контрола за отдалечен достъп до критични активи на мрежови и	3. Политика за контрол на достъпа, включително описание на роли, групи, права на достъп, процедури за предоставяне и отнемане на достъп. 4. Различни видове механизми за автентикация за различните видове достъп. 5. Регистър на нарушенията и изключенията на политиката за контрол на достъпа, одобрени от служителя по сигурността. 6. Правилата на минималните права и разделението на задълженията се документират и прилагат, където е уместно. 7. Отдалеченият достъп, от трети страни, до критични активи е сведен до минимум и е подложен на строг контрол

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
	информационни системи от трети страни.	на достъпа, включително съвременен контрол за автентикация, оторизация и одит, особено за привилегировани акаунти.
3	ж) Оценка на ефективността на политиките и процедурите за контрол на достъпа и въвеждане на кръстосани проверки на механизмите за контрол на достъпа. з) Политиката за контрол на достъпа и механизмите за контрол на достъпа се преразглеждат и при необходимост се ревизират.	8. Доклади за тестове (на сигурността) на механизмите за контрол на достъпа. 9. Инструменти за откриване на извънормалното използване на системи или поведение на системи (като системи за откриване на проникване и откриване на аномалии). 10. Регистри на системите за откриване на проникване и откриване на аномалии. 11. Актуализации на политиката за контрол на достъпа, преглед на коментари или регистрите на промените. 12. Документиран анализ на риска за прилагането на вписванията „(logging)“ и ограниченията. 13. Процедури, които гарантират, че контролът за достъп е в сила през цялото време и че се променя заедно с развитието на мрежата.

Област на сигурност 3: Сигурност на системите и съоръженията

Цел на сигурност 12: Цялост на мрежовите и информационните системи

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Уверяване, че софтуерът на мрежовите и информационните системи не е манипулиран или променян, например чрез контрол на входа и защитни стени. б) Проверка за злонамерен софтуер във (вътрешната) мрежа и информационните системи.	1. Софтуерът и данните в мрежовите и информационните системи са защитени с помощта на контрол на входа, защитни стени, криптиране и подписване. 2. Има системи за откриване на злонамерен софтуер и са актуални.
2	в) Прилагане на стандартни мерки за сигурност в индустрията, осигуряващи	3. Документация за това как се реализира защитата на софтуера и данните в мрежата и

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
	задълбочена защита срещу подправяне и промяна на системите. г) Прилагане на засилен контрол на целостта на софтуера, управление на актуализирането и корекциите за критични активи във виртуализирани мрежи.	информационната система. 4. Инструменти за откриване на аномалии в използването или поведението на системите (като системи за откриване на проникване и откриване на аномалии). 5. Регистър на събитията на системи за откриване на проникване и откриване на аномалии. 6. Адекватни инструменти и процеси за осигуряване на целостта на софтуера при извършване на софтуерни актуализации и прилагане на корекции на сигурността към критични активи във виртуализирани мрежи.
3	д) Изграждане на най-съвременния контрол за защита на целостта на системите. е) Оценка и преглед на ефективността на мерките за защита на целостта на системите.	7. Съвременен контрол за защита на целостта на системите, като подписване на код, технически средства за предотвратяване на инциденти и др. 8. Документация за процеса на проверка на регистри на системи за откриване на аномалии и проникване.

Област на сигурност 3: Сигурност на системите и съоръженията

Цел на сигурност 13: Използване на криптиране

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Където е подходящо, да се предотврати и/или да се сведе до минимум въздействието на инциденти със сигурността върху потребителите и върху други мрежи и услуги, да се криптират данните по време на тяхното съхранение и/или предаване чрез мрежи.	1. Описание на основните потоци от данни и протоколите за криптиране и алгоритмите, използвани за всеки поток. 2. Описание на обоснованите изключения и ограничения при прилагане на криптирането.
2	б) Прилагане на политика за криптиране. в) Използване на индустриални стандарти при алгоритмите за криптиране и съответните препоръчителни дължини на ключовете за криптиране.	3. Документирана политика за криптиране, включваща подробности за криптографските алгоритми и съответните криптографски ключове, съгласно най-добрите международни практики и стандарти. 4. Документирани обосновани изключения, които дават причината за

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
		това кога данните не са криптирани, включително съответната оценка на въздействието.
3	г) Преглед и актуализация на политиката за криптиране. д) Използване на съвременни алгоритми за криптиране.	5. Актуализирана политика за криптиране, преглед на коментари и/или регистри на промените. 6. Политиката за криптиране включва подробности за състоянието на използваните съвременни криптографски протоколи.

Област на сигурност 3: Сигурност на системите и съоръженията

Цел на сигурност 14: Защита на критични данни за сигурността

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Уверяване, че материалът за криптографските ключове и секретната информация за удостоверяване (включително материала за криптографски ключ, използван за удостоверяване) не са разкрити или подправени. б) Достъпът до частни ключове е строго контролиран и наблюдаван.	1. Материалът за криптографските ключове и секретната информация за удостоверяване са защитени с помощта на най-добрите практики и стандарти за защитните механизми (като разделени знания и двоен контрол, криптиране, хеширане, защитен хардуер и т.н.). 2. Описание на механизмите за контрол и наблюдение на достъпа до частни ключове.
2	в) Прилагане на политика за управление на криптографските ключове. г) Прилагане на политика за управление на потребителски пароли.	3. Политика за управление на ключове, включително роли, отговорности и контрол за използването, защита и време валидност на криптографските ключове през целия им период на съществуване, включително контрол за достъп и архивиране, и възстановяване на частни ключове. 4. Политика за управление на потребителските пароли, включваща процеси, методи и техники за сигурно съхранение на потребителските пароли, като се използват най-добрите практики в индустрията.
3	д) Преглед и актуализация на политиката за управление на ключовете. е) Преглед и актуализация на	5. Актуализирана политика за управление на ключове, преглед на коментари и/или регистри на промените. 6. Актуализирана политика за управление

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
	политиката за управление на потребителските пароли.	на пароли на потребителите, преглед на коментари и/или регистри на промените.

Област на сигурност 4: Управление на операциите
Цел на сигурност 15: Оперативни процедури

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Създаване на оперативни процедури и възлагане на отговорности за експлоатацията на критичните системи.	1. Документиране на оперативни процедури и отговорности за ключови мрежови и информационни системи.
2	б) Приложение на политика за работа на системи, чрез които да се гарантира, че всички критични системи се експлоатират и управляват в съответствие с предварително дефинирани процедури.	2. Документирана политика за работа на критичните системи, включително преглед на мрежовите и информационните системи в обхвата.
3	в) Преглед и актуализиране на политика/процедури за експлоатация на критични системи, като се вземат предвид инциденти и/или промени.	3. Актуализирана политика/процедури за критични системи, преглед на коментари и/или регистри за промени.

Област на сигурност 4: Управление на операциите
Цел на сигурност 16: Управление на промените

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Следване на предварително дефинирани методи или процедури, когато се правят промени в критични системи.	1. Документация, описваща предварително дефинирани методи или процедури, следвани при извършване на промени в критични системи.
2	б) Приложение на политика/процедури за управление на промените, за да се гарантира, че промените на критичните системи винаги се извършват по предварително зададен начин. в) Документиране на процедурите за управление на промените и записване на всяка промяна от стъпките на следваната процедура.	2. Документиране на политиката/процедурите за управление на промените, включително системи, предмет на политиката, целите, процедурите за възстановяване и т.н. 3. За всяка промяна е наличен доклад, описващ стъпките и резултата от промяната.
3	г) Редовен преглед и актуализиране на процедурите за управление на промените, като се вземат предвид промените и миналите инциденти.	4. Актуални процедури за управление на промените, преглед на коментари и/или регистри на промените.

Област на сигурност 4: Управление на операциите
Цел на сигурност 17: Управление на активи

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Идентифициране на критични активи и конфигурации на критични системи.	1. Списък на критични активи и критични системи. Списъкът трябва да включва всички критични активи и критични системи на мрежата или услугата, експлоатация и сигурност, включително съответните активи на трети страни.
2	б) Прилагане на политика/процедури за управление на активи и контрол на конфигурациите.	2. Документирана политика/процедури за управление на активи, включително класификация, роли и отговорности, активите и конфигурациите, които са предмет на политиката, целите на управлението на активите. 3. Инвентар (опис) или инвентари (описи) на критични активи и зависимостта между активите. 4. Инвентар/опис или инвентари/описи на конфигурациите на критичните системи.
3	в) Редовен преглед и актуализиране на политиката за управление на активите въз основа на промени и минали инциденти.	5. Актуални политика/процедури за управление на активи, преглед на коментари и/или регистър на промените.

Област на сигурност 5: Управление на инциденти

Цел на сигурност 18: Процедури за управление на инциденти

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Уверение, че персоналът е на разположение и е подготвен за управление и справяне с инциденти. б) Поддържане на запис за всички големи инциденти.	1. Персоналът е наясно как да се справя с инциденти и кога да ги ескалира. 2. Опис на значимите инциденти и за всеки инцидент, въздействие, причина, предприети действия и изводи.
2	в) Прилагане на политика/процедури за управление на инциденти.	3. Политика/процедури за управление на инциденти, включително видове инциденти, които биха могли да възникнат, цели, роли и отговорности, подробно описание за всеки тип инцидент, справяне с инцидента, кога да се ескалира до висшето ръководство (напр. CISO) и др.
3	г) Разследване на големи/значими инциденти и изготвяне на окончателни	4. Индивидуални доклади за обработката на големи инциденти.

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
	доклади за инцидентите, включително предприети действия и препоръки за смекчаване на бъдещата поява на този тип инциденти. д) Оценка на политиката/процедурите за управление на инциденти въз основа на минали инциденти.	5. Актуална политика/процедури за управление на инциденти, преглед на коментари и/или регистри на промените.

Област на сигурност 5: Управление на инциденти

Цел на сигурност 19: Възможност за откриване на инциденти

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Въвеждане на процеси или системи за откриване на инциденти.	1. Документирани примери за минали инциденти, които са били открити и своевременно изпратени на съответните хора.
2	б) Прилагане на индустриални стандартизирани системи и процедури за откриване на инциденти. в) Прилагане на системи и процедури за своевременно регистриране и изпращане на инциденти до подходящите хора.	2. Системи и процедури за откриване на инциденти, като инструменти за управление на инциденти и събития (SIEM), информационен център за сигурност за персонала, доклади и съвети от Националния екип за реагиране при инциденти с компютърната сигурност (CERT), инструменти за откриване на аномалии и др. 3. Мрежови оперативни центрове (NOC) и/или Оперативни центрове за сигурност (SOC) за осигуряване на ефективно наблюдение на мрежата и за откриване на аномалии и за идентифициране и избягване на заплахи.
3	г) Регулярен преглед на системите и процесите за откриване на инциденти и актуализирането им, като се отчитат промените и миналите инциденти. д) Прилагане на съвременни системи и процедури за откриване на инциденти.	4. Актуална документация на системите и процесите за откриване на инциденти. 5. Документация за преглед на процеса на откриване на инциденти, преглед на коментари и/или регистри на промените. 6. Използват се NOC/SOC решения с най-съвременни възможности – напр. SOAR (Оркестрация на сигурността, автоматизация и реакция), осигуряваща интеграция с управление на заплахи и уязвимости, и функция за реагиране на инциденти, автоматизация на операциите за сигурност и др.

Област на сигурност 5: Управление на инциденти

Цел на сигурност 20: Докладване на инциденти и комуникация

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Комуникация и докладване за текущи или минали инциденти на трети страни, клиенти и/или държавни органи, когато е необходимо.	1. Доказателства за минали комуникации и докладване на инциденти.
2	б) Прилагане на политика и процедури за комуникация и докладване за инциденти.	2. Документирана политика и процедури за комуникация и докладване за инциденти, описване на причини/мотиви за комуникация или докладване (бизнес причини, правни причини и др.), вида на инцидентите в обхвата, необходимото съдържание при комуникация, уведомления или доклади, каналите, които трябва да бъдат използвани, и ролите, отговорни за комуникацията, уведомяването и докладването. 3. Шаблони за докладване на инциденти и комуникация.
3	в) Оценка на минали комуникации и докладване за инциденти. г) Преглед и актуализиране на плановете за докладване и комуникация въз основа на промени или минали инциденти.	4. Списък на докладите за инциденти и минали съобщения за инциденти. 5. Актуална политика за реакция при инциденти и комуникация, преглед на коментари и/или регистри на промените.

Област на сигурност 6: Управление на непрекъсваемостта

Цел на сигурност 21: Стратегия за непрекъснатост на услугата и планове за действие при извънредни ситуации

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Прилагане на стратегия за непрекъснатост на услугата за комуникационните мрежи и/или предоставяните услуги.	1. Документирана стратегия за непрекъснатост на услугите, включително цели за времето за възстановяване за ключови услуги и процеси.
2	б) Прилагане на планове за действие при извънредни ситуации за критични системи. в) Наблюдаване на активирането и изпълнението на плановете	2. Планове за извънредни ситуации за критични системи, включително ясни стъпки и процедури за често срещани заплахи, тригери за активиране, стъпки и цели за времето за възстановяване. 3. Процес на вземане на решение за активиране на планове за действие при извънредни

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
	за непредвидени ситуации, регистрирайки успешни и неуспешни времена за възстановяване. г) Прилагане на планове за действие при извънредни ситуации за зависими и взаимозависими критични сектори и услуги.	ситуации. 4. Регистри на активирането и изпълнението на планове за действие при извънредни ситуации, включително взети решения, последвани стъпки, окончателно време за възстановяване. 5. Карта на критичните сектори и услуги, които са от съществено значение за и/или зависят от непрекъснатостта на работата на мрежата и услугите, и плановете за действие при извънредни ситуации за смекчаване на въздействието, свързано със зависими и взаимозависими сектори и услуги. Отнася се за случаите, при които ползвател от критичен сектор е информирал предприятието за такава услуга.
3	д) Периодичен преглед и преработка на стратегията за непрекъснатост на услугите. е) Преглед и преработка на плановете за действие при извънредни ситуации въз основа на минали инциденти и промени.	6. Актуална стратегия за непрекъснатост и планове за действие при непредвидени ситуации, преглед на коментари и/или регистри на промените.

Област на сигурност 6: Управление на непрекъсваемостта

Цел на сигурност 22: Способност за възстановяване при бедствия

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Подготовка за възстановяване и подновяване на услугите след бедствия.	1. Съществуват мерки за справяне с бедствия, като резервирани елементи на мрежата в други региони, архивиране на критични данни на отдалечени места и т.н.
2	б) Прилагане на политика/процедури за внедряване на възможности за възстановяване при бедствия. в) Прилагане на стандарти за възстановяване на мрежите и услугите при бедствия или осигуряване на наличност от трети страни (като националните мрежи за спешни случаи).	2. Документирана политика/процедури за внедряване на възможности за възстановяване при бедствия, включително списък на природни и/или големи бедствия, които биха могли да засегнат услугите, и списък на възможностите за възстановяване при бедствия (налични вътрешно или предоставени от трети страни). 3. Стандарти за възстановяване на

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
		мрежите и услугите при бедствия, като преносимо оборудване, преносими обекти, резервирани обекти и др.
3	г) Създаване на съвременни възможности за възстановяване при бедствия за смекчаване на природни и/или големи бедствия. д) Редовен преглед и актуализиране на способността за възстановяване при бедствия, като се отчитат промени, минали инциденти и резултати от тестове и тренировки.	4. Съвременни възможности за възстановяване при бедствия, като пълно резервиране и механизми за осигуряване при отказ при справяне с природни и/или големи бедствия. 5. Актуализирана документация за наличните възможности за възстановяване при бедствия, преглед на коментари и/или регистрите на промените.

Област на сигурност 7: Мониторинг, одит и тестване

Цел на сигурност 23: Политики за наблюдение и регистриране

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Прилагане на мониторинг и регистриране при критични системи.	1. Регистри на промените и доклади за мониторинг на критични мрежови и информационни системи.
2	б) Прилагане на политика за регистриране и наблюдение на критичните системи. в) Въвеждане на инструменти за наблюдение на критични системи. г) Въвеждане на инструменти за събиране и съхраняване на регистрите на критични системи.	2. Документирана политика за мониторинг и регистриране, включително минимални изисквания за мониторинг и регистриране, период на съхранение и общите цели за съхраняване на данни от мониторинг и регистри на промените. 3. Инструменти за системи за наблюдение и събиране на данни от регистрите на промените. 4. Списък с данни за наблюдение и регистрационни файлове в съответствие с политиката.
3	д) Въвеждане на инструменти за автоматизирано събиране и анализ на данни за наблюдение и регистри на промените. е) Преглед и актуализиране на политика/процедури за регистриране и мониторинг, като се вземат предвид промените и минали инциденти.	5. Инструменти за улесняване на структурното записване и анализ на мониторинга и регистрите на промените. 6. Актуализирана документация за политика/процедури за наблюдение и регистриране, преглед на коментари и/или регистрите на промените.

Област на сигурност 7: Мониторинг, одит и тестване

Цел на сигурност 24: Планове за тренировки при непредвидени ситуации

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Тренировки и тестване на резервните планове и плановете за извънредни ситуации, за да е сигурно, че системите и процесите работят и персоналът е подготвен за големи повреди и непредвидени ситуации.	1. Доклади от минали тренировки за резервни планове и планове за действие при извънредни ситуации.
2	б) Приложение на редовна програма за тренировки на резервни планове и планове за действие при извънредни ситуации, използвайки реалистични сценарии, обхващащи редица различни ситуации във времето. в) Сигурност, че проблемите и уроците, извлечени от тренировките, са адресирани от отговорните хора и че съответните процеси и системи се актуализират съобразно.	2. Програма за тренировки за резервни планове и планове за действие при извънредни ситуации, включително видове непредвидени обстоятелства, честота, роли и отговорности, образци и процедури за провеждане на учения, образци за доклади за учения. 3. Доклади за учения и тренировки, показващи изпълнението на плановете за действие при извънредни ситуации, включително уроци, извлечени от ученията. 4. Въпросите и уроците, извлечени от минали тренировки, са били разгледани от отговорните лица.
3	г) Преглед и актуализиране на плановете за учения, като се вземат предвид промените и миналите инциденти и непредвидени обстоятелства, които не са били обхванати от програмата за учения. д) Включване в тренировки на доставчици и други трети страни, като бизнес партньори или клиенти.	5. Актуализирани планове за тренировки, преглед на коментари и/или регистрите на промените. 6. Информация от доставчици и други участващи трети страни за това как да се подобрят сценариите за тренировки.

Област на сигурност 7: Мониторинг, одит и тестване

Цел на сигурност 25: Тестване на мрежови и информационни системи

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Тестване на мрежи и информационни системи преди използване или свързването им със съществуващи системи.	1. Доклади от тестове на мрежата и информационните системи, включително тестове след големи промени или въвеждане на нови системи.

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
2	б) Прилагане на политика/процедури за тестване на мрежови и информационни системи. в) Внедряване на инструменти за автоматизирано тестване.	2. Политика/процедури за тестване на мрежи и информационни системи, включително кога трябва да се извършат тестове, планове за тестване, казуси, шаблони за протоколи от тестове.
3	г) Преглед и актуализиране на политиката/процедурите за тестване, като се вземат предвид промените и миналите инциденти.	3. Списък с доклади от тестове. 4. Актуализирана политика/процедури за тестване на мрежи и информационни системи, преглед на коментари и/или регистрите на промените.

Област на сигурност 7: Мониторинг, одит и тестване

Цел на сигурност 26: Оценки на сигурността

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Уверение, че критичните системи редовно се подлагат на сканиране и тестване на сигурността, особено когато се въвеждат нови системи и следват промени.	1. Доклади от минали сканирания за сигурност и тестове за сигурност.
2	б) Прилагане на политика/процедури за оценка на сигурността и тестване на сигурността.	2. Документирана политика/процедури за оценки на сигурността и тестване на сигурността, включително кои активи, при какви обстоятелства, вида на оценките и тестовете за сигурност, период, одобрените страни (вътрешни или външни), нивата на поверителност за оценка и резултатите от тестовете и целите за оценка на сигурността и тестове.
3	в) Оценяване на ефективността на политиката/процедурите за оценка на сигурността и тестване на сигурността. г) Преглед и актуализация на политиката/процедурите за оценки на сигурността и тестване на сигурността, като се вземат предвид промените и минали инциденти.	3. Списък на докладите за оценка на сигурността и тестове за сигурност. 4. Доклади за последващи действия за оценка и резултати от тестове. 5. Актуални политика/процедури за оценки на сигурността и тестване на сигурността, преглед на коментари и/или регистрите на промените.

Област на сигурност 7: Мониторинг, одит и тестване

Цел на сигурност 27: Мониторинг на съответствието

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Наблюдение на спазването на стандартите и законовите изисквания.	1. Доклади, описващи резултата от мониторинга на съответствието.
2	б) Прилагане на политика/процедури за наблюдение на съответствието и одит.	2. Документирани политика/процедури за оценка на съответствието и одита, включително какво (активи, процеси, инфраструктура), честота, насоки, кой трябва да извършва одити (вътрешни или външни), съответни политики за сигурност, които са обект на мониторинг за съответствие и одит, целите и подходът на високо ниво за мониторинг на съответствието и одит, шаблони за одиторски доклади. 3. Подробни планове за мониторинг и одит, включително дългосрочни цели и планиране на високо ниво.
3	в) Оценка на политиката/процедурите за съответствие и одит. г) Преглед и актуализиране на политиката/процедурите за съответствие и одит, като се вземат предвид промените и миналите инциденти.	4. Списък на всички доклади за съответствие и одит. 5. Актуализирани политика/процедури за съответствие и одит, преглед на коментари и/или регистрите на промените.

Област на сигурност 8: Информираност за заплахи

Цел на сигурност 28: Разузнаване на заплахи

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Извършване на редовно наблюдение на заплахите.	1. Редовен мониторинг на емисии на разузнавателни данни за външни заплахи (OSINT, търговски източници, проучвания на сигурността и др.) със записани данни от регистрите на промените за съответните значими заплахи. 2. Неформално и предварително споделяне на съответната информация за заплахата със съответните организации на двустранна основа.
2	б) Прилагане на разузнавателна програма за заплахи.	3. Документирана и внедрена програма за разузнаване на заплахи, която включва роли, отговорности, процедури

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
		и механизми за събиране на информация, свързана със значителни заплахи и съответни мерки за смекчаване.
3	в) Преглед и актуализиране на програмата за разузнаване на заплахите. г) Програмата за разузнаване на заплахи използва модерни разузнавателни системи за заплахи.	4. Актуализирана програма за разузнаване на заплахи, преглед на коментари и/или регистрите на промените.

Област на сигурност 8: Информираност за заплахи

Цел на сигурност 29: Информиране на ползвателите за заплахи

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
1	а) Информиране на крайните ползватели на комуникационни мрежи и услуги за конкретни и значителни заплахи за сигурността на мрежата или услугата, които могат да засегнат ползвателя.	1. Бюлетин за сигурността, специализирана уеб страница за информация за заплахи или друг документиран и тестван механизъм за достигане до ползвателите в случай на значителни заплахи. 2. Документирани списъци с най-добри практики и препоръки за сигурност за ползватели за намаляване на типичните рискове (напр. криптиране, надеждна автентикация, актуализации, архиви, информираност на ползвателите и т.н.).
2	б) Приложение на политика/процедури за редовно осведомяване на ползватели относно заплахи за сигурността на мрежата или услугата, които могат да засегнат ползватели.	3. Документирана и внедрена политика за контакт с ползватели с определени роли и отговорности, механизми и критерии за идентифициране на значителни заплахи и процедури, инструменти и методи за навременно и подходящо информиране на ползватели. 4. Политиката включва механизми за идентифициране и споделяне на препоръките и най-добрите практики за ползватели за смекчаване на конкретни заплахи.
3	в) Преглед и актуализиране на политиката/процедурите за редовно информиране на ползватели относно заплахите за	5. Актуализирана политика за уведомяване, преглед на коментари и/или регистрите на промените.

Ниво на сигурност	Мерки за сигурност	Доказателство за изпълнение
	сигурността на мрежата или услугата, които могат да засегнат ползвател.	

Приложение № 2 към чл. 22, ал. 1 и чл. 23

Количествени критерии към чл. 22, ал. 1:

За фиксирана гласова услуга, фиксиран достъп до интернет, междуличностна съобщителна услуга без номер и услуги за разпространение на радио- и телевизионни програми:

Брой ползватели, засегнати от инцидента	Продължителност на инцидента
>= 150 000	>= 1 час
>= 100 000	>= 2 часа
>= 50 000	>= 4 часа
>= 10 000	>= 6 часа
>= 1 000	>= 8 часа

За мобилна гласова услуга, мобилен достъп до интернет и услуги, при които се използва комуникация Машина – Машина:

Брой ползватели, засегнати от инцидента	Продължителност на инцидента
>= 500 000	>= 1 час
>= 250 000	>= 2 часа
>= 100 000	>= 4 часа
>= 50 000	>= 6 часа
>= 10 000	>= 8 часа

Количествен критерий към чл. 23:

Брой ползватели, засегнати от инцидента >= 10 000

Приложение № 3 към чл. 25

Форма за уведомление за инцидент

Предприятие	
Лице за контакт (за целите за проследимост на инцидента)	
Дата и час на възникване на инцидента	
Възникналият инцидент компрометира:	☐ *наличност* ☐ *автентичност* ☐ *цялост* ☐ *поверителност*
Критерий за докладване на инцидента:	☐ *броят ползватели/продължителност* ☐ *географски обхват* ☐ *степента, в която е засегнато функционирането на мрежата или*

	услугата ☐ *степента на въздействие върху стопанските и обществените дейности*
Въздействие на инцидента: Засегнати услуги *(попълва се при окончателно уведомление)* Брой на засегнатите ползватели (за всяка от засегнатите услуги) Дата и час за възстановяване	 ☐ *мобилна гласова услуга* ☐ *мобилен достъп до интернет* ☐ *фиксирана гласова услуга* ☐ *фиксиран достъп до интернет* ☐ *междуличностна съобщителна услуга без номер* ☐ *услуги за разпространение на радио- и телевизионни програми* ☐ *услуги, при които се използва комуникация Машина – Машина* ☐ *други услуги за пренос на сигнали*
Причина за възникване на инцидента:	☐ *природни бедствия и аварии* ☐ *човешка грешка* ☐ *злонамерени атаки* ☐ *повреди в техническото оборудване и програмните продукти* ☐ *външни причини*
Описание на инцидента	
Засегната технология	
Засегнати активи	