ITP125

IT OPERATIONS POLICY
POLICY AND PROCESSES

Table of Contents

1. POLICY INTRODUCTION

This policy establishes an effective, accountable, and transparent framework for the main operations activities of the National Ambulance IT department (IT) in the support of National Ambulance activities.

This policy is relevant to the [Leadership and Commitment, Organizational Roles and Responsibilities, Risk Evaluation and Management, Policies and Objectives, Implementation Monitoring and Reporting, Managing of Non conformances and Action Items, Auditing and Inspections, Continuous Improvement Management System Components.

2. SCOPE

This policy defines a framework for the activities undertaken by IT in there BAU role for IT services as defined in the IT Service Catalogue covering:

- Service Governance / segregation of IT duties compliance
- System Acceptance / Baseline configurations
- Service Desk
- Incident and Request Management
- Major Incident Management and DR
- User Account / Access Provisioning
- Configuration and Change Management
- Data Security, Backup, malware, and patch management
- Problem management in conjunction with QHSE
- Capacity and Availability planning
- Standard operating procedures
- Logging and monitoring

Out of Scope:-

Development, Projects and other non BAU Activities.

3. ROLES AND RESPONSIBILITIES

Define who is responsible for implementation of the policy and procedures.

Role	Responsibilities
Executive	Approving and actively supporting the policy
Chief Financial Officer	Chief Information Security Officer (CISO) Charged with overseeing and compliance reporting for all information related processes and activities.
Managers	Ensuring their teams conform with the policy requirements and make themselves aware of the policy requirements.
Staff	Adhering to the requirements of this policy and any associated policies, guidelines, and procedures
CISO	Ensuring that Security elements of the policy are complied with
IT Manager	Ensuring the IT team follow and comply with the requirements of this policy. That any issues or exceptions are escalated and managed accordingly
IT Team members	Ensuring they follow and comply with the requirements of this policy. That any issues or exceptions are escalated to the IT Manager promptly.
QHSE	Assist IT in managing Problems and identifying issues and root cause analysis

4. POLICY STATEMENT

This policy governs the operational support framework for National Ambulance IT in the following areas.

4.1. SERVICE GOVERNANCE

IT Services will be maintained as per the requirements set out in COP425 National Ambulance Business Service Catalogue with changes to the service being approved by the service owners or representatives as needed. Any change with significant downtime or change to service value must be authorized by Executive prior to implementation.

4.1.1. SEGREGATION OF DUTIES

Users with Administrative duties to systems will be provided with a mechanism to split their admin rights from their normal access to the system if they are also required to use the system in their normal work to ensure that normal security principles apply to their BAU access.

This may be achieved in a number of ways, either by having two accounts for the system in question, one with normal BAU user access, the other with elevated rights to perform administrative tasks, or by the use of profile interfaces where by the elevated rights can be enabled and disabled as required by the user.

Changes to Administrative access to any system must be accompanied by a change request approved by the appropriate service owner or CAO if access is provided to multiple systems.

4.2. IT SERVICE CATALOGUE

The IT Service Catalogue will be maintained as part of the National Ambulance Business Service Catalogue

4.3. SYSTEM DEVELOPMENT AND DESIGN

Systems will be developed and designed with information security and privacy in mind and ensure that rights and access to protected information is maintained to appropriate standards and restricted according to need and role.

Systems that have access to Confidential or Private information should only be accessible over secure links by an authenticated user or integration.

Integrations between systems should only share the necessary information to achieve the required task and not allow access to additional information unless required by the use case.

Testing must form an integral part of any release cycle of any applications that involve the management, collection, or transmission of confidential or private information.

Security issues that impact confidential or private information must be given a high priority in any remediation backlog.

Security updates and threats may trigger new releases as apparent in the application or platforms used in the application.

4.3.1. Software Development Life Cycle (SDLC)

Software development will be managed by the ePMO project management processes and follow an agile methodology by using the following main lifecycle steps:-

- Requirements Capture including:-
  - Bug fixes / Security updates for the existing system
  - User Requirements, use cases and user interface requirements (UX)
  - Service Requirements, SLAs, Availability and Capacity ect.
  - System Requirements
  - Data and Security and privacy Requirements
- Systems Design including analysis and prioritization of requirements with key stakeholders
- Development in a separate development environment
- Testing in a separate or non production environment
- Deployment or promotion to production
- Review and capture of production issues feeding into the requirements for the next cycle.

4.4. System Acceptance / Baseline configurations

The following criteria must be met to be accepted into service.

4.4.1. System Acceptance

System acceptance will be based on the following criteria and subject to testing prior to acceptance sign off by the service owner and / or IT Manager:-

- Systems ownership must be identified, and service owner agreed.
- Systems must be currently supported by OEM and vendor contracts.
- Hardware and Software support lifecycle must be more than 3yrs to end of support at the time of acceptance.
- Licenses, Warrantees, certificates of authenticity must be made available to the support teams before acceptance.
- Systems will be compatible with National Ambulance backup DR and access control and security systems.
- Support staff will be trained in the support of the systems before transfer to production.

4.4.2. Baseline configurations

Systems will be configured to the following minimum standards: -

- Currently supported configuration and version of O/S Application or firmware
- Meet current Manufacturer recommended / required specifications.
- Using supported Chipsets and Drivers.
- Patched to the currently supported security levels.
- Critical Vulnerabilities patched or mitigated e.g. Firewalls enabled.
- Malware agents or scanners installed if available.
- AutoRun features disabled for removable media.
- Strong admin passwords
- Default passwords disabled.
- Guest access disabled
- Unauthenticated access disabled unless required as part of the service to be provided.
  E.g. Public website with no authentication requirement
- Clock / Timestamps synchronized with National Ambulance NTP services or UAE Internet Provider NTP services if in the public network.
- Plain text password storage / authentication / acceptance disabled.
- Where there is no impact to operational response, systems will be set to lock or logout the user after periods of inactivity.
  E.g. MDTs, 998 response systems will not timeout due to patient safety concerns but will be managed accordingly.

- Additional, Unused services and ports disabled or configured to reject connection.
- Admin account passwords recorded in the IT Admin password vault.
- Testing / Training accounts disables once the testing and training has completed.
- Security Controls as required for the level of information managed by the system.

Systems not meeting the above minimum configurations should be patched, upgraded, migrated, or decommissioned as required to ensure secure, reliable service provision.

4.5. Service Desk

IT will provide and maintain a support service desk for all internally supported IT services which is accessible 24/7 by phone and email with appropriate support resources available to ensure systems and services are supported during their service hours. Service support hours will be defined for Incident, Major Incident, and Request management in the National Ambulance Business Service Catalogue.

4.6. Incident and Request Management

All Incidents and requests will be logged and managed using the service desk application following the process outlined in section 6.1 Incident and Request Management Process. Incidents will be prioritized according to business impact and urgency as follows.

4.6.1. Incident Priority and Response times

Impact and Urgency Criteria	Incident Priority	Response Time	Target Fix Time
Any of the following: - • Major outage impacting significant numbers of users. • Security or Privacy incident putting company / patient data or operations at significant risk • Significant loss of data or functionality of critical or core systems	Major Incident	<=15 Mins Onsite within 1hr	As per response plan / situation dictates
Any of the following: - • 30 or greater users impacted • Whole team or department impacted • Multiple users not able to complete a critical activity • VIP / Exec not able to complete a critical activity	Priority 1	<=30 Mins Onsite within 1hr if required	<= 4hrs
Any of the following: - • 6 - 30 users impacted • Single user not able to complete a critical activity • VIP / Exec impacted but able to work or a non-critical activity impacted	Priority 2	<=1 hr	<=8hrs
2 - 5 impacted but able to work or a non-critical activity impacted	Priority 3	<=8hrs (support hrs)	<=24hrs (support hrs)
Single user impacted but able to work or a non-critical activity impacted	Priority 4	<=16hrs (support hrs)	<=48hrs (support hrs)

4.7. Major Incident Management and DR

Should a major incident be identified then the Major incident process will be followed as detailed in section 6.2 Major Incident / Outage / Security Incident Process.

Any of the following should be considered a major incident: -

- Major outage impacting significant numbers of users.
- Security or Privacy incident putting company / patient data or operations at significant risk
- Significant loss of data or functionality of critical or core systems

The Owner of the incident will ensure the process is followed to:-

- Identify the outage / issue.
- Plan and contain the impact.
- Rectify and restore the service.
- Ensure Root Cause analysis is complete.
- Record and action any lessons learned.

While ensuring clear, timely, coordinated communication is taking place to ensure all impacted stakeholders are informed of the status and planned activities to contain and resolve the issue.

The Executives or in extreme circumstances the Major Incident Owner may invoke the Business Continuity or DR plan if required as a resolution or parallel activity as required to minimize business and service impact during the incident.

A Major incident that involves the release of confidential information or involves patient private information should be reported to authorities within 24hrs of the incident.

Root cause analysis must be completed in accordance with QHSE guidelines and using the appropriate methodology along with the recording and action of any lessons learned from the Major Incident.

4.8. User Account / Access Provisioning

User access and rights provision will be granted on an as needs basis with suitable authorization from either the service or content owner or delegated to line manager approval as described in the service catalogue entry for that service and the process detailed in section 6.3 User Account / Access Provisioning.

Several National Ambulance services are mandatory for legal and regulatory purposes and users cannot request to be removed from these systems unless approved by the Executive.

Users may have their access temporarily suspended if requested by an Executive or due to an ongoing security, HR, legal or other investigation / issue that is deemed to impact the safety and security of the service to be accessed or data within.

Where feasible, user's access to systems will be provided through Active Directory /LDAP services and limited to areas where the user requires access for the purposes of their duties.

User accounts will be removed once informed by HR that the user has completed their assignment and the accounts are no longer required.

Passwords for new accounts or password updates must be sent by SMS to the users registered mobile or by other separate route to ensure delivery to the user only.

4.9. Configuration and Change Management

National Ambulance IT will maintain asset information for all IT assets and manage changes to critical infrastructure, applications, and services.

4.9.1. Configuration Management

Configuration information for all critical infrastructure and Applications will be maintained in a central data store to provide information for the use in recovery and change management.

4.9.2. Change Management

Changes to any critical infrastructure, system or application will be managed using the change management process outlined in section 6.4 Change Management Process

4.9.3. Change procedures

The change process is broken down into the following phases: -

- Raise and Assess.
- Conflict assessment and resolution
- Impact assessment and Classification
- Initial Approval
- CAB Approval for Non-Minor Changes
- Implementation
- Review and Verification
- Closure

4.9.4. 4.9.4. Change Risk impact assessment.

Changes must be assessed for impact and risk to service and data security and privacy. Any risk to data security or privacy must be assessed and plan detailed as to how the risk will be managed before, during and after the change.

The change impact score must be calculated using the following matrix criteria and scoring, the total change score being the result of multiplying all the factors together to reach the final score:-

Impact Assessment (Multiply to get change score)				
Data Classification	**Public** (1)	**Restricted** (2)	**Confidential** (3)	**Secret** (6)
(Highest data classification impacted)	e.g. Website or other public information	e.g. Dispatch data, company policies and processes, general rosters ect.	e.g. Patient, HR, Financial data	We do not have any Secret Data
Predicted Outage	**Low** (1)	**Medium** (2)	**High** (3)	**Extreme** (6)
(During the Change)	No interruption of service	Interruption of service outside of core service hours	Small Interruption of service inside core hours	Major Interruption of service inside core hours
No of Users	**Small** (1)	**Medium** (2)	**Large** (3)	**Huge** (6)
(Affected)	0 to 50 Users	51 to 99 Users	100 to 299 Users	300 + Users
Possible Risk	**Low** (1)	**Medium** (2)	**High** (3)	**Extreme** (6)
(To the business)	Noncritical system with workaround	Noncritical system with no workaround or Critical system with workaround	Critical system with no workaround	Core system used by other critical systems
Change Score	**Minor** (1-2)	**Significant** (3-12)	**Major** (13-27)	**Huge** (28+)
Authorization Required	**Business Owner or IT Manager**	**Business Owner + IT Manager**	**Business Owner + IT Manager + CAO**	**Business Owner + IT Manager + CAO + Exec + CEO**

4.9.5. CHANGE CLASSIFICATION

Many services have standard changes which do not require impact assessment or have by process and approval loops reduced the impact to acceptable levels. Standard changes are regulated by the incident request process and standard requests and changes and include for example. User password changes, Group permissions changes, new user hardware ect.

Changes are categorized by the predicted business impact of the change and risk associated with the change.

Changes which have a significant or higher risk should be discussed at the Change Advisory Board (CAB) to allow stakeholders to review the change and raise any concerns or possible conflicts before the change is scheduled for implementation.

The CAB will be held weekly and will be attended by the IT Manager, Change Requestors and Service Managers to assess new changes for approval and review implemented changes from the previous week. Optionally the CAO may attend CAB if there are several Major or significant changes presented that require additional input or assessment prior to approval.

Change Types: -

- Standard Change – Managed by the normal service request process
- Minor Changes which have a low impact, no operational impact will be considered minor and may be approved by the IT manager or service business owner.
- Significant changes with no service outage or related service impact may be approved by the appropriate service owner and IT manager
- Major changes require approval from the CAO and impacted managers before implementation.
- Huge changes or changes which impact more than one critical system require approval from the CAO, Exec and/or CEO and impacted managers before implementation.

Emergency changes should follow the same process as normal changes however due to time frame issues may be verbally approved over the phone or escalated to the appropriate Executive staffing the justification for the urgency prior to implementation.

4.9.6. CHANGE RISK ASSESSMENT MATRIX

Criteria	Change Type	Approval
No Risk, templated change e.g. user equipment replacement.	Standard Change	By business service request process and approval.
Low risk, Low impact change e.g. add a server to the network	Minor Change	IT Manager with impacted Business Owner approval as appropriate
Higher risk, Higher impact change to a single non-critical service without impact to other services Addition or changes to Admin access to a single service e.g. Website Update	Significant Change	Business Owner + IT Manager approval with impacted Manager approval as appropriate
High risk or High impact change with Service downtime Critical or multiple services Addition or changes to Admin access to Multiple services e.g. Network Upgrade with downtime	Major Change	CAO +Business Owner + IT Manager approval with impacted Manager approval as appropriate
Change that can potentially impact all areas of the business or all users to a significant level. Change to a core system that impacts multiple critical services. e.g. Core switch upgrade	Huge Change	EXEC/CEO + CAO +Business Owner + IT Manager approval with impacted Manager approval as appropriate
Any change that cannot be assessed within the normal change time frame	Emergency Change	Approval by Phone / eCAB as the above approval matrix

4.9.7. CHANGE MANAGEMENT RACI CHART

Change Management RACI	Role						
Service RACI **R**- Responsible for action (Do-er) **A**- Ultimatly accountable for (Oversee-er) **C**- Consulted (Two way communication) **I**- Informed (One way communication)	**Change Process Owner (CISO???)**	**Change Manager (IT Manager)**	**CAB / CAO**	**Change Requestor**	**Service Owner**	**Implementer / Tester**	**3rd Party Supplier**
Change Management Process	**A**	R	C	I	I	I	I
Raise / Record	I	C/I	I	**A/R**	I		
Assess / Approve	C	**A/R**	R	R	R		
Authorise	A	R	R	C	I		
Schedule	C	**A/R**	R	R/C	I	I	C
Implement	I	C	C	I	I	**A**	R
Monitor	I	**A**	R	I	I	R	R
Close	I	**A**	R	I	I	I	I
Reporting	**A**	R	I	I	I	I	I

4.10. DATA SECURITY, BACKUP, MALWARE, AND PATCH MANAGEMENT

As part of normal operations, IT will complete a Monthly Data Security, Backup, Malware and Vulnerability assessment which will be used to drive the remediation and update of any areas which are not to the required baseline. The assessment report will be made available to CISO for comment and any additional actions.

4.10.1. DATA SECURITY

Systems will be maintained according to the policies and restrictions noted in COP401, COP402 and COP403. With the approvals noted in the Service Governance and Service Catalogue XXX

4.10.2. BACKUP

All systems will be backed up according to the requirements of the Service Catalogue, and IT Backup policy ITP106 with date retained according to COP402 Data retention policy.

4.10.3. MALWARE AND PATCH MANAGEMENT

All systems must meet the system baselines as documented in section 4.4.2 Baseline configurations and be reviewed and assessed on a monthly basis.

Any systems which cannot be brought back to baseline within 1month of the reported issues will be reported to CISO as an exception with a plan to bring back the baseline requirement or replacement of the system.

4.11. PROBLEM MANAGEMENT

The IT Department will report any problems using the QHSE risk and problem management process

4.12. CAPACITY AND AVAILABILITY PLANNING

Capacity and Availability planning and monitoring will be undertaken by the IT team to ensure systems are meeting the requirements of the business and resources are being used efficiently.

4.12.1. CAPACITY PLANNING

As part of normal operations, IT will review the capacity of all systems quarterly or by Executive request in case of organizational changes.
IT will also ensure future changes are considered when planning budgets for the next financial year

Critical systems, links and applications will be monitored in terms of:-

- Resource Capacity (RAM, CPU, Disk, ect)
- Bandwidth Use
- License Use

To ensure that resources are optimized, and shortfalls are dealt with before an operational impact occurs. Business changes will be assessed and their impact on the above as part of the normal change management process.

4.12.2. AVAILABILITY PLANNING

Availability requirements are defined in National Ambulance Business Service Catalogue. Solution designs and monitoring alarms will be tailored to meet and monitor these requirements as needed.

Monthly system availability reports will be completed including the overall availability for the service for the period, any downtime or major issues and outages.

Systems which no longer perform according to the availability requirements will be assessed and a remediation plan created and escalated to the involved stakeholder for comment and approval prior to implementation.

4.13. STANDARD OPERATING PROCEDURES

Where practical, IT will develop standard operating procedures (SOPs). SOPs are stored in the IT shared drive and are accessible to all IT support staff. Updates to SOPs is usually considered a standard change unless it involves any of the following: -

- Changes to Admin Rights and Permissions
- Introduction of a new process, or policy
- Changes which may impact Operations or services.

In which case the change will be assessed as any other change request using the change process.

4.14. 4.14. LOGGING AND MONITORING

All critical applications or systems will be monitored in terms of:-
System / Health Alarms
Capacity Alarms
Availability Alarms

Alarms that have been generated will be assessed and if intervention is required created as an incident for remediation.
Where feasible, critical system logs will be monitored for anomalous behaviors and reported on accordingly.

5. RELEVANT LEGISLATION

International, federal or local legislation and circulars relevant to this Policy. Full detail on this legislation can be found in QHP109 Legal Register.

Code, Name of Legislation	Jurisdiction
Code, Name of Legislation, Year here	Jurisdiction here

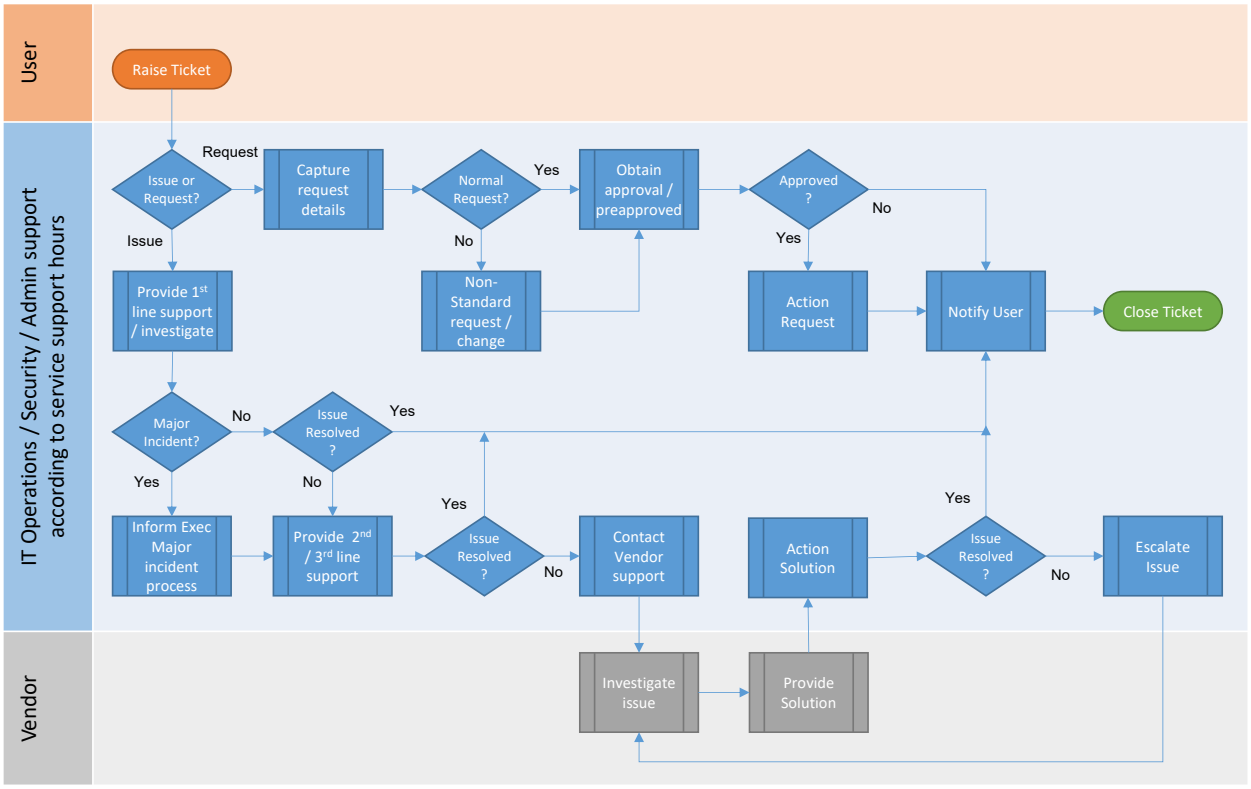
6. KEY PROCESSES

As a part of maintaining a quality system, for each process we provide a process map, identify the owner of the process (position), the owner of each step, potential failure points and process, the monitoring and measuring of the process and any interactions of this process with other key processes.

A summary of all key processes is provided within the QHSE Management System via QHF805 Key Process Register.

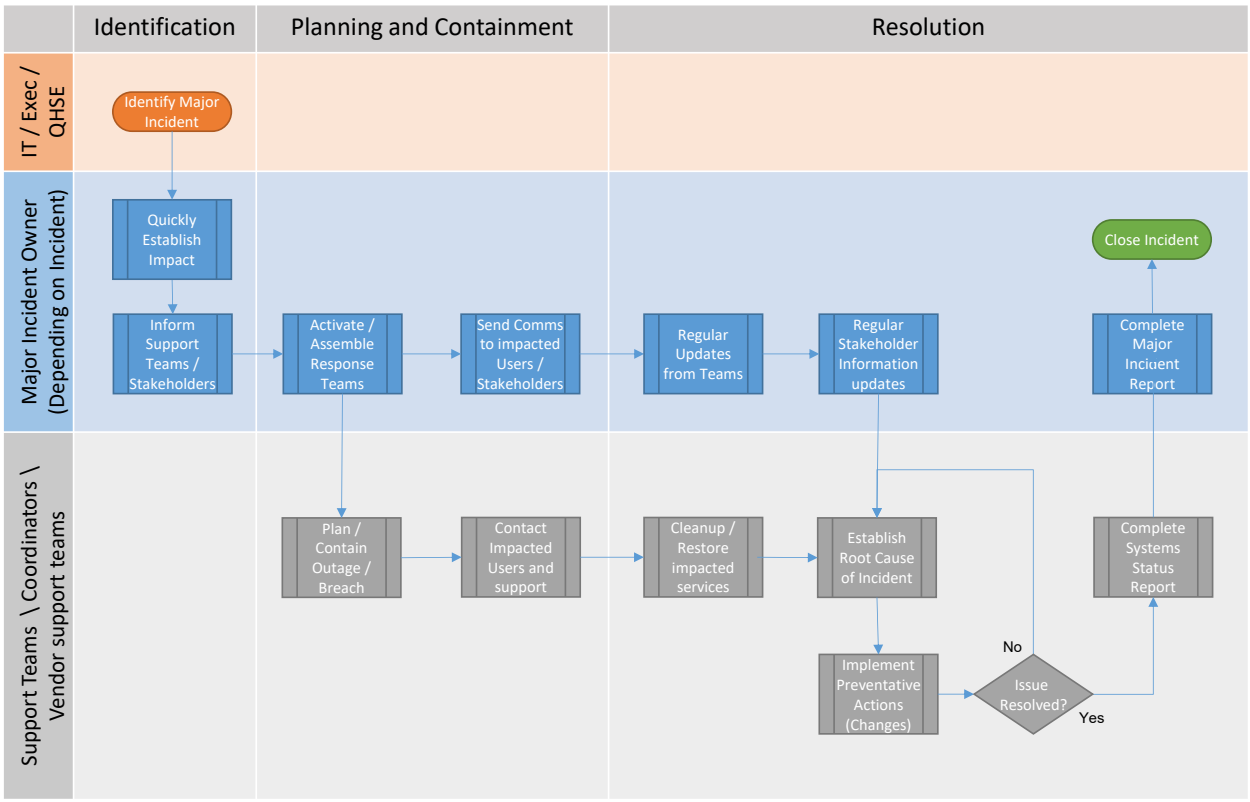
6.1. Incident and Request Management Process

Process Name	Incident and Request Management Process
Process Ownership	IT Manager
Process Measurement	Response Time Objective Resolution Time Objective
Interaction with Other Processes	QHSE Issue/Problem Process Major Incident / Outage / Security Incident Process User Account / Access Provisioning Process IT Change Process
Forms Used	TBC



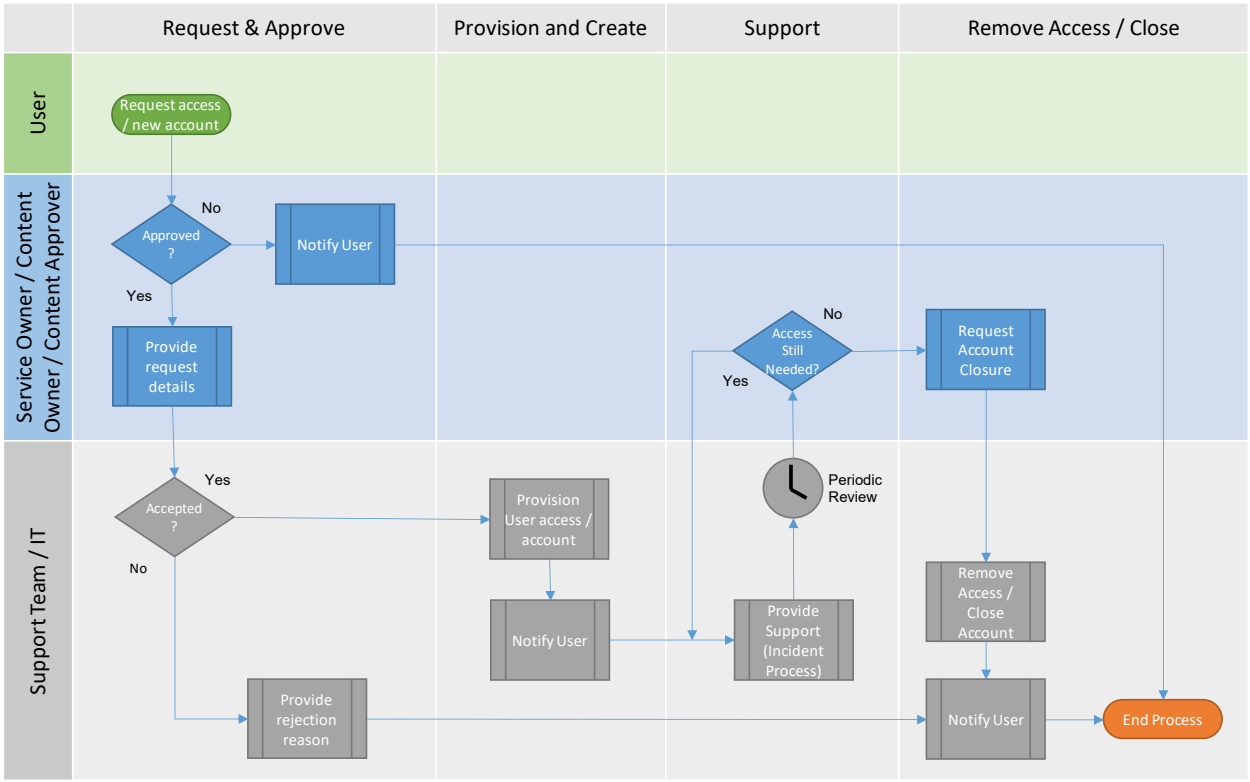
6.2. Major Incident / Outage / Security Incident Process

Process Name	Major Incident / Outage / Security Incident
Process Ownership	CISO
Process Measurement	TBC
Interaction with Other Processes	Incident / Request Management Process
Forms Used	


Identification
Planning and Containment
Resolution
IT / Exec / QHSE
Major Incident Owner (Depending on Incident)
Support Teams \ Coordinators \ Vendor support teams
Identify Major Incident
Quickly Establish Impact
Inform Support Teams / Stakeholders
Activate / Assemble Response Teams
Send Comms to impacted Users / Stakeholders
Regular Updates from Teams
Regular Stakeholder Information updates
Close Incident
Complete Major Incident Report
Plan / Contain Outage / Breach
Contact Impacted Users and support
Cleanup / Restore impacted services
Establish Root Cause of Incident
Complete Systems Status Report
Implement Preventative Actions (Changes)
Issue Resolved?
No
Yes

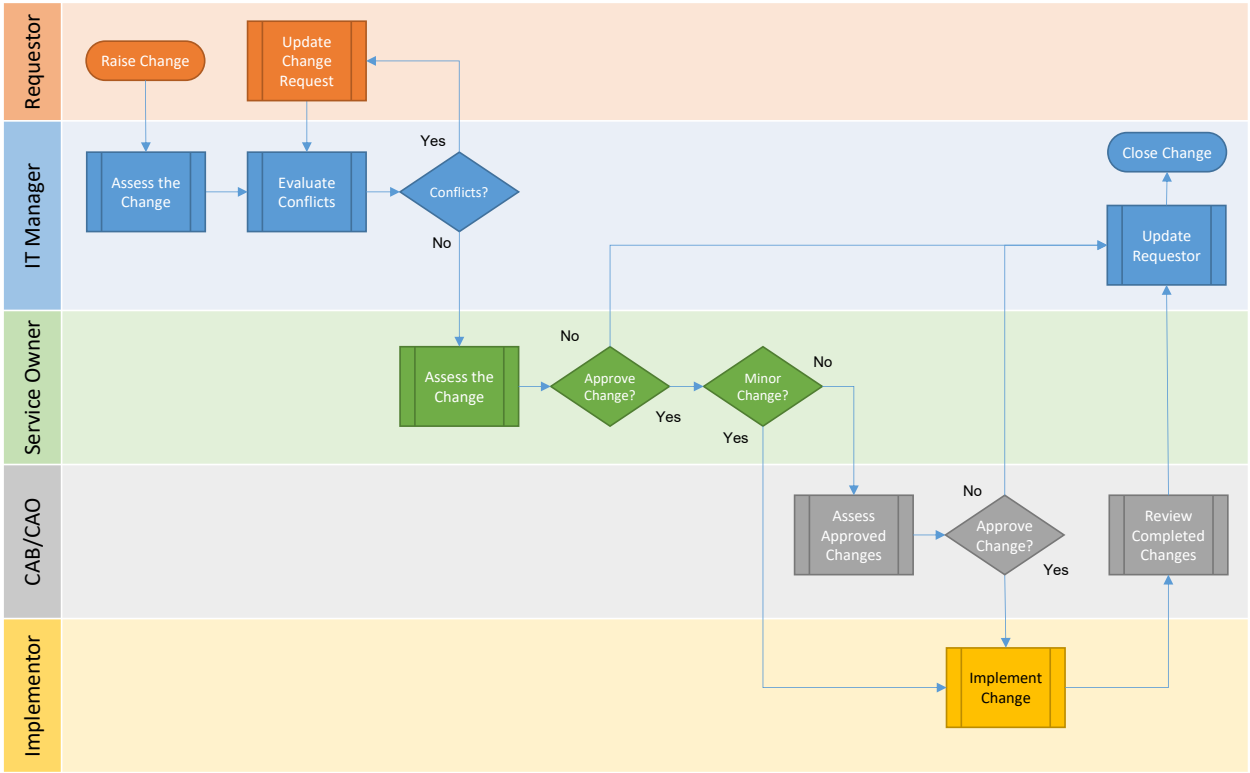
6.3. User Account / Access Provisioning Process

Process Name	User Account / Access Provisioning Process
Process Ownership	CISO
Process Measurement	TBC
Interaction with Other Processes	Incident and Request Management Process Data Security, Backup, malware, and patch management
Forms Used	TBC



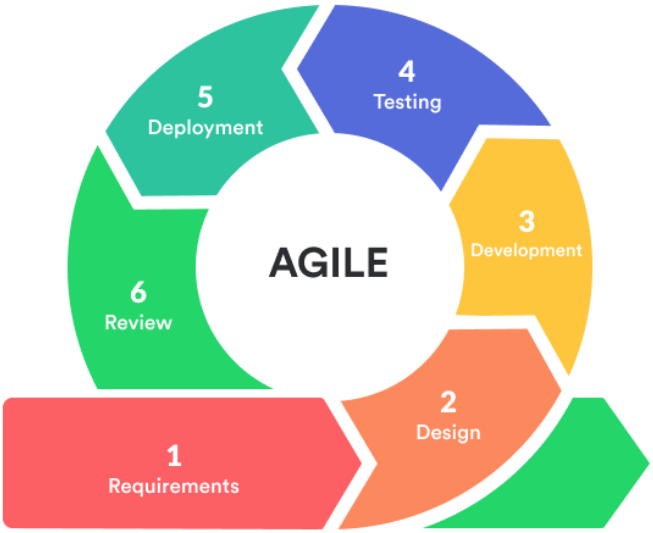
6.4. CHANGE MANAGEMENT PROCESS

Process Name	Change Management Process
Process Ownership	CISO
Process Measurement	TBC
Interaction with Other Processes	Incident / Request Management Process
Forms Used	



6.5. Software Development Lifecycle

Process Name	Software Development Lifecycle
Process Ownership	IT Manager
Process Measurement	TBC
Interaction with Other Processes	Change Management
Forms Used	



7. RELATED POLICIES AND FORMS

List related policies and procedures to the created/updated policy.

Policy & Procedure /Form
IT Operation Procedures and Work Instructions.
COP401 Information Management Policy
COP402 Document Retention Policy and Procedure
COP403 General Confidentiality Policy -
ITP102 Acceptable Use of IT Asset Policy
ITP119 Access Control Policy
New Corporate Communication Policy and Procedure
PUP203 Asset Management Policy

8. FEEDBACK

Any feedback or suggestions for improvement to this Policy, Processes or Procedures can be submitted to qhse@nationalambulance.ae

9. DOCUMENT CONTROL AND OWNERSHIP

A review and update of this document will take place as necessary, when changes occur that identify the need to revise this Policy such as changes in roles and responsibilities, release of new legislative or technical guidance, or identification of a new policy area.

This document ownership for editing is identified as:

- IT Manager

This controlled document is managed / overseen by the Policy Review Committee.

Change Brief

Version No.	Date	Change
0.1	05/09/2020	*Initial Draft*
2.0	June 2021	Added comments and assigned process ownership to CISO Added and updated areas for Patient Privacy and ADHICS compliance Added points 4.3 System Development and Designs 4.3.1. Software Development Life Cycles 4.9.4. Change Risk Impact Assessment 6.5 Software Development Life Cycles Added information to 4.7. Major Incident Management and Dr 4.8. User Account / Access Provisioning 4.9.5. Change Classification Added information to 4.9.6 Change Risk Assessment Matrix: Criteria: Change that can potentially impact all areas of the business or all users to a significant level. Change to a core system that impacts multiple critical services. e.g. Core switch upgrade Change Type: Huge Change Approval: EXEC/CEO + CAO +Business Owner + IT Manager approval with impacted Manager approval as appropriate 4.9.5 Change Classification in the Changes Types

CEO Approval

Board Member Verification