ПОЗИЦИЯ

на Консултативния съвет по въпросите на сигурността на обществените мобилни наземни електронни съобщителни мрежи и мобилни услуги (Консултативен съвет по сигурността на мобилните мрежи и услуги), създаден с Решение № 425 от 17.12.2020 г. на Комисия за регулиране на съобщенията (КРС), изменен с Решение № 34 от 28.01.2021 г.

УПЪЛНОМОЩЕНИТЕ ПРЕДСТАВИТЕЛИ В КОНСУЛТАТИВНИЯТ СЪВЕТ,

като взеха предвид резултатите от проведените заседания на Консултативния съвет по сигурността на мобилните мрежи и услуги и писмените становища на представители на предприятия, предоставящи мобилни мрежи и услуги, и техните браншови организации, участвали в работата на Консултативният съвет,

ПРИЕХА НАСТОЯЩАТА ПОЗИЦИЯ ПО ОТНОШЕНИЕ НА РАЗГЛЕДАНИТЕ ВЪПРОСИ, КАКТО СЛЕДВА:

Консултативният съвет е форум за сътрудничество и обмен на добра практика и опит между предприятията с цел постигане на общо разбиране относно изискванията към сигурността на обществените мобилни електронни съобщителни мрежи и мобилни услуги.

Въз основа на изготвената Позиция, предприятията, предоставящи обществени мобилни електронни съобщителни мрежи и мобилни услуги ще се стремят да постигат ниво на сигурност, съобразено с особеностите на конкретните мрежи и услуги, още от етапа на проектирането им.

При изготвянето на Позицията са взети предвид относимите документи на Агенцията на Европейския съюз за киберсигурност (ENISA), както следва:

1. Насоки на ENISA за мерки за сигурност/Guideline on Security Measures under the EECC[1];
2. Допълнителни мерки за 5G към Насоки на ENISA за мерки за сигурност /5G SUPPLEMENT To the Guideline on Security Measures under the EECC[2];
3. Насоки на ENISA за докладване на инциденти/Technical Guideline on Incident Reporting[3];
4. Инструментариум на ЕС за киберсигурността в областта на 5G/Cybersecurity of 5G networks EU Toolbox of risk mitigating measures[4];
5. Заплахи за 5G мрежи - 2020/ENISA THREAT LANDSCAPE FOR 5G NETWORKS-2020[5];
6. Спецификации за сигурност на 5G /SECURITY IN 5G SPECIFICATIONS[6]

Обществените мобилни електронни съобщителни мрежи и мобилни услуги са дефинирани в Закона за електронните съобщения (ЗЕС), като за целите на сигурността

---

[1] https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc
[2] https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc
[3] https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc
[4] https://ec.europa.eu/bulgaria/news/secure-5g-networks-ec-endorses-eu-toolbox-and-sets-next-steps_bg
[5] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks
[6] https://www.enisa.europa.eu/publications/security-in-5g-specifications

услугите се категоризират съобразно Насоките на ENISA за докладване на инциденти, по следния начин:

а) мобилна телефонна услуга (гласова телефонна услуга, видео телефонна услуга, SMS, MMS ...);

б) мобилен достъп до интернет (предоставян чрез GPRS, 3G, 4G, 5G, ...);

в) комуникация Машина - Машина (включително 5G URLCC, MTC). Изискванията за сигурност към услугите Машина - Машина се отнасят и до предприятията, предоставящи съответната услуга.

„Сигурност на мрежите и услугите" е способността на електронните съобщителни мрежи и услуги да издържат - при определено ниво на увереност - 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.

- „Автентичност" е свойството на данните (трафични и за ползвателите на услугата), че са тези за които се представят;
- "Наличност" е свойството на електронните съобщителни мрежи или услуги за достъпност и използваемост при поискване;
- „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;
- „Цялост" е свойството на данните (трафични и за ползвателите на услугата) за точност и пълнота.

Съгласно чл. 3 от Правилата за осъществяване на дейността на консултативния съвет по въпросите на сигурността на обществените мобилни електронни съобщителни мрежи и мобилни услуги (Приложение към Решение № 34 от 28.01.2021 г. на КРС), задачите на Консултативния съвет по сигурността на мобилните мрежи и услуги са свързани с обсъждане на изискванията за сигурност на обществените мобилни електронни съобщителни мрежи и мобилни услуги и постигане на съгласие по въпроси, относими към:

1. управление на риска на сигурността;
2. минималните изисквания за сигурност;
3. критерии за определяне на въздействието на инцидент, свързан със сигурността;
4. оценяване на рисковия профил на доставчиците на мрежово оборудване;
5. стратегия за използване на множество доставчици на мрежово оборудване.

Предвид проведените заседания и представените писмени становища, участниците в Консултативния съвет по сигурността на мобилните мрежи изразяват своята обща позиция по въпросите за управление на риска за сигурността на мобилните мрежи и услуги, минималните изисквания за сигурност и критериите за определяне на въздействието на инцидент, свързани със сигурността:

1. Управление на риска на сигурността

Управление на риска на сигурността, включва оценка на риска, изготвяне на мерки за намаляване на риска, изследване на инциденти и одит на сигурността. Всяко предприятие, предоставящо обществените мобилни електронни съобщителни мрежи и/или мобилни услуги изготвя собствена методика за управление на риска, съобразно предоставяните мрежи и/или услуги. В случай че предприятията имат вече установени политики, процеси и рамки, базирани на приложими хармонизирани международни

стандарти, като ISO27000, и с цел избягване на дублиране на документи, е достатъчно същите да се съобразят (допълнят) с изискванията на ENISA.
При внедряване на нови 5G елементи от функционалната архитектура в мрежите на операторите, при оценката на риска ще се използва доколкото е приложим списък Приложение №1, изготвен на база документа на ENISA Заплахи за 5G мрежи.

2. Минимални изискванията за сигурност

Въз основа на оценката на риска предприятията, предоставящи обществени мобилни електронни съобщителни мрежи и/или мобилни услуги предприемат подходящи и пропорционални технически и организационни мерки за намаляване на риска. При изготвянето се използват всички приложими мерки от Насоките на ENISA за сигурност, Приложение № 2 към настоящата Позиция. Част от допълнителните мерки за 5G изисквания водят до допълнителни усилия и време за изпълнение, което следва да бъде отчетено при налагане на задълженията, поради това следва да бъдат включени на по-късен етап при наличие на съответната техническа възможност и нормативна обезпеченост. Списък с неприложими мерки за сигурност е изготвен в Приложение №3.

3. Оценка на рискови доставчици

Управлението на рисковия профил на доставчика е част от цялостното управление на риска за сигурността. Управлението на риска при информационна сигурност е процесът на идентифициране, оценка и адресиране на рисковете, свързани с ценната информация на организацията. Той разглежда несигурността около тези активи, за да гарантира постигането на желаните бизнес резултати.
Управлението на рисковия профил на доставчика намира отражение наред с друго под формата на подходящи договорни условия, които да предвидят мрежовите оператори в отношенията си с доставчици на оборудване и софтуер.
В тази връзка, в Приложение №4 „Оценка на рисковите доставчици“ сме постигнали съгласие по отношение на задължителните и препоръчителните мерки за сигурност.

4. Стратегия за множество доставчици

Задължението за изготвяне на стратегии за използване на множество доставчици на мрежово оборудване е възложено на предприятията с издадените разрешения за ползване на индивидуално определен ограничен ресурс в 2.6GHz и 3.6GHz, в тази връзка считаме за подходящо да се приложи индивидуален подход, с което да се постигне укрепване на устойчивостта на национално ниво.

5. Критерии за определяне на въздействието на инцидент, свързан със сигурността

По отношение на първоначалното информиране за инцидент - предлагаме да се предостави срок от напр. 24 часа от възникване или установяване на инцидента. По този начин ще е възможно както установяване на действителния мащаб на инцидента, така и предоставяне на по-подробна информация за него на регулатора.
Считаме, че за мобилните услуги следва да има различни прагове за докладване на инциденти:

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

По отношение на качествените критерии:

- Критерият „географският обхват на областта, засегната от инцидента, свързан със сигурността“ считаме, че трябва да обхваща площ на една административна област, цялата територия на гр. София и трудно достъпни райони;
- Критерият „засягащи осъществяването на повиквания към единния европейски номер за спешни повиквания 112 и националните номера за спешни повиквания“ предлагаме да се формулира „засягащи достъпа към единния европейски номер за спешни повиквания 112 и националните номера за спешни повиквания“;
- Критерият „има широк медиен отзвук“ би следвало да отпадане.
- Критерият „засегнати критични функции за обществото“ считаме, че не може да бъде изпълнен от страна на предприятията, тъй като не разполагат с информация кои електронни съобщителни услуги се ползват от критичните функции.

Настоящата Позиция е публикувана на страницата на КРС в раздел „Сигурност на мрежите и услугите“.

За „А1 България” ЕАД:

.....
/...../

За „Българска телекомуникационна компания” АД:

.....
/...../

За „Теленор България“ ЕАД и „Цетин България“ ЕАД:

.....
/...../

За „Българска асоциация на кабелните и комуникационните оператори“:

.....
/...../

Приложение №1
Списък на елементите от функционалната архитектура
на мобилните наземни мрежи от пето поколение

1. Елементи от Опорната мрежа - CORE NETWORK
- 1.1. Access and Mobility Management function (AMF)
- 1.2. Session Management function (SMF)
- 1.3. User plane function (UPF)
- 1.4. Policy Control Function (PCF)
- 1.5. Network Exposure Function (NEF)
- 1.6. Network Repository Function (NRF)
- 1.7. Unified Data Management (UDM)
- 1.8. Authentication Server Function (AUSF)
- 1.9. Application Function (AF)
- 1.10. Unified Data Repository (UDR)
- 1.11. Unstructured Data Storage Function (UDSF)
- 1.12. Network Slice Selection Function (NSSF)
- 1.13. Gateway Mobile Location Centre (GMLC)
- 1.14. Localisation Management Function (LMF)
- 1.15. Service Communication Proxy (SCP)
- 1.16. UE radio Capability Management Function (UCMF)
- 1.17. Network Slice Specific Authentication and Authorisation Function (NSSAAF)

2. Елементи от Network Slicing (NS)
- 2.1. Service Instance Layer (Communication Services)
- 2.2. Communication Service Management Function (CSMF)
- 2.3. Network Slice Management Function (NSMF)
- 2.4. Network Slice Subnet Management Function (NSSMF)
- 2.5. Network Slice Instance (NSI)
- 2.6. Network Slice Subnet Instance (NSSI)
- 2.7. Network Functions (NF)
- 2.8. Core Network Functions (CNF)
- 2.9. Access Nework Functions (gNB)
- 2.10. Network Functions Virtualization Management and Network Orchestration (NFV MANO)
- 2.11. Element Management System (EMS)
- 2.12. Operations Support System (OSS)
- 2.13. Resources layer
- 2.14. Management Functions Service Based Interface (SBI)
- 2.15. Os-Ma-nfvo reference point

3. Елементи от Radio Access Network (RAN)
- 3.1. User Equipment (UE)
- 3.2. Next generation Node/Base Station (gNB)
- 3.3. gNB Distributed Unit (gNB-DU)
- 3.4. gNB Central Unit (gNB-CU)
- 3.5. Xn network interface
- 3.6. NG interface
- 3.7. New Radio Unified Air Interface (NR Uu)
- 3.8. Integrated Access and Backhaul Donor (IAB Donor)

3.9. Integrated Access and Backhaul Node (IAB Node)
3.10. Non Acces Stratum (NAS)
3.11. Access Stratum (AS)
3.12. F1 interface

4. Елементи от Network Function Virtualisation (NFV)
4.1. Operations Support System / Business Support System (OSS/BSS)
4.2. Virtualised Network Function (VNF)
4.3. Element Management (EM)
4.4. Network Functions Virtualization Infrastructure (NFVI)
4.5. Хардуерни ресурси - Hardware Resources
4.6. Virtualisation Layer and Virtualised Resources
4.7. Virtualised Infrastructure Manager
4.8. Network Functions Virtualization Orchestrator
4.9. Virtual Network Function Manager (VNFM)
4.10. Os-Ma-nfvo reference point
4.11. Ve-Vnfm-em reference point
4.12. Ve-Vnfm-vnf reference point
4.13. NFVI – Virtualised Infrastructure Manager (Nf-VI)
4.14. NFV Security Manager (NSM)
4.15. NFVI Security Manager (ISM)
4.16. Security Element Manager (SEM)
4.17. Virtual Security Function (VSF)
4.18. NFVI-based Security Function (ISF)
4.19. Physical Security Function (PSF)
4.20. NFVI – Virtualised Infrastructure Manager (NF-VI)

5. Елементи от Software Defined Network (SDN)
5.1. Software-define Networking controller (SDN controller)
5.2. SDN Application
5.3. SDN resources
5.4. Northbound Interface
5.5. Southbound Interface
5.6. Eestbound-Westbound Interface
5.7. Control Plane (CP)
5.8. Data Plane (DP) or Forwarding Plane (FP)

6. Елементи от Multi-Access Edge Computing (MEC)
6.1. Customer facing service (CFS) portal
6.2. Device application
6.3. Application Client(s)
6.4. Edge Enabler Client (EEC)
6.5. Edge Configuration Server (ECS)
6.6. User application lifecycle management (LCM) proxy
6.7. Multi-access edge orchestrator
6.8. Multi-Access Edge Computing Host (MEC host)
6.9. Virtualisation infrastructure
6.10. MEC platform
6.11. Edge Enabler Server (ESS)
6.12. MEC applications

6.13. Edge Application Server (EAS)
6.14. MEC service
6.15. Service registry
6.16. Application Data Traffic
6.17. MEC host level management
6.18. MEC platform manager
6.19. Virtualisation infrastructure manager

7. Елементи от Архитектурата за сигурност - Security Architecture (SA)
7.1. Mobile Equipment (ME)
7.2. Universal Subscriber Identity Module (USIM)
7.3. 5G Node Base Station Central Unit (gNB-CU)
7.4. Non-3GPP Access Network
7.5. Non-3GPP access Inter-Working Function (N3IWF)
7.6. Access and Mobility Management Function (AMF)
7.7. Security Anchor Function (SEAF)
7.8. Authentication server function (AUSF)
7.9. Authentication credential Repository and Processing Function (ARPF)
7.10. User Data Management (UDM) Function
7.11. Unstructerd Data Repository (UDR)
7.12. Security Edge Protection Proxy (SEPP)
7.13. Network Slice Specific Authentication and Authorisation Function (NSSAAF)
7.14. Authentication, Authorization and Accounting server (AAA-S)
7.15. AAA proxy (AAA-P)
7.16. Extensible Authentiaction Protocol (EAP-ID)
7.17. NFV Security Services Agent (SSA)
7.18. NFV Security Controller (SC)
7.19. NFV Security Services Provider (SSP)
7.20. NFV Security Monitoring Database
7.21. SA/VSF Catalogue Database (VSF-NVNF-CAT)
7.22. Audit DB
7.23. Security Monitoring Analytics System
7.24. Subscription Concealed Identifier (SUCI)
7.25. Subscription Permanent Identifier (SUPI)
7.26. Вектор за удостоверяване - Authentication Vector
7.27. Anchor Key
7.28. Key Hierarchy

8. Елементи от Implementation Options / Migration Paths
8.1. Evolved Packet Core (EPC)
8.2. Evolved Packet Core Plus (EPC+)
8.3. 5G основна мрежа - 5G Core Network (5GC)
8.4. En-gNB
8.5. Master node (MeNB)
8.6. X2 Interface
8.7. S1 interface
8.8. Mobility Management Entity (MME)
8.9. Serving Gateway (SGW)
8.10. User Equipment (UE)

Приложение №2
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	Мерки за сигурност	Доказателство за изпълнение
1	a) Задаване на високо ниво на политика за сигурност, насочена към сигурността на мрежите и услугите. b) Информиране на ключовия персонал за политиката за сигурност.	i. Документирана политика за сигурност, включително за мрежи и услуги по обхват, критични активи, които ги поддържат, и цели за сигурност. ii. Ключовият персонал е запознат с политиката за сигурност и нейните цели (интервю).
2	c) Задаване на подробни политики за сигурността на информацията за критични активи и бизнес процеси. d) Запознаване на целия персонал относно политиката за сигурност и какво означава тя за тяхната работа. e) Преглед на политиката за сигурност след инциденти.	iii. Документирани политики за сигурността на информацията, одобрени от ръководството, включително приложими законови и регулаторни разпоредби, достъпни за персонала. iv. Персоналът е наясно с политиката за сигурност на информацията и какво означава тя за тяхната работа (интервю). v. Преглед на коментарите или регистрите на промените на политиката.
3	f) Периодичен преглед на политиката за сигурност на информацията и вземане предвид на нарушенията, изключенията, предишни инциденти и тестове/тренировки, и инциденти засягащи други (подобни) доставчици в сектора.	vi. Политиките за информационна сигурност са актуални и одобрени от висшето ръководство. vii. Регистри на изключенията от политиката, одобрени от съответните роли. viii. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) Изготвяне на списък с основните рискове за мрежите и услугите, отчитайки основните заплахи за критичните активи. b) Запознаване на ключовия персонал с основните рискове и начините за намаляването им.	i. Списък на основните рискове, описани на високо ниво, включително на основните заплахи и тяхното потенциално въздействие върху сигурността на мрежите и услугите. ii. Ключовия персонал знае основните рискове (интервю).

2	c) Създаване на методология и/или инструменти за управление на риска, базирани на индустриални стандарти. d) Уверение, че ключовият персонал използва методологията и инструментите за управление на риска. e) Преглед на оценките на риска след промени и инциденти. f) Уверение, че остатъчните рискове са приети от ръководството.	iii. Документирани методология и/или инструменти за управление на риска. iv. Насоки за персонала за оценка на рисковете. v. Списък с рисковете и доказателства за актуализации /прегледи. vi. Преглед на коментари или регистрите на промените за оценка на риска. vii. Одобрение на остатъчните рискове от ръководството.
3	h) Преглед на методологията и/или инструментите за управление на риска, като се вземат предвид промени и минали инциденти.	viii. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) Разпределение на ролите и отговорностите по сигурността на персонала. b) Уверение, ролите за сигурността са достъпни в случай на инцидент.	i. Списък с ролите по сигурността (Главен служител по сигурността на информацията, Длъжностно лице по защита на данните, Ръководител по непрекъснатостта на дейностите и т.н.), кой ги заема и данни за контакт.
2	c) Персоналът е назначен официално на длъжност, свързана с роля по сигурността. d) Уведомяване на персонала за ролите по сигурността в организацията и кога трябва да бъдат потърсени.	ii. 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.). iii. Материали за персонала за осведоменост/разпространение, обясняващи ролите по сигурността и кога/как те трябва да бъдат потърсени.
3	e) Структурата на ролите и отговорностите по сигурността редовно се преразглеждат и преработват въз основа на промени и/или минали инциденти.	iv. Актуална документация за структурата на назначенията и отговорностите на ролите по сигурността. v. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) Включване на изисквания за сигурност в договорите с трети страни, включително за конфиденциалност и сигурен трансфер на информация.	i. 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	b) Задаване на политика по сигурността за договори с трети страни. c) Уверение, че всички доставки на/поръчки на услуги/продукти от трети страни следват политиката. d) Преглед на политиката по сигурността за трети страни след инциденти или промени. e) Изискване за специфични стандарти за сигурност в процесите на трети страни доставчици по време на доставката. f) Намаляване на остатъчните рискове, които не се разглеждат от третата страна.	ii. Документирана политика по сигурността за договори с трети страни. iii. Списък на договорите с трети страни. iv. Договорите за услуги на трети лица съдържат изисквания за сигурност, в съответствие с политиката по сигурността за доставка. v. Преглед на коментарите или промените в регистрите на политиката. vi. Договорите с доставчици на оборудване съдържат изисквания за спазване на добрите практики за сигурност и индустриални стандарти. vii. Остатъчните рискове, произтичащи от зависимост от трети страни, са изброени и намалени.
3	g) Проследяване на инциденти на сигурността, свързани или причинени от трети страни. h) Периодичен преглед и актуализиране на политиката за сигурност за трети страни на редовни интервали, като се отчитат минали инциденти, промени и т.н.	viii. Списък на инциденти на сигурността, свързани с или причинени от ангажимент с трети страни. ix. Документация на процеса на преглед на политиката.

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

ниво	Мерки за сигурност	Доказателство за изпълнение
1	a) Проверка на професионалните препоръки на ключовия персонал (системни администратори, служители по сигурността, охрана и др.).	i. Документиране на проверките на професионалните препоръки за ключов персонал.
2	b) Извършване на проверки / филтриране за ключовия персонал, когато е необходимо и законово разрешено.	ii. Политика и процедура за проверки/филтриране. iii. Насоки за персонала относно това кога/как да се извършват проверки.

	c) Създаване на политика и процедура за проверка на миналото.	
3	d) Преглед и актуализиране на политиката/процедурите за проверка на миналото и проверки на препоръките на редовни интервали, като вземете предвид промените и миналите инциденти.	iv. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) Осигуряване на подходящо обучение и материали по въпросите на сигурността на ключовия персонал.	i. Ключовият персонал е преминал обучения и има достатъчно познания по сигурността (интервю).
2	b) Изпълнение на програма за обучение, като се провери, че ключовият персонал разполага с достатъчно и актуални познания за сигурността. c) Организиране на обучения и сесии за осведоменост на персонала по теми за сигурността, важни за организацията.	ii. Персоналът участва в сесии за осведоменост по теми за сигурността. iii. 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	d) Периодичен преглед и актуализиране на програмата за обучение, като се отчитат промените и миналите инциденти. e) Проверка на знанията по сигурността на персонала.	iv. Актуализирана програма за осведоменост и обучение по сигурността. v. Резултати от тестове на знанията по сигурността на персонала. vi. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) След промени в персонала да се отнемат правата за достъп, пропуск, оборудването и т.н., ако вече не са необходими или допустими. b) Информиране и обучаване на новия персонал за действащите политики и процедури.	i. Доказателства, че промените в персонала са последвани от отнемане на права за достъп, пропуск, оборудване и др. ii. Доказателства, че новите служители са били инструктирани и обучени в действащите политики и процедури.
2	c) Прилагане на политика/процедури за промени в персонала, като се вземат предвид своевременното отнемане на права за достъп, пропуски и оборудване.	iii. Документиране на процеса за промени в персонала, включително отговорности за ръководене на промените, описание на правата за достъп и притежание на активи по

	d) Прилагане на политика/процедури за образоване и обучение на персонала в нови роли.	роли, процедури за инструктаж и обучение на персонала за нови роли. iv. Доказателство, че промените на персонала са извършени в съответствие с процеса и че правата за достъп са актуализирани своевременно (например контролни списъци).
3	e) Периодична проверка дали политиката/процедурите са ефективни. f) Преглед и оценка на политиката/процедурите за промени на персонала, като се вземат предвид промените или минали инциденти.	v. Доказателства за проверки на правата за достъп и т.н. vi. Актуални политика/процедури за управление на промените на персонала. vii. Преглед на коментарите или регистрите на промените.

Област на сигурност 2: Сигурност на човешките ресурси
Цел на сигурност 08: Справяне с нарушенията

ниво	Мерки за сигурност	Доказателство за изпълнение
1	a) Персоналът да се държи отговорен за инциденти, свързани със сигурността, причинени от нарушения на политиките, например чрез трудовия договор.	i. Правила за персонала, включително отговорности, кодекс за поведение, нарушения на политики и др., възможно като част от трудови договори.
2	b) Създаване на процедури за нарушения на политиките от персонала.	ii. Документация на процедурите, включително видове нарушения, които могат да бъдат предмет на дисциплинарни действия и какви дисциплинарни действия могат да бъдат предприети.
3	c) Периодичен преглед и актуализиране на дисциплинарния процес въз основа на промени и минали инциденти.	iii. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) 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.	i. 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	b) Внедряване на политика за мерки за физическа сигурност и контрол на средата.	ii. Документирана политика за мерки за физическа сигурност и контрол на

	c) Внедряване на стандарти за физически контрол и контрол на средата. d) Прилагане на засилен контрол за физически достъп до критични активи.	средата, включително описание на съоръженията и системите. iii. Физически контрол и контрол на средата, като електронен контрол на входната и одитната пътека, сегментиране на пространствата според нивата на упълномощаване, автоматизирани пожарогасители с халокарбонови газове и др. iv. Политиката включва списъци с критични активи и засилен физически контрол за достъп до тези активи.
3	e) Периодична оценка на ефективността на физическия контрол и контрола на средата. f) Преглед и актуализация на политиката относно мерките за физическа сигурност и контрол на средата, като се вземат предвид промените и миналите инциденти.	v. Актуална политика за мерки за физическа сигурност и контрол на средата. vi. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) Осигуряване на сигурност на критичните доставки.	i. Сигурността на критичните доставки е защитена по основен начин, например, налично е резервно захранване и/или резервно гориво.
2	b) Прилагане на политика за сигурност на критичните доставки. c) 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.).	ii. Документирана политика за защита на критичните доставки като електрическа енергия, гориво и др., описваща различни видове доставки и мерки за сигурност, защитаващи доставките. iii. Доказателство за индустриални стандартизирани мерки за защита на сигурността на критичните доставки.
3	d) Прилагане на най-съвременни мерки за сигурност за защита на критични доставки (като активно охлаждане, UP, паралелно работещи генератори, Споразумение за ниво на обслужване (SLA) с компании за доставка на гориво, резервирано охлаждане и системи за резервно захранване).	iv. Доказателства за съвременни мерки за защита на сигурността на критични доставки. v. Актуализирана политика за осигуряване на критичните доставки и спомагателни съоръжения, преглед на коментари и/или регистрите на промените.

	e) Регулярен преглед и актуализиране на политиката и процедурите за осигуряване на критични доставки, като се вземат предвид промените и миналите инциденти.	

Област на сигурност 3: Сигурност на системите и съоръженията
Цел на сигурност 11: Контрол на достъпа до мрежови и информационни системи

ниво	Мерки за сигурност	Доказателство за изпълнение
1	a) Потребителите и системите имат уникални идентификатори и се удостоверяват преди достъп до услуги или системи. b) Прилагане на логически механизъм за контрол на достъпа за мрежови и информационни системи, за да се позволи само упълномощен достъп.	i. Регистрите за достъп показват уникални идентификатори за потребители и системи, когато им е предоставен или отказан достъп. ii. Преглед на методите за автентикация и контрол на достъпа за системи и потребители.
2	c) 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. d) Избор на подходящи механизми за удостоверяване, в зависимост от вида на достъпа. e) Наблюдението на достъпа до мрежови и информационни системи да има процес за одобряване на изключения и регистриране на нарушения на достъпа. f) Подсилване на контрола за отдалечен достъп до критични активи на мрежови и информационни системи от трети страни.	iii. Политика за контрол на достъпа, включително описание на роли, групи, права на достъп, процедури за предоставяне и отнемане на достъп. iv. Различни видове механизми за автентикация за различните видове достъп. v. Регистър на нарушенията и изключенията на политиката за контрол на достъпа, одобрени от служителя по сигурността. vi. Правилата на минималните права и разделението на задълженията се документират и прилагат, където е уместно. vii. Отдалеченият достъп, от трети страни, до критични активи е сведен до минимум и е подложен на строг контрол на достъпа, включително съвременен контрол за автентикация, оторизация и одит, особено за привилегировани акаунти.
3	g) Оценка на ефективността на политиките и процедурите за контрол на достъпа и въвеждане на кръстосани проверки на механизмите за контрол на достъпа. h) Политиката за контрол на достъпа и механизмите за контрол на достъпа се преразглеждат и при необходимост се ревизират.	viii. Доклади за тестове (на сигурността) на механизмите за контрол на достъпа. ix. Инструменти за откриване на извън нормалното използване на системи или поведение на системи (като системи за откриване на проникване и откриване на аномалии).

		x. Регистри на системите за откриване на проникване и откриване на аномалии. xi. Актуализации на политиката за контрол на достъпа, преглед на коментари или регистрите на промените. xii. Документиран анализ на риска за прилагането на вписванията и ограниченията. xiii. Процедури, които гарантират, че контрола 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	Мерки за сигурност	Доказателство за изпълнение
1	a) Уверяване, че софтуерът на мрежовите и информационните системи не е манипулиран или променян, например чрез контрол на входа и защитни стени. b) Проверка за злонамерен софтуер във (вътрешната) мрежа и информационните системи.	i. Софтуерът и данните в мрежовите и информационните системи са защитени с помощта на контрол на входа, защитни стени, криптиране и подписване. ii. Има системи за откриване на злонамерен софтуер и са актуални.
2	c) Прилагане на стандартни мерки за сигурност в индустрията, осигуряващи задълбочена защита срещу подправяне и промяна на системите. d) Прилагане на засилен контрол на целостта на софтуера, управление на актуализирането и корекциите за критични активи във виртуализирани мрежи.	iii. Документация за това как се реализира защитата на софтуера и данните в мрежата и информационната система. iv. Инструменти за откриване на аномалии в използването или поведението на системите (като системи за откриване на проникване и откриване на аномалии). v. Регистър на събитията на системи за откриване на проникване и откриване на аномалии. vi. 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	e) Изграждане на най-съвременния контрол за защита на целостта на системите.	vii. Съвременен контрол за защита на целостта на системите, като подписване на код, технически

	f) Оценка и преглед на ефективността на мерките за защита на целостта на системите.	средства за предотвратяване на инциденти и др. viii. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) 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.	i. Описание на основните потоци от данни и протоколите за криптиране и алгоритмите, използвани за всеки поток. ii. Описание на обоснованите изключения и ограничения при прилагане на криптирането.
2	b) Прилагане на политика за криптиране. c) Използване на индустриални стандарти при алгоритмите за криптиране и съответните препоръчителни дължини на ключовете за криптиране.	iii. Документирана политика за криптиране, включваща подробности за криптографските алгоритми и съответните криптографски ключове, съгласно най-добрите международни практики и стандарти. iv. Документирани обосновани изключения, които дават причината за това, кога данните не са криптирани, включително съответната оценка на въздействието.
3	d) Преглед и актуализация на политиката за криптиране. e) Използване на съвременни алгоритми за криптиране.	v. Актуализирана политика за криптиране, преглед на коментари и/или регистри на промените. vi. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) Уверяване, че материалът за криптографските ключове и секретната информация за удостоверяване (включително материала за криптографски ключ, използван за удостоверяване) не са разкрити или подправени. b) Достъпът до частни ключове е строго контролиран и наблюдаван.	i. 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.).

		ii. Описание на механизмите за контрол и наблюдение на достъпа до частни ключове.
2	c) Прилагане на политика за управление на криптографските ключове. d) Прилагане на политика за управление на потребителски пароли.	iii. 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. iv. 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	e) Преглед и актуализация на политиката за управление на ключовете. f) Преглед и актуализация на политиката за управление на потребителските пароли.	v. Актуализирана политика за управление на ключове, преглед на коментари и/или регистри на промените. vi. Актуализирана политика за управление 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	Мерки за сигурност	Доказателство за изпълнение
1	a) Създаване на оперативни процедури и възлагане на отговорности за експлоатацията на критичните системи.	i. Документиране на оперативни процедури и отговорности за ключови мрежови и информационни системи.
2	b) 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.	ii. Документирана политика за работа на критичните системи, включително преглед на мрежовите и информационните системи в обхвата.
3	c) Преглед и актуализиране на политика/процедури за експлоатация на критични системи, като се вземат предвид инциденти и/или промени.	iii. 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	Мерки за сигурност	Доказателство за изпълнение

1	a) Следване на предварително дефинирани методи или процедури, когато се правят промени в критични системи.	i. Документация, описваща предварително дефинирани методи или процедури, следвани при извършване на промени в критични системи.
2	b) Приложение на политика/ процедури за управление на промените, за да се гарантира, че промените на критичните системи винаги се извършват по предварително зададен начин. c) Документиране на процедурите за управление на промените и записване на всяка промяна от стъпките на следваната процедура.	ii. Документиране на политиката/ процедурите за управление на промените, включително системи, предмет на политиката, целите, процедурите за възстановяване и т.н. iii. За всяка промяна е наличен доклад, описващ стъпките и резултата от промяната.
3	d) Редовен преглед и актуализиране на процедурите за управление на промените, като се вземат предвид промените и миналите инциденти.	iv. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) Идентифициране на критични активи и конфигурации на критични системи.	i. 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	b) Прилагане на политика/ процедури за управление на активи и контрол на конфигурациите.	ii. Документирана политика/ процедури за управление на активи, включително роли и отговорности, активите и конфигурациите, които са предмет на политиката, целите на управлението на активите. iii. Инвентар (опис) или инвентари (описи) на критични активи и зависимостта между активите. iv. Инвентар/опис или инвентари/описи на конфигурациите на критичните системи.
3	c) Редовен преглед и актуализиране на политиката за управление на активите, въз основа на промени и минали инциденти.	v. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) Уверение, че персоналът е на разположение и подготвен за управление и справяне с инциденти. b) Поддържане на запис за всички големи инциденти.	i. Персоналът е наясно как да се справя с инциденти и кога да ги ескалира. ii. Опис на значимите инциденти и за всеки инцидент, въздействие, причина, предприети действия и изводи.
2	c) Прилагане на политика/ процедури за управление на инциденти.	iii. 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	d) Разследване на големи/значими инциденти и изготвяне на окончателни доклади за инцидентите, включително предприети действия и препоръки за смекчаване на бъдещата поява на този тип инциденти. e) Оценка на политиката/процедурите за управление на инциденти въз основа на минали инциденти.	iv. Индивидуални доклади за обработката на големи инциденти. v. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) Въвеждане на процеси или системи за откриване на инциденти.	i. Документирани примери за минали инциденти, които са били открити и своевременно изпратени на съответните хора.
2	b) Прилагане на индустриални стандартизирани системи и процедури за откриване на инциденти. c) Прилагане на системи и процедури за своевременно регистриране и изпращане на инциденти до подходящите хора.	ii. 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. iii. 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	d) Регулярен преглед на системите и процесите за откриване на инциденти и актуализирането им , като се отчитат промените и миналите инциденти. e) Прилагане на съвременни системи и процедури за откриване на инциденти.	iv. Актуална документация на системите и процесите за откриване на инциденти. v. Документация за преглед на процеса на откриване на инциденти, преглед на коментари и/или регистри на промените. vi. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) Комуникация и докладване за текущи или минали инциденти на трети страни, клиенти и/или държавни органи, когато е необходимо.	i. Доказателства за минали комуникации и докладване на инциденти.
2	b) Прилагане на политика и процедури за комуникация и докладване за инциденти.	ii. 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. iii. Шаблони за докладване на инциденти и комуникация.
3	c) Оценка на минали комуникации и докладване за инциденти. d) Преглед и актуализиране на плановете за докладване и комуникация въз основа на промени или минали инциденти.	iv. Списък на докладите за инциденти и минали съобщения за инциденти. v. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) Прилагане на стратегия за непрекъснатост на услугата за комуникационните мрежи и/или предоставяните услуги.	i. Документирана стратегия за непрекъснатост на услугите, включително цели за времето за възстановяване за ключови услуги и процеси
2	b) Прилагане на планове за действие при извънредни ситуации за критични системи. c) Наблюдаване на активирането и изпълнението на плановете за непредвидени ситуации, регистрирайки успешни и неуспешни времена за възстановяване. d) Прилагане на планове за действие при извънредни ситуации за зависими и взаимозависими критични сектори и услуги.	ii. 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. iii. Процес на вземане на решение за активиране на планове за действие при извънредни ситуации. iv. Регистри на активирането и изпълнението на планове за действие при извънредни ситуации, включително взети решения, последвани стъпки, окончателно време за възстановяване. v. 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.
3	e) Периодичен преглед и преработка на стратегията за непрекъснатост на услугите. f) Преглед и преработка на плановете за действие при извънредни ситуации въз основа на минали инциденти и промени.	vi. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) Подготовка за възстановяване и подновяване на услугите след бедствия.	i. Съществуват мерки за справяне с бедствия, като отказоустойчиви сайтове в други региони, архивиране на критични данни на отдалечени места и т.н.

2	b) Прилагане на политика/процедури за внедряване на възможности за възстановяване при бедствия. c) Прилагане на стандарти за възстановяване на мрежите и услугите при бедствия или осигуряване на наличност от трети страни (като националните мрежи за спешни случаи).	ii. 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). iii. Стандарти за възстановяване на мрежите и услугите при бедствия, като преносимо оборудване, преносими обекти, резервирани обекти и др.
3	d) Създаване на съвременни възможности за възстановяване при бедствия за смекчаване на природни и/или големи бедствия. e) Редовен преглед и актуализиране на способността за възстановяване при бедствия, като се отчитат промени, минали инциденти и резултати от тестове и тренировки.	iv. Съвременни възможности за възстановяване при бедствия, като пълно резервиране и механизми за осигуряване при отказ при справяне с природни и/или големи бедствия. v. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) Прилагане на мониторинг и регистриране при критични системи.	i. Регистри на промените и доклади за мониторинг на критични мрежови и информационни системи.
2	b) Прилагане на политика за регистриране и наблюдение на критичните системи. c) Въвеждане на инструменти за наблюдение на критични системи. d) Въвеждане на инструменти за събиране и съхраняване на регистрите на критични системи.	ii. 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. iii. Инструменти за системи за наблюдение и събиране на данни от регистрите на промените. iv. Списък с данни за наблюдение и регистрационни файлове, в съответствие с политиката.
3	e) Въвеждане на инструменти за автоматизирано събиране и анализ на данни за наблюдение и регистри на промените.	v. Инструменти за улесняване на структурното записване и анализ на мониторинга и регистрите на промените.

	f) Преглед и актуализиране на политика/процедури за регистриране и мониторинг, като се вземат предвид промените и минали инциденти	vi. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) 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.	i.Доклади от минали тренировки за резервни планове и планове за действие при извънредни ситуации.
2	b) 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. c) Сигурност, че проблемите и уроците, извлечени от тренировките, са адресирани от отговорните хора и че съответните процеси и системи се актуализират съобразно.	ii. 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. iii. Доклади за учения и тренировки, показващи изпълнението на плановете за действие при извънредни ситуации, включително уроци, извлечени от ученията. iv. Въпросите и уроците, извлечени от минали тренировки, са били разгледани от отговорните лица.
3	d) 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. e) Включване в тренировки на доставчици и други трети страни, като бизнес партньори или клиенти.	v. Актуализирани планове за тренировки, преглед на коментари и/или регистрите на промените. vi. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) Тестване на мрежи и информационни системи, преди използване или свързването им със съществуващи системи.	i. Доклади от тестове на мрежата и информационните системи, включително тестове след големи промени или въвеждане на нови системи.

2	b) Прилагане на политика/процедури за тестване на мрежови и информационни системи. c) Внедряване на инструменти за автоматизирано тестване.	ii. 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	d) Преглед и актуализиране на политиката/процедурите за тестване, като се вземат предвид промените и миналите инциденти.	iii. Списък с доклади от тестове. iv. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) Уверение, че критичните системи редовно се подлагат на сканиране и тестване на сигурността, особено когато се въвеждат нови системи и следват промени.	i. Доклади от минали сканирания за сигурност и тестове за сигурност.
2	b) Прилагане на политика/ процедури за оценка на сигурността и тестване на сигурността.	ii. 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	c) Оценяване на ефективността на политиката/процедурите за оценка на сигурността и тестване на сигурността. d) Преглед и актуализация на политиката/процедурите за оценки на сигурността и тестване на сигурността, като се вземат предвид промените и минали инциденти.	iii. Списък на докладите за оценка на сигурността и тестове за сигурност. iv. Доклади за последващи действия за оценка и резултати от тестове. v. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) Наблюдение на спазването на стандартите и законовите изисквания.	i. Доклади, описващи резултата от мониторинга на съответствието.

2	b) Прилагане на политика/процедури за наблюдение на съответствието и одит.	ii. 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 подхода на високо ниво за мониторинг на съответствието и одит, шаблони за одиторски доклади. iii. Подробни планове за мониторинг и одит, включително дългосрочни цели и планиране на високо ниво.
3	c) Оценка на политиката/процедурите за съответствие и одит. d) Преглед и актуализиране на политиката/процедурите за съответствие и одит, като се вземат предвид промените и миналите инциденти.	iv. Списък на всички доклади за съответствие и одит. v. 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	Мерки за сигурност	Доказателство за изпълнение
1	a) Извършване на редовно наблюдение на заплахите.	i. 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. ii. Неформално и предварително споделяне на съответната информация за заплахата със съответните организации на двустранна основа.
2	b) Прилагане на разузнавателна програма за заплахи.	iii. Документирана и внедрена програма за разузнаване на заплахи, която включва роли, отговорности, процедури и механизми за събиране на информация, свързана със значителни заплахи и съответни мерки за смекчаване. iv. Програмата включва също механизми за систематично споделяне на информация за заплахата със съответната организация на двустранна и многостранна основа,

		използвайки специална платформа за споделяне на информация за заплахи (напр. MISP). v. Съществува подходяща схема за маркиране на информация за улесняване на споделянето на чувствителна информация за заплаха (например TLP).
3	c) Преглед и актуализиране на програмата за разузнаване на заплахите. d) Програмата за разузнаване на заплахи използва модерни разузнавателни системи за заплахи.	vi. Актуализирана програма за разузнаване на заплахи, преглед на коментари и/или регистрите на промените. vii. Използва се платформа за разузнаване на заплахи (TIP) със съвременна функционалност (напр. консолидиране на емисии за разузнаване на заплахи от различни източници, автоматизация, анализ на сигурността и интеграция с други инструменти за сигурност и т.н.)

Област на сигурност 8: Информираност за заплахи
Цел на сигурност 29: Информиране на потребителите за заплахи

ниво	Мерки за сигурност	Доказателство за изпълнение
1	a) Информиране на крайните потребители на комуникационни мрежи и услуги за конкретни и значителни заплахи за сигурността на мрежата или услугата, които могат да засегнат крайния потребител.	i. Бюлетин за сигурността, специализирана уеб страница за информация за заплахи или друг документиран и тестван механизъм за достигане до крайните потребители в случай на значителни заплахи. ii. Документирани списъци с най-добри практики и препоръки за сигурност за крайните потребители за намаляване на типичните рискове (напр. криптиране, надеждна автентикация, актуализации, архиви, информираност на потребителите и т.н.).
2	b) Приложение на политика/ процедури за редовно осведомяване на крайните потребители относно заплахи за сигурността на мрежата или услугата, които могат да засегнат крайния потребител.	iii. Документирана и внедрена политика за контакт с крайните потребители с определени роли и отговорности, механизми и критерии за идентифициране на значителни заплахи и процедури, инструменти и методи за навременно и подходящо информиране на крайните потребители.

		iv. Политиката включва механизми за идентифициране и споделяне на препоръките и най-добрите практики за крайните потребители за смекчаване на конкретни заплахи.
3	c) Преглед и актуализиране на политиката/процедурите за редовно информиране на крайните потребители относно заплахите за сигурността на мрежата или услугата, които могат да засегнат крайния потребител.	v. Актуализирана политика за уведомяване, преглед на коментари и/ или регистрите на промените.

Приложение №3
Неприложими мерки за сигурност от
Допълнителните мерки за 5G

По цел на сигурност 02: Управление и ръководене на риска
По отношение на Заплахи за 5G мрежи - 2020 на ENISA очакваме рамката да бъде динамична от гледна точка на новорегистрирани заплахи, рискове и различни елементи от технологичната архитектура, които могат да бъдат засегнати. Предвид това не виждаме смисъл конкретните рискове да бъдат изрично залагани като част от Правилата.

По цел на сигурност 04: Сигурност на зависимост от трети страни
По отношение на подхода за рефериране към стандарти за сигурност на доставките от трети страни, които тепърва ще бъдат публикувани:
Покриването на приложимите стандарти, издавани от 3GPP, ETSI, както и GSMA акредитация на оборудването са част от заложените изисквания към нашите доставчици. Въпрос на бъдеща дискусия трябва да бъде колко време ще имаме възможност да дадем на доставчиците да се съобразят с нови публикувани стандарти различни от 3GPP, ETSI, както и нови акредитационни схеми на GSMA.

По цел на сигурност 06: Знания и обучения по сигурност
По отношение на начина, по който да се включат бъдещи специализирани обучения, считаме, че биха могли да бъдат част от нормалния обучителен цикъл на служителите. Такива обучения се включват от доставчика на конкретно решение за нова технологична архитектура. В допълнение могат да се търсят специализирани доставчици на технически обучения на база последната ревизия на 3GPP стандартите.

По цел на сигурност 09:
По отношение на изискванията към мрежовите елементи, считаме за редно част от тях да се отнасят само за крайни устройства, както следва:
Изисквания за изчистване на данни (data clearing) да са приложими за крайни устройства, докато за ревалидиране (re-authentication) да са приложими за мрежови елементи.
Изискванията за "безопасно дистанционно изключване" (failsafe remote shutdown) в случай на кражба на мрежови елементи са неприложими.

По цел на сигурност 13: Използване на криптиране
По отношение на изискването за криптиране на сигнализационен трафик да се прилага съобразно възможностите и особеностите на съответната технология.
Например: криптиране на 5G сигнализационния трафик е приложимо в случай, че се ползва публичен IP пренос.
По отношение на изискването за криптиране на Транспортен трафик между мрежовите функции да не се прилага за собствената мрежа на предприятието.
Считаме, че на база оценка на риска изискването за криптиране на връзката между различни мрежови функции е приложимо само в случай на комуникация на критични мрежови функции, както и да се прилага съобразно възможностите и особеностите на съответната технология.

По цел на сигурност 23: Политики за наблюдение и регистриране
По отношение на изискването приложимостта за наблюдение и запис на сесии при отдалечен достъп, както и роуминг и взаимно свързване, да не се прилага за собствената мрежа на предприятието.

Извършването на мониторинг ще се осъществява с отдалечен достъп, което е с потенциално висок риск за сигурността. Също така са налични ограничения за мониторинг на роуминг и взаимно свързване от гледна точка на мрежовата неутралност и защита на личните данни.

По цел на сигурност 28: Разузнаване на заплахи
Във връзка с изисквания за обмяна на информация свързана със заплахи като част от цел 28 считаме, че би следвало да има активен ангажимент от държавен орган (например CERT) за предоставяне на подходяща платформа за целите на такъв обмен.

Приложение №4
Договори с трети страни за доставка на оборудване, софтуер и управлявани услуги

1. При сключване на договор с доставчици на оборудване (хардуер, софтуер) и управлявани услуги, наречени „трети страни“, предприятието:
а) трябва да предвиди подходящи изисквания за сигурност, включително за:
- гарантиране на качеството на предлаганите продукти и услуги;
- оперативна съвместимост на предлаганите продукти и съответствието им с приложими международни стандарти;
- сигурност на информацията; изисквания, свързани с достъпа на представители на трети страни до информация и активи на предприятието;
- адекватни мерки за защита на личните данни
- последици при неспазване на изискванията за сигурност на информацията;
- условия за гаранционна и/или възложена извънгаранционна поддръжка, включително по отношение на актуализациите на софтуера за осигуряване на сигурността на мрежата;
- 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.

б) може да предвиди подходящи изисквания за сигурност, включително за:
- 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;
- 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;
- за прозрачност на веригата на доставките; третата страна трябва да е способна да докаже произхода на предлагания ресурс/услуга и неговата сигурност;
- 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;
- осигуряване на информация за извършването на редовни одити и оценка на риска на веригата на доставки.

2. Предприятието определя служител/служители, отговарящ/отговарящи за спазване на изискванията по т. 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. Предприятието предвижда парични санкции за неизпълнение на договорите с трети страни – доставчици на оборудване, а когато е приложимо разваляне на договорите.