This document is to be considered as a **non-exhaustive model**.
Data are given as non-representative sample.

Support document for the preparation of a security plan

Operator's name

Address

Contact person

Considerations

This document is intended to assist operators in preparing their security plan.

More information can be found in the two guidelines below published by ENISA[1]:

- Technical Guideline on Security Measures.
- Technical Guideline on Threats and Assets.

[1] https://www.enisa.europa.eu/publications

Content of an OSP

1. General description of the critical infrastructure

1.1. Overview of the delivered services

1.1.1. Voice

1. Mobile
2. Fixed

1.1.2.Data

1. Mobile
2. Fixed

1.1.3.Internet

1.1.4.Other mobile services

1.1.5.Other fixed services

1.2. Overview of the critical infrastructures

1.1.6.Physical (per site)

1. Locations

Location	Address	Type
BRUSSELS-DC	GPS coordinates Street name …	Datacenter
BRUSSELS-NO	GPS coordinates Street name …	Network office

1.1.7.Logical (HLD)

Per service defined in section 1, an explanation and a plan of the supporting infrastructure.

1.1.8.Services oriented (service: on which site, redundancy …)

Per asset located in a critical infrastructure, a list to point out where assets are, which services they are supporting and how redundant they are.

Site	Location								
Services	Fixed			Mobile			Internet	Redundancy	Type of redundancy
	Voice	Data	Other	Voice	Data	Other		Intersites, local, none	N+1, fibres, generator….
BSC				x	x	x		Intersites	Double coverage
RNC				x	x	x		Intersites	Double coverage
Edge RTR	x	x	x	x	x	x		Local	at card level

Assets to be taken into account (as relevant):

Feeder	LE (Local Exchange)	PoP (IP transit)
Routers	TAX	Twisted (copper) pair
Edge routers	Tandem exchange	Coaxial cables
SBC	MSC	Optical fibres
HLR/AUC	VLR	SMS-C
HSS	SGSN	MMS-C
BTS	GGSN	Diesel generator
BSC	SGW	UPS
NodeB and eNodeB	ePDG	STP
RNC	SDH, ADM, ROADM, ODXC	SCP
MME	WDM and DWDM	Firewall
ANDSF	DHCP	Hypervisor
PCRF	DNS	IXPs

2. Risk analysis

2.1. Impact analysis overview

A list where the significance/potential impact (as a % of the total number of customers) of each location identified in 1.1.6.1 is examined in relation with each delivered service (1).

Location	Voice Mobile 2G	Internet Mobile 2G	Internet Mobile 3G	Internet Mobile 4G	Voice Fixed	….	Significance (Very low … very high)
BRUSSELS-DC	30%	40%	10%	50%	Nihil		High

2.2. Scenarios

2.2.1. Threats

Inventory and description of the threats that are taken into account in the study:

Threats	Description	Likelihood (scale hereunder)
Software bug		Credible
Vandalism	Act of gratuitous deterioration of the infrastructure.	Credible

Non-exhaustive list of threats:

- Electromagnetic interference
- Hardware theft
- Hardware failure
- Software bug
- Faulty hardware change/update
- Faulty software change/update
- Overload
- Network traffic hijack
- Malware and viruses
- Advanced persistent threat
- Policy/procedure flaw
- Spying
- Kidnapping/Hijacking
- Human errors
- Malicious intents of internal employees
- Denial of Service attack
- Power/Cables/Cooling outage
- Design error
- Security shutdown
- Natural disaster
- Fire
- Arson
- Fuel/Water exhaustion
- Terrorist attack
- Vandalism
- Others

2.2.2. Risk matrix

Risks can be assessed based on their potential impact and their likelihood:

Risks		Likelihood				
		Minimal	Unlikely	Possible	Credible	Frequent
Impact	Minor	Very Low	Very Low	Low	Low	Moderate
	Noticeable	Very Low	Low	Low	Moderate	High
	Moderate	Low	Low	Moderate	High	High
	Severe	Low	Moderate	High	High	Very high
	Catastrophic	Moderate	High	High	Very high	Very high

3. Permanent measures

3.1. Inventory

Inventory and description of the existing measures preventing the threats identified in section 2 per site.

Residual impact of the threats identified in section 2 after measures are taken into account.

Site	BRUSSELS-DC				
Threats	Vulnerabilities	Permanent measures	Residual impact per service	Residual likelihood	Residual risk
Power outage	Only one generator	Redundant transformer Generator with 3 days of fuel	Mobile voice: Moderate Fixed voice: Low	Minimal	Mobile voice: low Fixed: lery low
Fire	Electrical component. High temperature of the device	Argonite system. Extinguishers in all rooms. Direct line to 101.	Noticeable	Possible	Low

3.2. Remote autonomy

Site	Presence	Remote service	Remote access	Contingency
BRUSSELS-DC	24/7	Supervision: NOC	Fixed voice (2 physical cables) Fixed data (1 fibre)	Mobile phone from other provider. Replace fibre/cable.
LEUVEN-RTR	Working day 0700-1700	Supervision: NOC Badge service: BRUSSELS-DC.	Fixed voice (1 physical cable) Fixed data (4 logical links + 2 different fibre entries)	Permanence on site within 2 hours. Keypass available in NOC. ….

3.3. Physical security

Location	Security elements							
	Guards	Gate	Doors	Zones	Badge system	Key	CCTV	Alarm
BRUSSELS-DC	YES Private security firm 24/7	YES	YES	Different zones.	YES	Permanence + On-site personel	YES 1 week recording	FIRE + Intrusion + Flood.
LEUVEN-RTR	No	No	YES	Only 1 security zone.	YES	NOC + Permanence	YES 1 week recording	FIRE + Intrusion + Flood.

4. Graduated measures

4.1. General graduated measures

Inventory and description of the existing measures preventing the threats identified in 2.

Threshold triggering the gradual measures.

Threats	Gradual measures	Trigger
Terrorist attack	Security barriers are closed. ….	CUTA 4

4.2. Specific gradual measures

4.2.1. Prioritisation between services

In case of major failure, the service will be restarted in the following order:

- …

4.2.2. Communication plan.

Trigger/Impact	Communication means	Description
Voice fixed >100,000	SMS/Media	Expected repair time
…		

4.2.3. Measures to minimise impact

Per threat and, if needed, per site or asset, list of the actions undertaken in case of threat occurrence.

Threats	Sites	Assets	Actions
Fire	All sites	All assets	• Argonite system activation. • Physical check . • Call firefighters. Or see Manual section XXX (to provide)
Power outage	All sites	All assets	• Outdoor generator installation. • ….
Hardware failure	BRUSSELS_DC	Router	• Manual rerouting of traffic. • Bring spare on site. • ….

4.2.4. Recovery processes

Measures in place to recover a site from crash per asset.

Sites	Assets	Spare	Recovery process
BRUSSELS_DC	Router	YES	• Pick up the spare in central store. • Upgrade router. • Load router with latest backup configuration (max 24 h old) • Inspect failed router to find out the root cause of the failure.
BRUSSEL-DC	MME racks	YES in contingency container	• Bring the contingency container on site. • Connection of the container. • Start-up of the container. • ….

5. Operational test

Planning of the main tests:

Critical infra	Type of tests	Purpose of the tests	Frequency	Tests limitations
All critical sites	Power supply	Test of the generator	1/month	No load.
BRUSSELS-DC	Air cooling	Test of the backup system	1/year.	None.

6. Annexes

6.1. Vendors dependency per asset

Assets	Vendors	Type	Services	Dependency	Escalation	Vendors / Company delivering support Security Assessment
Edge routers	Router maker	RouterXXX	ALL	Need support to operate	Level 1: BE Telecom - Belgium Level 2: Telco Company - India	Router maker: Internal BE Telecom: Authority Telco Company: Internal

Services field refer to services defined in section 1.1.

Dependency has to be evaluated as below:

- No need of support to operate.
- Need support to operate.
- Need support to install/replace (parts of) devices.
- Other.

Escalation field must contain the different escalation levels, the country where it is operating and the company name.

The security assessment field must contain per vendor/company delivering support the type of security assessment that occurred during the contractual phase:

- Internal: internal assessment executed by the operator.
- External: external assessment executed by a private entity.
- Authority: external assessment executed by a government entity.
- None.

6.2. Others