ΚΟΙΝΟΠΡΑΞΙΑ: ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ, ΥΠΟΥΡΓΕΙΟ ΥΓΕΙΑΣ ΚΑΙ ΕΘΝΙΚΗ ΑΡΧΗ ΗΛΕΚΤΡΟΝΙΚΗΣ ΥΓΕΙΑΣ

Project Title:

Deployment of Generic Cross Border eHealth Services in Cyprus

Agreement number: INEA/CEF/ICT/A2015/11S1451

Action No: 2015-CY-IA-0095

Title: Annex OP 1 Service Operation Plan - Cyprus

Based on:

CEF eHealth DSI

Patient Summary and ePrescription

Service Operation Plan

Cyprus

Original document

Version: 2017-06-20

Date: V0.1 (template)

Author(s): eHDSI

Release: v6.0

Αρ. Αναφ. Φακέλου: ΠΚ/2018/05/15

Λευκωσία

30 Ιουνίου, 2020

Βασικές Πληροφορίες Έργου

Πληροφορίες Έργου	
Τίτλος Έργου	**NCPeH CY**
Κωδικός Έργου	***2015-CY-IA-0095***
Ιδιοκτήτης Έργου	**ΕΘΝΙΚΗ ΑΡΧΗ ΗΛΕΚΤΡΟΝΙΚΗΣ ΥΓΕΙΑΣ**
Στοιχεία Επικοινωνίας Συντονιστή έργου	Καθ. Κωνσταντίνος Παττίχης, Τμήμα Πληροφορικής, Πανεπιστήμιο Κύπρου, Λεωφόρος Πανεπιστημίου 1 Αγλαντζιά Λευκωσία 2109 ΚΥΠΡΟΣ (+357) 22892697 (+357) 22892701 pattichi@cs.ucy.ac.cy

ΙΣΤΟΡΙΚΟ ΑΝΑΘΕΩΡΗΣΕΩΝ

Αριθμός Έκδοσης	Ημερομηνία	Συγγραφείς	Εκδότης	Αναθεώρηση
1	14/05/2018	Καθ. Παττίχης Κωνσταντίνος Δρ Μηνάς Κυριακίδης Μόνικα Καλακουτή Δρ Μάριος Νεοφύτου	ΥΥ & ΠΚ	Πρώτο Προσχέδιο /
2	18/06/2018	Καθ. Παττίχης Κωνσταντίνος Δρ Μηνάς Κυριακίδης Μόνικα Καλακουτή Δρ Μάριος Νεοφύτου	ΥΥ & ΠΚ	Δεύτερο Προσχέδιο
3	25/06/2018	Καθ. Παττίχης Κωνσταντίνος Δρ Μηνάς Κυριακίδης Μόνικα Καλακουτή Δρ Μάριος Νεοφύτου	ΥΥ & ΠΚ	Τρίτο Προσχέδιο
4	14/09/2018	Καθ. Παττίχης Κωνσταντίνος Δρ Μηνάς Κυριακίδης Μάριος Νεοφύτου	ΥΥ & ΠΚ	Τέταρτο Προσχέδιο
5	08/07/2019	Καθ. Παττίχης Κωνσταντίνος Δρ Μηνάς Κυριακίδης	ΥΥ & ΠΚ	Πέμπτο Προσχέδιο

6	30/06/2020	Καθ. Παττίχης Κωνσταντίνος Ηρακλής Κυριακίδης	ΥΥ & ΠΚ & ΕΑΗΥ	Τελική έκδοση Έγινε αλλαγή στο ιδιοκτήτη του NCPeH. Η ΕΑΗΥ είναι ο νόμιμος ιδιοκτήτης. MOH change to NeHA as the legal authority

Θεώρηση Εντύπου

Όνομα	Ιδιότητα	Ημερ. Θεώρησης
Δρ Βάσος Σκουτέλλας	Συντονιστής ελέγχου ποιότητας παραδοτέων	07/10/2020

Έγκριση Εντύπου

Όνομα	Ιδιότητα	Ημερ. Έγκρισης
Καθ. Χρίστος Σχίζας	Πρόεδρος Εθνικής Αρχής Ηλεκτρονική Υγείας	08/10/2020

Executive Summary

The purpose of this document is to provide information about how the NCPeH CY service for cross border health care is provided, operated and managed. Moreover, the document provides useful information how the service follows-adopts the MOH procedures.

Service operations are described, covering change management and emergency change management, followed by event management, incident management, problem management, request fulfilment and access management as adopted for operations of NCPeH. Furthermore, it is noted that the service operations are supported by the Service Desk Monitoring Tool.

Furthermore, the NCPeH CY service operations organogram and functions for NEHA, MOH and UCY are given, followed by sections on Technical Management, Applications Management and Operations Management, guaranteeing a smooth operation of service.

Table of Content

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

Σύντμηση	Πλήρης επεξήγηση
CBeHIS	Cross Border electronic Health Information System (Διασυνοριακό ηλεκτρονικό Πληροφοριακό Σύστημα Υγείας)
CEF	Connecting Europe Facility (Συνδέοντας την Ευρώπη)
eD	eDispensation (ηλεκτρονική Εκτέλεση συνταγής)
eP	ePrescription (ηλεκτρονική Συνταγή)
INEA	Innovations & Networks Executive Agency
MTC	Master Terminology Catalogue
NCPeH	National Contact Point electronic Health
PS	Patient Summary (Συνοπτικό Ιστορικό Υγείας)
ΓΝΑ	Γενικό Νοσοκομείο Αμμοχώστου
ΕΕ	Ευρωπαϊκή Ένωση
ΙΥ	Ιατρικές Υπηρεσίες
ΚΕΠ	Κέντρο Εξυπηρέτησης Πολιτών
ΚΜ	Κράτος Μέλος
ΜΠ	Μονάδα Πληροφορικής Υπουργείου Υγείας
ΜΠΥ	Μονάδα Παρακολούθησης Υγείας
ΟΠΣΥ	Ολοκληρωμένο Πληροφοριακό Σύστημα Υγείας
ΠΙΣ	Παγκύπριος Ιατρικός Σύλλογος
ΠΦΣ	Παγκύπριος Φαρμακευτικός Σύλλογος
ΠΚ	Πανεπιστήμιο Κύπρου
ΤΑΕΠ	Τμήμα Ατυχημάτων & Επειγόντων Περιστατικών
ΥΥ	Υπουργείο Υγείας
ΦΥ	Φαρμακευτικές Υπηρεσίες

1 Introduction

[*Strategic objectives are ultimately realized through service operation. ITIL Service Operation provides guidance on how to maintain stability in service operation, allowing for changes in design, scale, scope and service levels*.

Provide your country perspective on how this operational plan will support your country to realize strategic objectives as well as handle reactive and proactive change management]

The Cyprus NCPeH will act as the national contact point, adhering to the Directive and ensuring a better and safer cross-border health care. Overall, Cyprus is in line with the objectives of Directive 2011/24/EU and the deployment of the eHealth cross-border services shall contribute in the offering of better quality of care and its continuum throughout the EU. This will be facilitated by providing immediate clinical information needed in an emergency situation abroad and ensuring continuity of care across EU borders.

Based on the ITIL service operation guidelines the operation management plan will support NCYeH CY to maintain stability in service operation, allowing for changes in design, scale, scope and service levels.

1.1 Purpose

[*Service operation is responsible for ongoing management of the technology that is used to deliver and support services. Well designed and well implemented processes will be of little value if day to day operation of those processes is not properly conducted, controlled and managed; nor will service improvements be possible if day to day activities to monitor performance, assess metrics and gather data are not systematically conducted during service operation.*
Operational objectives include:

- *Responsive stable services*
- *Robust end to end operational practices*
- *Business as usual – day to day*
- *Execution of processes and services*
- *Responsive and operational validation*
- *Realising value*
- *Achieving service excellence*

Description of the aim this document]

The purpose of this document is to provide information about how the NCPeH CY service for cross border health care is provided, operated and managed. Moreover, the document provides useful information how the service follows-adopts the NEHA and the MOH procedures.

1.2 Scope

[***Services*** *- All activities associated with operational services regardless of whether they are executed by the service provider, a third party supplier or by users and customers.*
Service management processes *- Operational aspects of all processes whatever part of the lifecycle they originate from (e.g. operational aspects of capacity and availability management).*
Technology *- Management of the technology delivering the services.*
People *- The people managing the services, processes and technology.*
Describe how you envisage the scope in your country]

Service level agreements with all related third party service providers are strictly followed and monitored as documented in the corresponding agreements given in Annex OS 3.

All the above agreements are available upon request.

- Annex OS 3 Third parties service agreements
- Annex OS 4 Contract signed with GNOMON

1.3 Target Groups

[***Overall description on the different groups of people considered and audience for this document***]

This document will be communicated to the groups pf people documented in:

- Annex OP 2 Operation and Organizational Structure, section 6 Structure - NCPeH CY Organogram and Roles

Moreover, this document will be communicated to the health professionals who are users of the NCPeH services, i.e. the doctors and the pharmacists.

1.4 Articulation with other Deploying Countries

[**Perspective on possible liaison and cooperation activities *with other, regarding operations management***]

Cyprus will follow MLAs agreements signed with each EU deploying country so as to make possible the smooth operation of the cross border services.

1.5 References

REFERENCE	TYPE[1]	URL
Information Technology Infrastructure Library (ITIL) – [OpenCampus]	Methodology, web page	URL
ITIL – Introducing service operation [UCISA]	Article	URL
Service Operation materials [UCISA]	Resource index	URL
ITIL – Introduction to Service Desk [UCISA]	Article	URL
ITIL – Introducing service transition [UCISA]	Article	URL

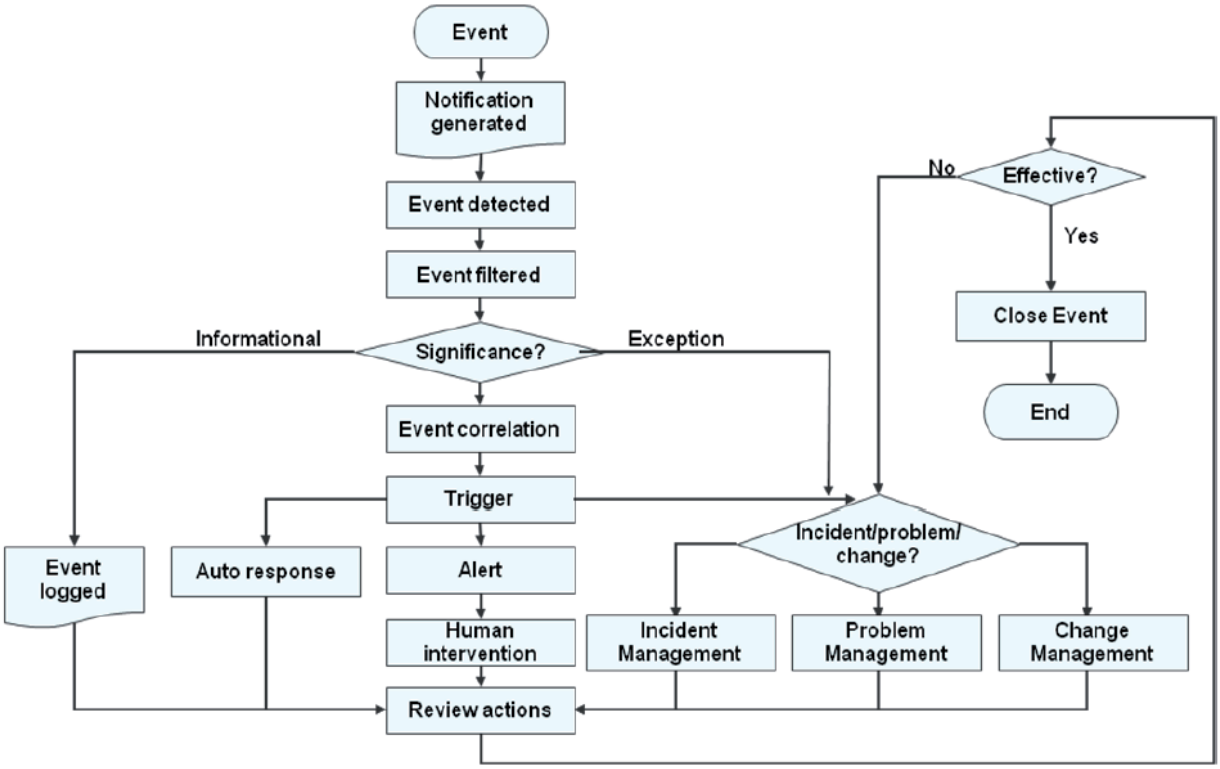
[1] Type: e.g. methodology, article, video, regulation, specification

2 Service Operation

[*Describe the rationale underlying your country Service Operation Plan design*]

The rationale followed by NCPeH for service operation is aligned with the following event flowchart documented in reference[2].

Event flowchart documented in reference [2] as adopted for operations of NCPeH



In this section Change Management and Emergency Change Management are documented as adopted for operations of NCPeH based on reference[3]. These are followed by Event Management, Incident Management, Problem Management, Request Fulfilment and Access Management as adopted for operations of NCPeH based on reference[4].

Furthermore, it is noted that the service operations are supported by the Service Desk Monitoring Tool (given in Annex OP 9 Service Desk Monitoring Tool).

KEY SERVICE	RATIONAL [4]
Event Management	Manages events throughout their life cycle. This life cycle includes coordination activities to detect events. Make sense of them and determine the appropriate control action.
Incident Management	Concentrates on restoring unexpectedly degraded or disrupted services to users as quickly as possible, in order to minimize business impact.

[2] Introduction to Service Operation [UCISA] (page 15) - URL

[3] EU Employment, Social Affairs & Inclusion, EESSI Change Management Guide, Version 1.0, https://ec.europa.eu/social/main.jsp?catId=1028&langId=en

[4]Service Operation – Processes https://www.greycampus.com/opencampus/itil-foundation/service-operation-processes

Problem management	Involves root cause analysis to determine and resolve the underlying causes of incidents, and proactive activities to detect and prevent future problems/incidents. This also includes the creation of known error records, that document root causes and workarounds to allow quicker diagnosis, and Resolution should further incidents occur.
Request fulfilment	Is the process for managing the life cycle of all service requests. Service requests are managed throughout their life cycle from initial request to fulfilment using separate request fulfilment records/tables to record and track their status. They are the mechanism by which users formally request something from an IT service provider.
Access management	Is the process of granting authorized users the rights to use a service while restricting access to non-authorized users. It is based on being able accurately to identify authorized users and then manage their ability to. Access services as required for their specific organizational role or job function. Access management has also been called identity or rights management in some organizations.

3 Change Management Procedures

The Change Management Procedures adopted for operations of NCPeH are based on reference [3]. See also, the Event flowchart documented in the beginning of section 2 Service Operations, based in reference [2] as adopted for operations of NCPeH for the handling of Events, Incidents/Problems and Changes.

3.1 Change Requests

Representatives of NCPeH Project Stakeholders can propose Change Requests for approved project artefacts during the development and implementation of the solution.

The NCPeH Desk may also formulate Change Requests, based on input received from the:

- Local Project Manager Board & Local Scientific Advisory Board decisions

Change Requests can also be raised by the NCPeH Project Team based on:

- Member States feedback
- Conformance testing
- Changes required to encompass Architecture or Project Direction changes
- Changes in the relevant legislation
- Risk response
- Issues identified from testing and operations.

For the purpose of this procedure, all the above audiences can be considered as having the **Reporter** role.

3.1.1 Summary of Change Management Process

3.1.1.1 Change Identification

When a Change Request is first created, it is saved in **Draft** state. While in Draft, the Change Request can be edited by and completed with additional details. The Reporter can upload documentation to support the Change Request.

When the information about Change Request is complete, the **Reporter** can **submit** the Change Request to the Help Desk.

The Service Desk will verify the Change Request for completeness and applicability to the project scope.

- If the Change Request is complete and contains the necessary details, it will be **sent to investigate** the relevant Expert for performing the Impact Assessment.
- If the Change Request is incomplete, it will be sent to the Change Request back in **Draft** state and assign it to the Reporter to provide additional details.
- If the Change Request is not applicable to the approved project artefacts (currently Documentation, Business Model and Software) it will be marked **Out of Scope** and **Closed**. Another issue type (by example an Incident) may be created by the Reporter.

3.1.1.2 Change Assessment and Prioritization

While the Change Request is in the **investigating** state, it is assigned to an NCPeH Expert who will perform the Impact Assessment. This document can be completed with support from multiple disciplines and describes the impact of the change in various areas of the project.

After completion, the document is recorded in the Change Request tool (see Annex 9 Service Desk Monitoring Tool), and **Impact** value is updated based on the information contained in the document. The Change Request is then **sent for Approval**.

Prioritization of the Change Requests will be made based on the recommendation from the NCPeH Expert and it will be reflected in the Priority field. The Priority can be revised by the Project Board.

After **Impact Assessment Form (IA)** is completed for a Change Request, a notification needs to be sent.

Project Board members are responsible to monitor the new Change Request submitted, and provide feedback on impact analysis regarding the national domain implementation.

3.1.1.3 Change Approval

The Change Requests for which impact assessment was completed and have Impact Assessment form attached are sent for approval. The approval process varies depending on the impact value.

- If the Impact is **Low** or **Medium**, the Change Requests needs to be approved by Project Board.
- If the Impact is **High** or **Very High**, the Change Requests needs to be referred to the Scientific Advisory board as well.

Project Board meets every 3 months (4 times / year). Additional meetings may be scheduled if there are many change requests that need to be approved. The following actions can be taken by the Project Board:

- **Reject** - This status is set when the approval process is successfully completed.
- **Approve** - This status is set when the approval process leads to rejection of the change request.
- **Merge** - This status indicates that this change has been merged into some other change so it is no longer being actively handled. Merging is common when large numbers of changes are being used. This will also be used if a Change Requests is a duplicate of existing Change Requests / included in already scheduled development.

The responsibility of the Project Board ends after approval/ rejection/ merging of each Change Request.

3.1.2 Change Implementation

The approved Change Requests will follow the next stages according to the Release process:

- **Planned** - This status indicates that this change is already updated in the Work Schedule/Project Plan.
- **Postponed** - This status is set for postponing the action to a certain date.
- **In Development** - This status indicates that this change is under development according to NCPeH related methodology.
- **Closed (Delivered)** - This status indicates that the change request has been made available for use by the relevant user groups.

The changes will be thoroughly tested before release into the operational environment.

3.1.3 Impact assessment form

Impact categories	None	Low	Medium	High	Very High
Impact to implement (by Project Board)	✓				
Impact on National Implementation	✓				
Impact on eHDSI Solution Provider	✓				
Impact on National Domain	✓				
Impact on Project Planning	✓				
Impact on Architecture	✓				
Impact on Business	✓				
Impact on Operations & Deployment	✓				
Impact on Security	✓				

3.2 Emergency Changes Procedure

The Change Procedures adopted for operations of NCPeH are based on reference[3]. See also, the Event flowchart documented in the beginning of section 2 Service Operations, based in reference [2] as adopted for operations of NCPeH for the handling of Events, Incidents/Problems and Changes.

3.2.1 Definition

Emergency change is a change that can be classified as critical or blocking, which is normally corrective in nature and requires urgent action for remediation, otherwise the issue will have a severe impact on the normal operation of NCPeH. Examples of emergency changes that could occur in NCPeH include:

- Data loss issue
- Major security issue
- Business Process step missing in software solution
- Missing Data items in electronic transactions
- Critical software functionality defect.

In all of these cases, wherever a change is identified as a potential emergency change the process to be followed will be simplified to the following:

> Change identified and the consequence of the change establishes this as an emergency change and therefore it does not require an impact assessment from the Project Board to determine the necessity for the change.
>
> Where a change is classified by the Project Manager as an emergency change, the decision point for resolution will be made by the Project Board.

3.2.2 Severity (urgency, priority & stop service)

The status can be assigned by the reporter, but the value may be later adapted by the Service Desk (also recorded by the Service Desk Monitoring Tool):

Blocker *Normal functioning is blocked*

- system unavailable, system crashes, system "hangs"
- users can't work, users are dropped out of the system
- user or system data are lost permanently without recovery
- inability of a process to perform

Immediate resolution (reaction) or work around is required

Critical *Normal functioning is drastically impacted*

- The issue causes impairment of critical system functions
- eP & Ps affected, but can be implemented with SLA breach
- No workaround exists

Urgent resolution (reaction) is required

Major *Normal functioning is somewhat impacted* ***(Default)***

- The issue causes impairment of one or more system functions
- User or system data may be lost or performance drastically degraded.
- workaround exists and eP&PS are implemented

Resolution (reaction) is required as soon as possible

Minor *Normal functioning is slightly impacted*

- loss of some functionality with workaround
- partial loss of a functionality

Resolution (reaction) within a limited timeframe

Trivial *Normal functioning is slightly or not impacted*

- System available and functions correct, but cumbersome to work with (e.g. poor response or poor screen flows)
- User interface or minor changes (e.g. spelling errors, translation errors, screen layout, etc.)
- Specific non-essential reports are not correct

3.2.3 Priority

Priority of the change request, from the perspective of the project team.

- Blocker
- Critical
- Major (default)
- Minor
- Trivial.

3.2.4 Impact Area

Impact area has a supporting role in impact assessment, and can have one of the following values:

- NCPeH, if the change is affecting the system as a whole
- International domain, if the change is affecting one or more of the international domain components
- National level, if the change is affecting national domain as a whole in at least one country
- Institutional domain, if the change is affecting a particular institution or set of institutions
- Individual if the change is affecting some individuals, but all the PS&eP/eD are running.

3.2.5 Level of the impact for the proposed change Request

- Very Low - the impact of change is minimal and can be absorbed as part of normal operations;
- Low - the impact of change is minimal and it has little effect on users, implementation, costs, project plan, architecture, business or operations;
- Medium - the impact of change is minimal an it has moderate effects in terms of users affected (one or few institutions), costs to implement;

- High – the impact of change on users is important (many institutions and users are affected), it requires significant efforts and costs to develop and implement;
- Very High – the impact of change on end-users is major (all users and institutions are affected), change is difficult to implement, impossible to revert, involves high risks and high costs.

The Impact level is determined by the Project Board after performing the Impact Assessment.

- **If the Impact is Low or Medium, the Change Request needs to be approved by Project Board;**
- **If the Impact is High or Very High, the Change Request needs to be approved also by Project.**

3.2.6 Beneficiaries and stakeholders notification

Beneficiaries and stakeholders affected by emergency changes that impact the service and routine operations are notified via email and announcements in the NCPeH CY website.

3.3 Event Management

An Event is defined as a change of state that has significance for the management of a configuration item or IT service.

The Event Management Procedures adopted for operations of NCPeH are based on reference (pages 12-16) [4]. See also, the Event flowchart documented in the beginning of section 2 Service Operations, based in reference [2] as adopted for operations of NCPeH for the handling of Events, Incidents/Problems and Changes.

Purpose to manage events throughout their lifecycle is the purpose of event management. This life cycle of activities to detect events, make sense of them and determine the appropriate control action, which is coordinated by the event management process. Event management is therefore the basis for operational monitoring and control.
If events are programmed to communicate operational information as well as warnings and exceptions, they can be used as a basis for automating many routine operations management activities.
Example: Executing scripts on remote devices, or submitting jobs for processing, or even dynamically balancing the demand for a service across multiple devices to enhance performance.
An event can be defined as any change of state that has significance for the management of a configuration item (CI) or IT service. Events are typically recognized through notifications created by an IT service, CI or monitoring tool. Effective service operation is dependent on knowing the status of the infrastructure and detecting any deviation from normal or expected operation.

3.3.1 Objectives

Event management provides the entry point for the execution of many service operation processes and activities. In addition, it provides a way of comparing actual performance and behaviour against design standards and Service Level Agreements. More specifically:

- Provides the ability to detect, interpret and initiate appropriate action for events
- **Is the basis for operational monitoring and control and the entry point for many service operation activities**
- Provides operational information as well as warnings and exceptions to aid automation
- Supports continual service improvement activities of service assurance and reporting.

The objectives of the event management process are to:

1. Detect all changes of state that have significance for the management of a Cl or IT service
2. Determine the appropriate control action for events, and ensure these are communicated to the appropriate functions
3. Provide the trigger, or entry point, for the execution of many service operation processes and operations management activities
4. Provide the means to compare actual operating performance and behavior against design standards and SLAs
5. Provide a basis for service assurance and reporting; and service improvement

3.3.2 Types of events

- **Informational Events**
  Events providing us with information like a scheduled workload has been completed. For example, a user has logged in to use an application and an email has reached its intended recipient. For more information please see Annex OP 3 Zabbix Open-source monitoring Tool.

- **Warning Events**
  Events providing us alerts when set thresholds levels have been achieved. For example, a server's memory utilization reaches within 5% of its highest acceptable performance level see Annex OP 3 Zabbix Open-source monitoring Tool).

- **Exceptional Events**
  Events indicating that a service operates abnormally. For example, a PC scan reveals the installation of unauthorized software, (see Annex OP 3 Zabbix Open-source monitoring Tool).

3.3.3 Process

Events are handled in a similar way to the Change Management Procedure, see sections 2.1.2 Summary of Change Management Process, 2.1.3 Change Implementation and 2.1.4 Impact assessment form.

3.4 Incident and Problem Management

The Incident and Problem Management Procedures adopted for operations of NCPeH are based on references[5],[6]. See also, the Event flowchart documented in the beginning of section 2 Service Operations, based in reference [2] as adopted for operations of NCPeH for the handling of Events, Incidents/Problems and Changes.

See also, Annex 7 Business Continuity Procedures, sections 3 and 4

3.4.1 Incident and Problem

3.4.1.1 Definition and lifecycle

An incident might affect any (or a combination) of the key properties: availability, confidentiality (including accountability) and integrity of the NCPeH.
A Problem is indicated by a single or a series of unwanted or unexpected events that have a significant probability of compromising business operations and threatening information security.

Examples of problems are (not an exhaustive list):

- loss of service, equipment or facilities
- system malfunctions or overloads
- detected vulnerabilities and/or threats
- breaches of physical or other security arrangements
- uncontrolled system changes
- access violations (intrusion to the network, application, system or building)
- laptop stolen or lost
- misrouting of information
- denial of service
- installation of a patch which opens a vulnerability or system problem
- malicious code
- information leakage or information theft
- unauthorized modification or elevation of access rights
- breach in confidentiality or integrity
- non-compliances with policies or guidelines
- misuse of system
- suspicion of someone breaking the law
- terrorism or cyber-terrorism suspicions
- others (e.g. directly or indirectly affecting secure operations of the system).

[5] Employment, Social Affairs & Inclusion EESSI Security Communications & Operations Policy, https://ec.europa.eu/social/main.jsp?catId=1028&langId=en

[6] IBM Project Initiation Document for MOH IHCIS

3.4.2 Policy statements and requirements

Actions

The specific operational activities of NCPeH incident handling are summarized in four main phases:

- **Preparation**: incident response methodologies typically emphasize preparation – not only establishing an incident response capability in order to respond to incidents, but also preventing incidents.
- **Identification and Analysis**: identification/detection of security incidents is necessary to alert the involved stakeholders whenever incidents occur. Proper analysis is needed to rule out false positives and to determine impact and containment strategies. This step includes the classification of the incident.
- **Containment, Eradication and Recovery**: when an incident has been detected and analyzed, it is important to contain it before the spread of the incident overwhelms resources or the damage increases. Most incidents require containment, so it is important to consider it early in the course of handling each incident.
- **Post-Incident activities**: a key part of the incident response is also the most often omitted: awareness, training and improving. The incident response team should evolve to reflect new threats, improved technology, and lessons learned.

Incident service management

The objectives of the incident management process are to:

1. Ensure that standardized methods and procedures are used for efficient and prompt response, analysis, documentation, ongoing management and reporting of incidents.
2. Increase visibility and communication of incidents to business and IT support staff.
3. Enhance business perception of IT through use of a professional approach in quickly resolving and communicating incidents when they occur.
4. Align incident management activities and priorities with those of the business.
5. Maintain user satisfaction with the quality of IT services.

A range of resources are available in order to manage the NCPeH related incidents (including specific / applicable information security incidents). NCPeH has implemented the following:

- A set of people dedicated to incidents response with enough technical and communications skills to face any incident.
- Physical room or building where security incidents can be treated and tracked in a safe way.
- The response team NCPeH Service Desk have the appropriate hardware and software toolsets to handle a wide spectrum of incidents.
- Communication lines: the following communication lines are available – as a minimum - to report incidents, in this preferred order:
    - **Phone (the number is 22604100) 24 by 7**
    - **eMail: ncphelpdesk@cs.ucy.ac.cy.**

  All this operational components and channels are available on a 24x7 basis.
- Tools: The service desk is using the Service Desk Monitoring Tool (given in Annex 9) to identify, classify and monitor incidents and problems.

The following table tabulates selected security incidents, their corresponding severity and a maximum reporting and resolution timeframes (based on the aforementioned references[5,6]). (see Annex OP 3 Zabbix Open-source monitoring Tool and Annex OP 9 Service Desk Monitoring Tool).

Table of Selected Security Incidents, Severity and Reporting and Resolution Timeframes

Security incident type	Further description	Severity	Reporting maximum timeframe	Resolve maximum timeframe
Unauthorised access to system	International domain	HIGH	1 hour	1 day
Unauthorised access to system	eP&Ps	- if privileged accounts: HIGH - otherwise: MEDIUM	1 hour 4 hours	1 day 2 day
Unauthorised physical access to infrastructure	International domain	HIGH	1 hour	1 day
Unauthorised physical access to infrastructure	National domain	MEDIUM	4 hours	2 day
Personal information disclosure	Massive NCPeH disclosure	HIGH	1 hour	6 hours
Personal information disclosure	Disclosure of one or a few SEDs	MEDIUM	1 day	2 days
Abusive content	As an attachment of documents	- if containing personal data or fraudulent: HIGH - otherwise MEDIUM	1 day 1 week	2 day 2 weeks
Availability – Denial of service	Denial of service attack at national level	- not NCPeH targeted: MEDIUM - if NCPeH targeted HIGH	4 hours 2 hours	1 day 12 hours
Availability – Denial of service	Denial of service attack at international level	HIGH	1 hour	1 day
Malicious code	Immediately removed	LOW	1 week	2 days
Malicious code	Spread in national domain - not blocking	MEDIUM	2 hours	1 day
Malicious code	Spread in national domain - blocking AP(s)	HIGH	1 hour	6 hours
Unauthorised design information disclosure		MEDIUM	1 day	2 days
System vulnerability and/or threat		Severity depending on the possible consequences of that vulnerability based on existing and possible threats.	From 1 day to 1 week	1 week
Achieving or providing unauthorised administrator level access	Compromising the international or national domain	HIGH	1 hour	1 day
Introduction of unauthorised encryption	International or national domain security bypassed	MEDIUM	1 day	2 days

3.4.3 Security incident state

Security incidents have, at any time, one the following states:

- **Open**: The incident has been communicated and created in the tracking system
- **Under investigation**: In incident is investigated in order to provide a solution
- **Applying solution**: The incident is handled and is in resolution phase
- **Suspended**: It is waiting for some tools, action or investigation
- **Closed**: The incident has been solved or closed
- **Conclusion**: Final analysis has been done about the incident response and solution
- **Concealed** – due to its impact and for security reasons, the incident was classified.

4 RASCI roles & responsibilities for the NCPeH Incident / Problem management process

The following table documents the RASCI roles responsibilities for the NCPeH Incident/Problem management process (based on the aforementioned references[5,6]).

Table of RASCI[7] Matrix for NCPeH incident/problem management

	Prevention	Detection	Notification	Contention	Analysis & Investigation	Solution and recover	Reflection and improve
Anybody	R	R/C	C	C	C	-	-
Project Management Board	A	A	R	C	S	C	I
Security Officer	A/R	S	A/S	R	R	A/R	C
eHealth DSI/eHMSEG	C/S	I	I	A/S	A/S	A	A
Assigned Project Management Board Team	-	I	-	-	I	R	S
Project Management Board & Scientific Advisory Board	C/S	I	-	-	I	I	R

[7]For RASCI definitions, see: https://managementmania.com/en/rasci-responsibility-matrix:

- **R** –**Responsible** - who is responsible for carrying out the entrusted task?
- **A** – **Accountable** (also Approver) - who is responsible for the whole task and who is responsible for what has been done?
- **S** – **Support** - who provides support during the implementation of the activity / process / service?
- **C** – **Consulted** - who can provide valuable advice or consultation for the task?
- **I** – **Informed** - who should be informed about the task progress or the decisions in the task?

4.1 Request fulfilment

Service Request is used as a generic description for many different types of demands that are placed upon the IT department by the users. Many of these are typically requests for small changes that are low risk, frequently performed, low cost etc (i.e. a request to change a password, or may be a request for information) [4].

The Request fulfillment procedures adopted for operations of NCPeH are based on reference [4]. Request fulfillment are handled in a similar way to the Incident/Problem Management Procedures. See also, the Event flowchart documented in the beginning of section 2 Service Operations, based in reference [2] as adopted for operations of NCPeH for the handling of Events, Incidents/Problems and Changes.

4.1.1 Objectives

The objectives of the request fulfilment process are to:

- Maintain user satisfaction through efficient and professional handling of all service requests.
- Provide a channel for users to request and receive standard services for which a predefined authorization and qualification process exists.
- Provide information to users about the availability of services and the procedure for obtaining them.
- Source and deliver the components of requested standard services (e.g. licenses and software media).
- Assist with general information, complaints or comments.

4.1.2 Types of requests and processes

Request fulfillment is the process responsible for managing the life cycle of all service requests from the users. It is the process for dealing with service requests, many of them are actually smaller, or low risk.

Request fulfillment are handled in a similar way to the Incident/Problem Management Procedures, see section 2.4 Incident and Problem Management.

4.2 Access management

Access management is the process of granting authorized users the right to use a service, while preventing access to non-authorized users[4].

The purpose of access management is to provide the right for users to be able to use a service or group of services. It is therefore the execution of policies and actions that are defined in the information security management (as documented in Annex IS 1 Information Security Policy and Procedures).

The Event Management Procedures adopted for operations of NCPeH are based on reference (pages 12-16) [4]. See also, the Event flowchart documented in the beginning of section 2 Service Operations, based in reference [2] as adopted for operations of NCPeH for the handling of Events, Incidents/Problems and Changes.

4.2.1 Objectives

The objectives of the access management process are to:

- Manage access to services based on policies and actions defined in information security management
- Efficiently respond to requests for granting access to services to entitled people
- Oversee access to services and ensure rights being provided are not improperly used.

4.2.2 Access policies, activities and processes

Access management is effectively the execution of the policies in information security management (as documented in Annex IS 1 Information Security Policy and Procedures). Access management ensures that users are given the right to use a service.

Access management is executed by IT operations and supported by the service desk.

Access management related to security incidents and problems will be handled as documented in section 2.4 Incident and Problem Management.

The activities of access management:

Requesting access – Access request in cases of:

- standard request
- request for change
- service request.

Verification – Access management verification request for access to an IT service:

- user requesting access is who they say they are
- have a legitimate requirement for that service.

Providing rights – Access management execution of the defined policies for service provision.

Logging and tracking access – Access management recording of access for the cross border services users.

Removing or restricting rights – Just as access management provides rights to use a service, it is also responsible for revoking those rights. Removing of access in the following cases:

- Death
- Resignation
- Removal of registration license (i.e. from the Pancyprian Medical Association, or from the Cyprus Pharmaceutical Organisation).

5 Service Operation Functions[8]

[***Describe the Service Operations Functions rationale for your country***]

[Figure 1 – Service Operation Functions[9]]

The main objective of service operations is to coordinate and carry out the activities and processes required to deliver and manage services to the users of the NCPeH CY. Service operation functions are required for the ongoing management of the technology that is used to deliver and support these services such as the service desk. The objectives of the service operation functions are to provide responsive stable services, robust end to end operational practices and achieve service excellence. Description of the service operation functions is documented in the following Annexes:

- Annex OP 2 Operation and Organizational Structure, section 7 Structure - NCPeH CY Organogram and Roles
- Annex OP 9 Service Desk Monitoring Tool
- Annex OP 3 Zabbix Open-source monitoring Tool
- Annex OP 11 Quality Management Plan

Further specific information with annex referencing is provided in the following sub-sections.

The NCPeH CY service operations organogram and functions for NEHA, MOH and UCY are given in the following 4 figures.

It is noted that Technical Management, Applications Management and Operations Management are supported by the same group of people given the size of operations of NCPeH CY.

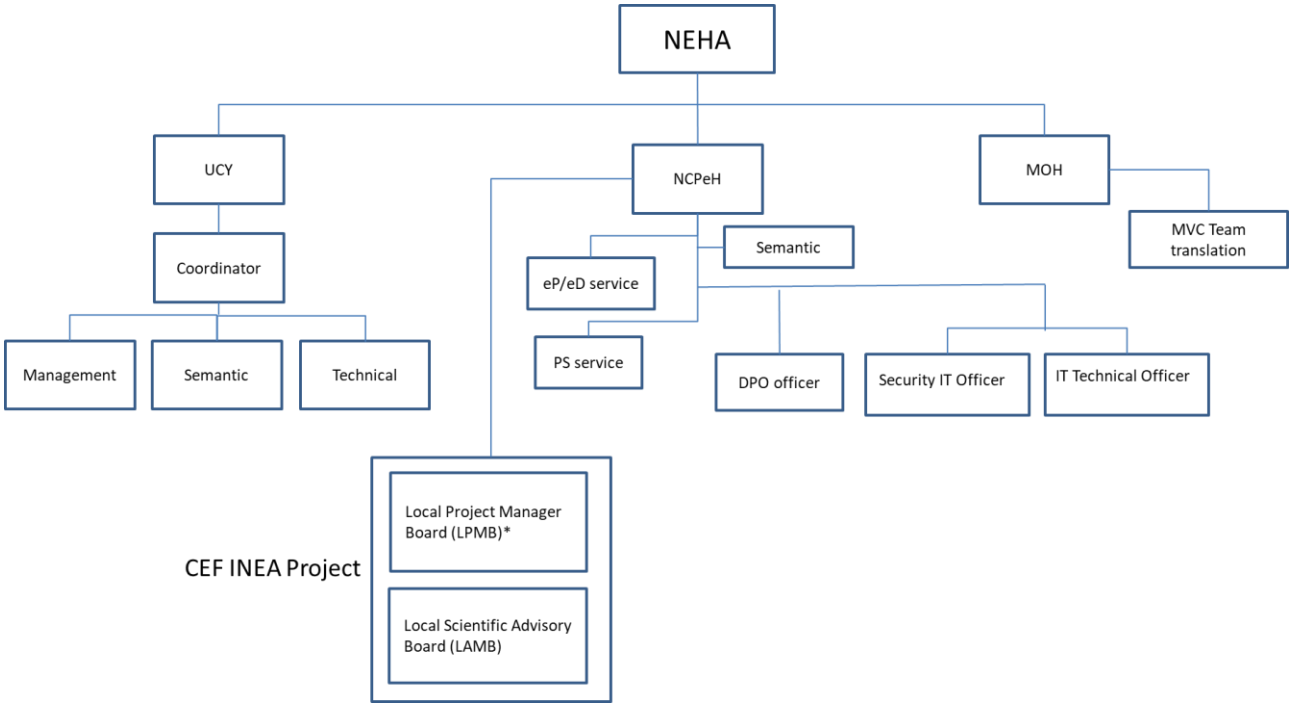


Figure 1a: The Service operation structure of the NEHA, UCY and MOH.

[8] Introduction to Service Operation [UCISA] (page 16) - URL

[9] Source: Introduction to Service Operation [UCISA]

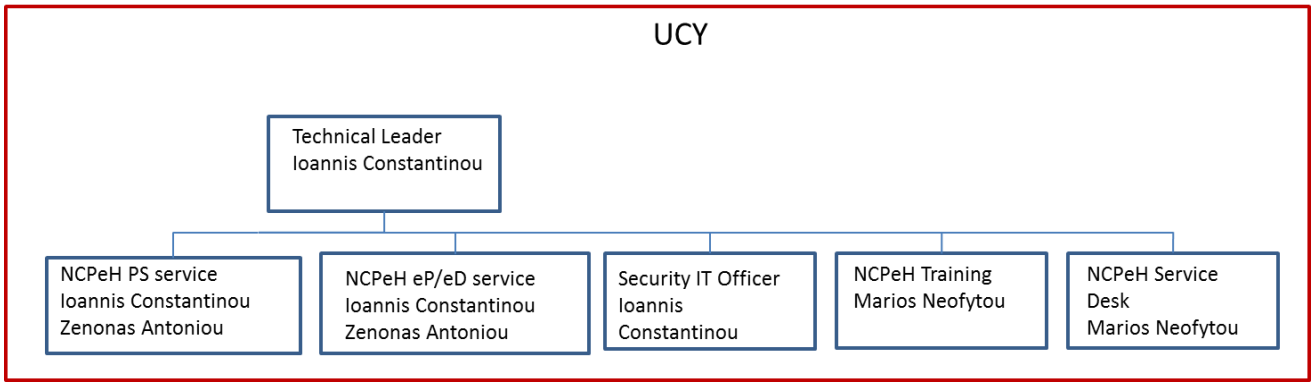


Figure 1b: The Service operation structure of the UCY.

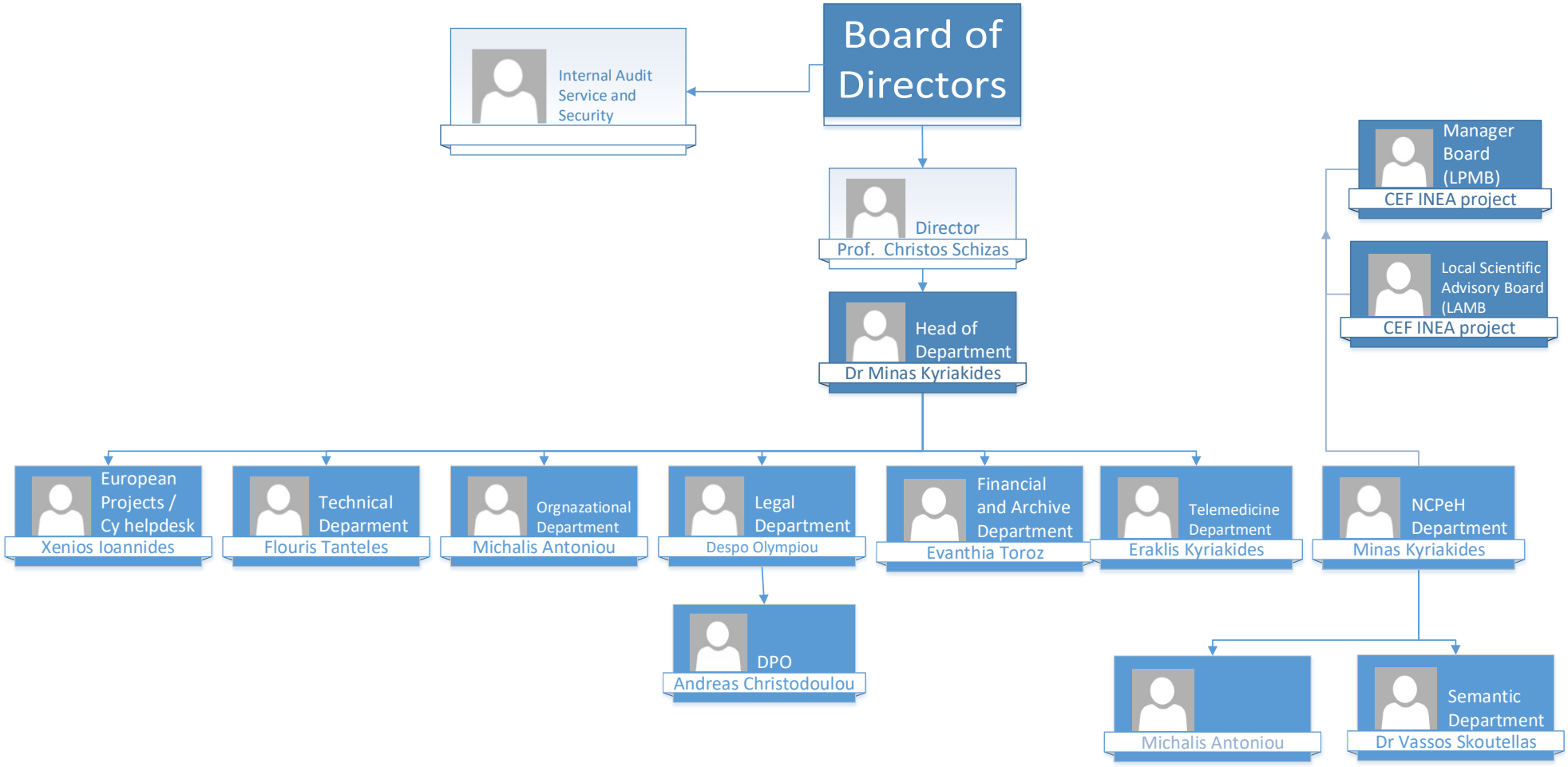


Figure 1c: The Service operation structure for the NCPeH CY of the NEHA.

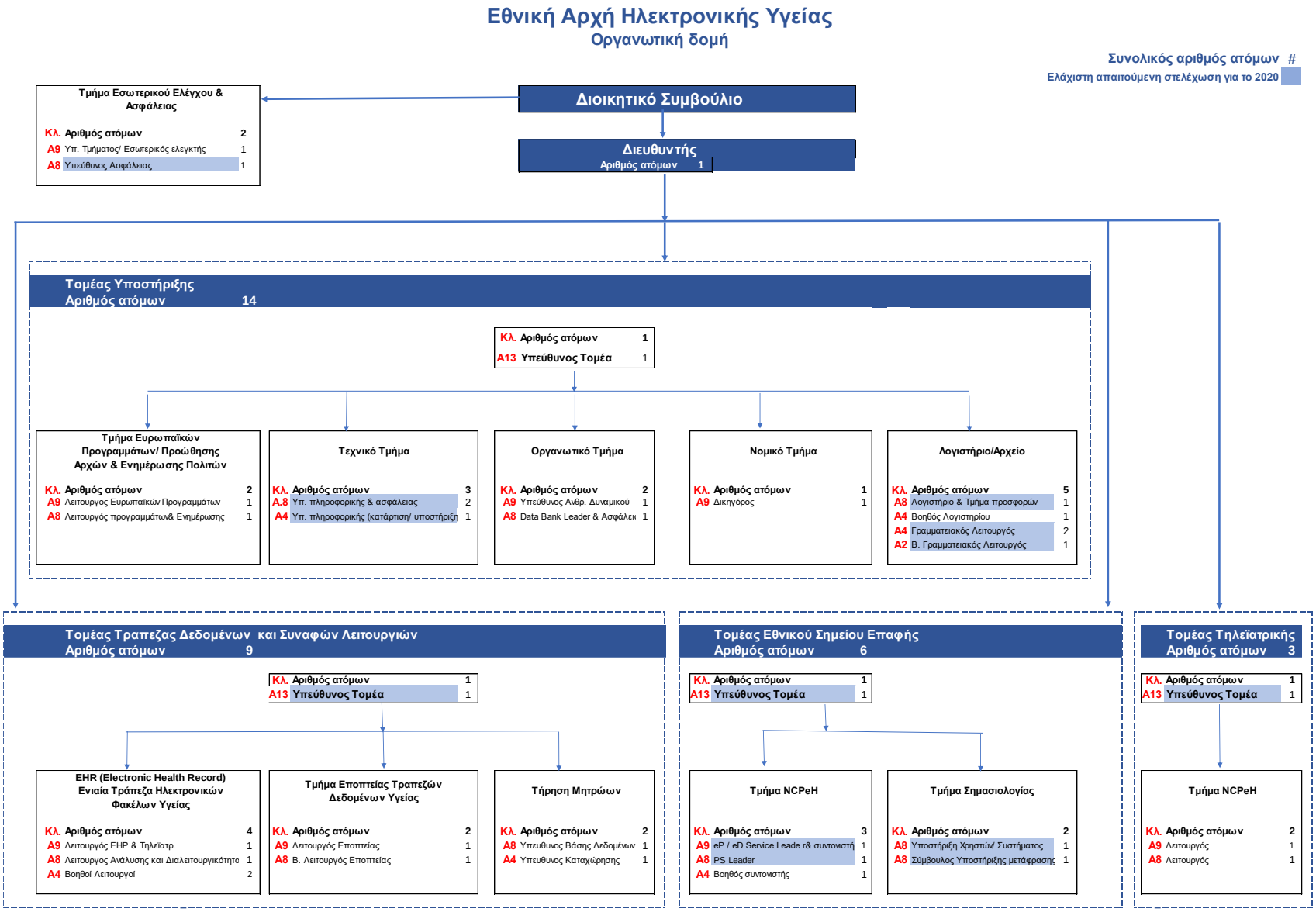


Figure 1D: The Service operation structure of the NEHA.

6 Service Desk[10]

The Service Desk is a key business function for NCPeH CY services.

A dedicated Service Desk for **changes, problem and incident management** supporting the NCPeH CY is used. The Service Desk concentrates on restoring unexpectedly degraded or disrupted services to users as quickly as possible, in order to minimize business impact. In addition, the personnel of the Service Desk perform root cause analysis to determine and resolve the underlying causes of incidents, and proactive activities to detect and prevent future problems/incidents. This also includes the creation of known error records, that document root causes and workarounds to allow quicker diagnosis and resolution.

The Service Desk is based on the OpenSupports (https://www.opensupports.com/) ticketing system. OpenSupports is an open source ticketing system giving support to clients of a company or to users of a platform. It provides better management of users inquiries. Users can send tickets through OpenSupports and the supporting personnel can handle them appropriately. The software has tools to manage the tickets, staff members, the departments where staff members belong to, custom responses, multi-language support. It also lets administrator staff to write articles for known errors, root causes and workarounds to allow quicker diagnosis and resolution.

Service Desk	Description	Index Reference
Objectives	• Provide a single point of contact between the service provider and the users • Manage changes, incidents and service requests • Handle communication with the users	• Annex OP 2 Operation and Organizational Structure, section 7 Structure - NCPeH CY Organogram and Roles • Annex OP 9 Service Desk Monitoring Tool • Annex OP 11 Quality Management Plan • Annex IS 1 Information Security Policy and Procedures

[10] Introduction to Service Desk [UCISA] - URL

Structure	• Centralised service desk • Virtual service desk • URL	• Service desk can be accessed under the NCPeH portal by the users at support.ncp.moh.gov.cy
Time coverage	• The time coverage foreseen for the service desk of the NCPeH CY is: 24x7	• Annex OP 3 Zabbix Open-source monitoring Tool
Single point of contact	• Describe whom users should contact when needing assistance	• Annex OP 2 Operation and Organizational Structure, section 7 Structure - NCPeH CY Organogram and Roles • Structure and domain expertise names given in the aforementioned 2 figures in section 3
Skill Levels	• Skills needed to provide assistance to the users	• Annex OP 2 Operation and Organizational Structure, section 7 Structure - NCPeH CY Organogram and Roles Annex VI: Roles and Service Plans • People assigned are domain experts
Metrics	Service desk metrics: • Number of tickets created over a defined period (last week, last month) • Number of tickets closed over a defined period (last week, last month) • Number of user registrations done over a defined period (last week, last month) • Number of tickets that have been answered (replies) over a defined period (last week, last month) • Trend analysis (statistics figure) of the above metrics • Activity notifications (who opened/reopened/commented on/closed/assigned/changed priority of) each ticket	• Annex OP 9 Service Desk Monitoring Tool, sections 4.1.2 Metrics and Trends and 4.1.3 Last Activity

6.1 Technical management

The technical management function provides detailed technical skills and resources needed to support the ongoing operation of the NCPeH CY IT infrastructure. Technical management also plays an important role in providing the actual resources to support the IT service management lifecycle, and ensures resources are effectively trained and deployed to design, build, transition, operate and improve the technology to deliver and support IT services.

It is noted that Technical Management, Applications Management and Operations Management are supported by the same group of people given the size of operations of NCPeH CY.

Technical management	**Description**	**Index Reference**
Objectives	• Ensuring that the required technical knowledge to design, test, operate and continually improve the IT services is available • Ensuring that staff is adequately trained and effective • Providing technical expertise and support for the management of the IT infrastructure	• Annex OP 2 Operation and Organizational Structure, section 7 Structure - NCPeH CY Organogram and Roles and Annex VI: Roles and Service Plans • Annex OP 3 Zabbix Open-source monitoring Tool • Annex OP 9 Service Desk Monitoring Tool • Annex OP 11 Quality Management Plan • Annex TE 1 NCP CY Technical deliverable
Activities	• Server management • Internet/web management • Network management • Database administration	

6.2 Applications management

Applications management is responsible for managing applications throughout their lifecycle. By supporting and maintaining operational applications, applications management plays an important role in the design, testing and improvement of applications that form part of the NCPeH CY services.

It is noted that Technical Management, Applications Management and Operations Management are supported by the same group of people given the size of operations of NCPeH CY.

Applications management	**Description**	**Index Reference**
Objectives	• Ensuring that resources are effectively trained and deployed to design, build, and transition, operate and improve the technology required to deliver and support IT services • Ensuring that the organisation meets business objectives • Responsible for applications throughout their lifecycle • Ensuring appropriate roles – Applications Managers/Team Leaders, Applications Analysts/Architects • Ensuring availability of functionality • Maintaining operational applications • Providing support during application failures	• Annex OP 2 Operation and Organizational Structure, section 7 Structure - NCPeH CY Organogram and Roles and Annex VI: Roles and Service Plans • Annex OP 3 Zabbix Open-source monitoring Tool • Annex OP 9 Service Desk Monitoring Tool • Annex OP 11 Quality Management Plan • Annex TE 1 NCP CY Technical deliverable • Annex OP 4 NCPeH Dissemination, education and training plan
Activities	• Identifying the knowledge and expertise required to manage and operate applications in the delivery of IT services • Designing and delivering end user training • Ensuring all system documentation is up to date and complete and that relevant staff are familiar with the contents.	

6.3 IT operations management

IT operations include all the processes and services administered by an organization's information technology department. IT operations include administrative processes and support for hardware and software. Effective IT operations management ensures the availability, efficiency and performance of the organization's processes and services. IT operations management defines methods by which IT approaches services, deployment and support to ensure consistency, reliability and quality of service. IT operations cover the daily operational activities needed to manage the IT infrastructure. This is done according to the performance standards defined during service design.

It is noted that Technical Management, Applications Management and Operations Management are supported by the same group of people given the size of operations of NCPeH CY.

IT operations management	Description	Index Reference
Objectives	• Responsible for the day to day running of the IT infrastructure • Maintaining the status quo to achieve infrastructure stability • Initial diagnosis and resolution of operational incidents	• Annex OP 2 Operation and Organizational Structure, section 7 Structure - NCPeH CY Organogram and Roles • Annex TE 1 NCP CY Technical deliverable
Activities	• Ensuring that routine operational tasks are carried out • Providing centralised monitoring and control activities • Management of the physical IT environment (data centres)	

7 Knowledge management[11]

The main objective of the knowledge management is to deliver a quality service based on the ability of the NCPeH CY to respond to specific circumstances. The rationale is to have a clear understanding of the roles and responsibilities of all stakeholders involved, to clarify acceptable risk levels and performance expectations and define the available resources and timescales. The NCPeH CY knowledge management scope is to improve the quality of management and decision-making by ensuring that reliable and secure information and data are available throughout the service lifecycle.

Knowledge management	**Description**	**Index Reference**
Objectives	• Improve the quality of the service, reduce costs, increase satisfaction • Ensuring staff have a clear and shared understanding of the value that their services they are providing to their customers (i.e. the doctors and pharmacists)	• Annex OP 2 Operation and Organizational Structure, section 7 Structure - NCPeH CY Organogram and Roles • Annex OP 7 Business Continuity Procedures NCPeH CY
Processes and Practices	• Knowledge identification capture and maintenance • Knowledge transfer • Data and information management • Establishing data and information requirements • Establishing data and information management procedures • Evaluation and improvement	

[11] Introducing service transition [UCISA] (page 2) - URL