COP424

THIRD PARTY SECURITY POLICY AND PROCEDURES

Table of Contents

1. POLICY INTRODUCTION 3

2. SCOPE 3

3. ROLES AND RESPONSIBILITIES 3

4. POLICY STATEMENT 3

4.1. DUE DELIGENCE AND RISK ASSESSTMENT RELEVANT LEGISLATION 3

4.1.1 Non-disclosure Agreement sign off 3

4.1.2. Third Parties Contract 4

4.1.3. Identification of Risk Related to Third Parties 4

4.14. Exchanges of Inforamtion 5

4.2. MONITORING AND REVIEWING OF THIRD PARTIES SERVICE 5

4.3. TERMINATION OF THIRD PARTIES SERVICES RELATED 5

4.4. REPORTING SECURITY INFORMATION INCIDENTS 5

5. RELEVANT LEGISLATION 5

6. RELATED POLICIES AND FORMS 5

7. FEEDBACK 6

8. DOCUMENT CONTROL OWNERSHIP 6

1. POLICY INTRODUCTION

This policy is designed to assist in managing the risk that may occur as a result of dealing with third party suppliers or outsourcing services.

It aims to ensure appropriate awareness, governance, and escalation is in place to demonstrate effective management of potential risk in departments that may deal with a third party.

The third party services should be controlled through suitable procedural obligations and contractual terms to secure privacy and protect information assets by establishing a suitable structure for third party management. Such as (but not limited to):

- Reduce probabilities of information leakage and loss
- Secure information assets
- Minimize unauthorized access and usage
- Uphold organizational reputation
- Ensure service continuity

2. SCOPE

This policy applies to all suppliers and outsourced employees and any third parties that support Supply Chain, IT department, or any other department in National Ambulance.

3. ROLES AND RESPONSIBILITIES

1. All Department Heads (interact with third party)

Must ensure that third party risk management is effectively performed within their areas of responsibility.

2. All Third Party entities

Are responsible for acting according to this policy and procedures. They are also responsible for ensuring that their staff comply with and act accordingly with this policy.

3. All Third Party staff that interact with National Ambulance or its Data

Are responsible for acting according to this policy and procedures. They are also responsible for ensuring that they attend or pursue any relevant training recommended by their Managers. (I.e. face to face or online training). This includes staff supporting operations functions i.e. dispatchers.

4. POLICY STATEMENT

NA employees who deal with third parties should ensure that risks associated with third party suppliers are managed consistently and effectively.

4.1. DUE DILIGENCE & RISK ASSESSMENT

The Supply Chain and IT Team must ensure there is a due diligence process which includes:

- Activities to identify, assess, monitor, manage and report third party risk exposures.
- The third party risk maintained and key controls are effectively communicated to all relevant employees.
- Due diligence must be completed before a contract or renewal of a contract is signed and the supplier is allowed to start work.
- Assess the strategic alignment and capabilities of the third party supplier and the risks.
- Completed to determine the required nature and frequency of ongoing monitoring and engagement with the supplier, commensurate with the level of risk to National Ambulance.
- Assess the level of access needed to National Ambulance facilities and information assets in accordance with ITP119 Access Control Policy and QHP213 QHSE Work Location Management Policy and Procedure.

4.1.1. NON-DISCLOSURE AGREEMENT SIGN OFF

- Ensure that NDA (Non-Disclosure Agreement) is signed by all Third Parties in which a contract is in place, including whenever there is a need to exchange information classified as per National Ambulance classification level of information, whether for contractual purposes or any other justified business need, and whenever a third party supplier enters National Ambulance facilities, or has access to information assets.
- The NDA shall be signed by the User/ Projects Managers / Contract Managers / Senior Management and Head of Department.
- The NDA shall be signed before commencing the information disclosure to the third party, whether it is for a project scoping phase or for any other justified business need.

4.1.2. THIRD PARTIES CONTRACT

Based on the criticality of the project and the engagement nature, the below clauses can be considered as part of Third Parties contracts:

- Compliance with legal and regulatory requirements.
- Compliance with Intellectual property rights requirements.
- Compliance with information security policies and procedures.
- Compliance with management of change process
- Clear allocation of responsibilities to all the involved parties.
- Statement on Non – Disclosure of information.
- National Ambulance rights to review and audit the compliance with the contracts.
- Adequate Service Level Agreements (SLA), where applicable.
- Types of information that third party service provider needs access to
- Measures and minimum baselines for each of the identified security requirements are established and monitored

Information security policies should be provided to and acknowledged by third party suppliers If they have access to National Ambulance facilities or information assets. The information security policies include:

- COP424 Third Party Policy
- ITP119 Access control Policy

Third party suppliers of manpower undergo the same induction process as National Ambulance staff in line with HRP104 On- Boarding and Induction Policy and Procedure.
In addition, contracts with Third Parties suppliers that include exchange of information and software should specify:

- Definitions of information to be protected
- Duration of agreement
- Process for notification of leakage
- Ownership

4.1.3 IDENTIFICATION OF RISK RELATED TO THIRD PARTIES

1. Contract Owner / Department Head / Contract Manager / Project Manager shall ensure that the periodic information security risk assessment identifies potential Third Parties risks that could compromise the Confidentiality, Integrity & Availability of Information & information processing facilities.
2. Project Manager in coordination with Information Security Specialist shall identify any additional information security risk specific to the project.
3. The analysis of risks related to Third Parties access to information shall consider the following:
    - Possible impacts to the controls of the information.
    - The classification of the information assets.
    - Processes for identifying, authenticating, authorizing and reviewing access rights of the Third Parties.
    - Security controls that are in place to control storing, processing, communicating, sharing or exchanging information.

4. All risks identified shall be appropriately addressed through risks mitigation measures and registered in the QHF702 Risk Assessment Register.

4.1.4. EXCHANGE OF INFORMATION

Exchange of information can only be initiated after the NDA is in place. Head of department/ responsible manager should ensure proper controls are planned, implemented, and monitored. Authorizing exchange of information is as per COP401 Information Management Policy.

Information exchanged is classified as:
1- Protected health information
2- Personally identifiable information

4.2. MONITORING AND REVIWEING OF THIRD PARTIES SERVICES

- Respective Projects Managers / Contract Managers shall maintain appropriate reports and records, to monitor and measure the compliance with the information security requirements.
- The Third Parties shall be responsible to take appropriate actions to address any non-conformities that might be identified during the compliance review.
- Security events logging shall be fully activated for all information to which access is provided to Third Parties as per the contractual obligations.

4.3. TERMINATION OF THIRD PARTIES SERVICES

- Proper transition and exit management provisions shall be considered to ensure correct procedures for handing over third party contracts or services back to the National Ambulance.
- Projects Managers / Contract Managers shall ensure that proper transfer of knowledge is obtained from the Third Parties for the ongoing operation / maintenance.
- Upon completion/termination of an engagement with Third Parties, the Projects Managers shall inform the relevant information assets owners/custodians to revoke the access rights of the Third Parties that was granted to information processing facilities.
- Projects Managers / Contract Managers shall ensure that all National Ambulance assets provided to the Third Parties are returned such as laptops, books, manuals, documentation, building keys, magnetic access cards etc.
- Any connections between the Third Parties' network and National Ambulance corporate network shall be terminated in cases of any security breach that may occur or non-compliance of the Third parties to any of the National Ambulance policies.

4.4. REPORTING INFORMATION SECURITY INCIDENTS

- Projects Managers / Contract Managers and all National Ambulance employees shall report any incidents related to Third Parties to QHSE and IT Helpdesk.

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
DoH – ADHICS Abu Dhabi Healthcare Information & Cyber Security Standard	Abu Dhabi

6. RELATED POLICIES AND FORMS

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

Policy & Procedure /Form
PUP103 Procurement Policy

QHP211 Contractor QHSE Management Policy and Procedure
COP401 Information Management Policy
QHP213 QHSE Work Location Management Policy and Procedure
QHF702 Risk Assessment Register

7. FEEDBACK

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

8. 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:

- HR & Corporate Services Manager.

This controlled document is managed / overseen by [Procurement and Tendering Committee and/or Audit and Risk Management Committee and/or HR and Compensation Committee].

Change Brief

Version No.	Date	Change
1	April 2021	*New Policy*

CEO Approval

Board Member Verification