# Operations and Maintenance Plan

# Purpose

The purpose of this service level agreement / Operations and Maintenance Plan is to define the required levels of on-going support for the CRVS system, both hardware and software and identify the people and/or organisations responsible for providing the support.

 1. Support Objectives and Assumptions

## 1.1. Support Objective

List the aims and goals of this Operations and Maintenance Plan e.g. to ensure that the CRVS system is monitored on a 24/7 basis, and that is a business continuity plan in place and that there are processes in place to ensure that interruptions to the CRVS service are minimised when software or hardware is upgraded.

## 2. Support Strategy and Environment

## 2.1. Support Strategy

Use this section to describe how long the Operations and Maintenance Plan will exist, frequency of revisions to the plan, what are the requirements for implementing changes and new releases

## 2.1.1. Support Lifetime

Document the timeframe estimated for the Operations and Maintenance Plan to be in place. List the conditions that require a review of the Operations and Maintenance Plan to capture necessary updates, e.g., every 6 months, a major release of the system, etc.

## 2.2. Support Environment

Describe the technical environment that the CRVS system requires and any special requirements or issues surrounding that environment. If there are multiple environments e.g. for development, training, testing and production, list all of them.

### 2.2.1. Software

### 2.2.2. Hardware and Infrastructure

### 2.2.3. Databases

### 2.2.4. Data Exchange

## 3. Support Responsibilities

### 3.1. Software Maintenance

List who provides maintenance of the software and how they can be contacted.

### 3.2. System Administration

List who provides the systems administration for the hardware and infrastructure and how they can be contacted.

### 3.3. Operational and user support

Consider the criticality of the application to the business function to determine hours and response time and types. Define objectives for maintaining the integrity of the system through data backup and disaster recovery.

### 3.4. Database Administration

List who provides the systems administration for the database and how they can be contacted.

### 3.5 Data Exchange/System Dependencies

List other systems or databases that:

* exchange data with this system
* are dependent on this system
* this system is dependent upon

and identify the organisation and persons responsible for those systems.

### 3.6 Licensing, data rights, and expiration of licenses

Provide a list of licenses, or a location or contact for this data, and include the process for license renewals

### 3.7. Security and Privacy Concerns

List any access restrictions for viewing, update, etc.

## 4. Support Process

*Describe the process that should be followed by end users who want to report a problem, ask for assistance or request a new feature.*

### 4.1. Problem Referral Contacts

Use this list for the final production environment for the system. Examples might be who to contact if a server goes down, for login or connection problems, etc. This may be an identified person within the organisation; it may be a Helpdesk, it may be the vendor under the terms of a service level agreement.

|  |  |  |
| --- | --- | --- |
| Type of Problem | Refer To  | Contact  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### 4.2. Escalation Procedures

*Describe the escalation process to be followed if a reported problem is not resolved within the agreed and expected timeframes.*

## 5. Support Approach

### 5.1. Monitoring and Control

Describe how the CRVS system is monitored. This could be automated monitoring that notifies a designated contact person if a problem occurs and/or it could mean manually checking some aspect of the system or specific components.

### 5.2 Business Continuity

#### 5.2.1 Business Impact Analysis

Conduct a Business Impact Analysis (BIA) to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency.

Document findings from the BIA here.

#### 5.2.2 Preventive Controls

*Define* measures that reduce the effects of system disruptions and can increase system availability and reduce costs.

#### 5.2.4 IT Contingency Plan

*Define a contingency plan that includes detailed guidance and procedures on how to restore a damaged system in any type of issue occurrence.*

#### 5.2.5 Routine Backups

*Describe the routine backup process, responsible persons, backups stored off-site, etc. including the test process to ensure the backups are working.*

#### 5.2.6 Disaster Recovery

*Describe the strategy for responding to unplanned incidents that threaten the CRVS system, which includes hardware, software, networks, processes and people. The aim is to minimise the negative impacts and ensure resumption of normal operations as soon as possible. The plan should identify critical IT systems and networks; prioritise the recovery time objective; and define the steps needed to restart, reconfigure, and recover them. It should include all the relevant contacts, sources of expertise for recovering disrupted systems and a logical sequence of action steps to take for a smooth recovery. This may include fail-over systems, alternative sites, etc.*

#### 5.2.7 Disaster Recovery and Contingency Plan Preparation

#### Define how you will test your disaster recovery and contingency plans to identify planning gaps.

#### Define what disaster recovery training will be provided and to which actors. This will ensure that all those involved in this activity effectively complete their job if/when they need to.

### 5.3 Updates/Release Strategy

Describe how to determine when to release a new version of the system.

#### 5.3.1. Release Process

Describe the steps that you will take before the release of an upgrade/ new version of the system. . This may include information about quality assurance testing, review board, change management, acceptance criteria, etc.

#### 5.3. 2 Regression Test Case

Describe some tests that should always be run when making any system changes to ensure that errors are not introduced when making changes.

## 6. Support Resources

### 6.1. Support Budgets

Develop and document cost estimates for providing ongoing support, including personnel, training, software and hardware. Identify timing for when costs are expected to occur as the system and support are developed, deployed, upgraded and expanded.. Consider growth in capacity required, hardware replacement, and system/database software upgrades, licensing fees, etc.