OPERATIONS MANUAL
FOR
<SYSTEM NAME>

**Quick Reference**

|  |  |  |
| --- | --- | --- |
| Executive Sponsor |  | <Job Title> |
| Business Owner |  |  |
| Technical Owner |  |  |
| Manual Author | <Your Name> | <Your Job Title> |

Table of Contents

[1. Revision History 3](#_Toc359939825)

[2. Key Operational Resources 3](#_Toc359939826)

[3. Introduction 4](#_Toc359939827)

[4. System Overview 4](#_Toc359939828)

[5. Information Inventory 5](#_Toc359939829)

[6. Deployment Profile 5](#_Toc359939830)

[7. Contract Administration 6](#_Toc359939831)

[8. Support Processes 6](#_Toc359939832)

[9. Security Processes 7](#_Toc359939833)

[10. Administrative Processes 7](#_Toc359939834)

[11. Appendix A 9](#_Toc359939835)

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision # | Date | Author | Comment |
| 1.0 | <YYYY-MM-DD> | <Your Name> | Original Document |
|  |  |  | <Annual updates (minimum) are recommended> |

# Key Operational Resources

<The purpose of this section is to eliminate any confusion over where system documentation is kept. Fill this table out with key documents, locations or websites related to operations. Give the location of the resource and hyperlink to it, whether it’s on the network drive, DIIMS, SharePoint, a website, etc… If there are operational intranet sites, public operational sites, etc… list them all.>

|  |  |
| --- | --- |
| Key Operational Documents | Where to Find |
| Operations Manual (this document) | Network Drive |
| Disaster Recovery Plan | Network Drive |
| Implementation Report | Network Drive |
| TSC System Guide | Network Drive |
| System Team Site | SharePoint |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Introduction

<The following sections vary substantially from system to system, department to department. Feel free to modify, add or remove sections to meet your needs. This template is only a starting place to help you cover many different areas. There is no requirement to fill in any particular section or to use any particular format.>

## Introduction and Purpose

<This section introduces and describes the purpose of the Operations Manual, the audience of the manual, the name of the system to which it applies>

<The intent of this manual is to bring together all the knowledge required by the operations team into a single document that can be easily taken offline and/or secured. Many sections are better treated elsewhere (like on a support team wiki) or specialized plans and documents. This manual should use hyperlinks to those documents wherever possible. Therefore, the only details in this manual should be those not found anywhere else, those too sensitive for other documents, or those too critical to be hyperlinked (since the network might be down when needed).>

## Note about the Security of this Manual

This manual contains sensitive information, which, in the wrong hands, could facilitate a major security breach. Distribution of this manual should be as limited as possible. This manual may contain sensitive details, such as how the system is secured, but **NOT** passwords or personal information. Security processes for sensitive documentation, such as this manual, are described below in Section 9.5.

## Glossary

|  |  |
| --- | --- |
| Special Term | Definition |
| <Acronyms, etc…> |  |
|  |  |

# System Overview

## System Application

<This section should answer the question: What is the system? It provides a brief description of the system, including its purpose and uses. It situates the system in its organizational context, related to other applications.>

## System Organization

<This section describes the organization of the system by the use of a chart depicting components and their interrelationships. This section should be kept at a high-level and should show how it fits into the broader organization. A more detailed component inventory, detailing the internal mechanics of the system, is given in Section 6.2>

## Codebase

<If appropriate, describe where the system’s code resides and how it is managed. Describe the version control system used, the programming language used, the typical development tools, etc… Even if the system is acquired, you still can describe how any configuration files and scripts are managed.>

## Systems Integration

<Describe the points of integration of this system with other systems, such as SAM. Include a diagram if appropriate. Reference any documents that pertain to the integration as well as any processes in this document that are related, using hyperlinks wherever possible. Detailed integration descriptions, such as data types, standards, formats, protocols, etc… should be reserved for a later section on specific processes or an external specification document.>

# Information Inventory

<This section provides information about data files, data sets and the databases that are produced or referenced by the system. This information is here described at a high level. Deployment details, such as number, configuration and location of database servers, can be treated in Section 6.>

## Data Store Inventory

<This section lists all permanent data stores and databases that are referenced, created, or updated by the system. Use a table if appropriate.>

## Report Inventory

<This section lists all reports produced by the system, including each report name and the software that generates it. Use a table if appropriate.>

# Deployment Profile

<This section should answer the question: How is the system deployed? This involves the hardware the system runs on, the various software components installed (including major versions), and the configuration of the system (including settings, users, permission schemes, etc…). Refer to other documents or appendices for any detailed lists. Processes should be described later on in Section 10.>

## Deployment History

<Give a brief history of the deployment of the system into production. Give dates, people involved, activities, exceptions, work-arounds, etc… Reference the [Implementation Report](http://test.fin.gov.nt.ca/ocio/sim/sdlc/2/), if possible.>

## Component Inventory

<Describe the different hardware and software deployed that comprise this system. For instance, there could be different modules of an application, an application server, a web server, a database server, as well as various other libraries, tools, extension and programs. The purpose here is to provide a thorough list of parts. You don’t need to describe all the processes around them here.>

<For instance, a list of servers could be presented as follows. A similar table could be made for software components, including the database server software.>

|  |  |  |
| --- | --- | --- |
| Common Name | URL | Notes for Support Staff and TSC |
| <The usual name this server is called> | <\\YKAPPXX\> | <Any notes that would help the support staff, such as resources assigned (like number of cores), the OS version, how/when to patch the server, failover capacity, which group can access it, major applications run, etc…> |
|  | <\\YKVSQLXX> |  |

## Key Software Configuration Profiles

<This section should answer the question: How is the system configured? The information should allow the operational team to understand the areas that are configured, where to find the configuration, what format it is in, how to change it, what the rationale is for key configuration decisions, etc… The user permissions structure (such as Active Directory groups) should be described here, too, as it is usually a major area of configuration that is critical for operational teams to understand.>

# Contract Administration

<This section answers the question: What does the operational team need to know about any ongoing contracts in place and what do they need to do to manage those contracts?>

## Contract History

<Describe the history that has been established between the project/system team and the vendor, especially the vendors that will continue supporting the system in operations. Make reference to key emails, documents, contracts, etc… with hyperlinks if possible>

## Vendor Management

<What does the operational team need to know to manage the vendor properly? What service levels have been established, either formally or informally? How is vendor performance monitored and corrected?>

# Support Processes

<This section should answer the question: How is the system supported? This refers to training, service desk operations, troubleshooting, error-tracking and so on>

## Training

<How is training accomplished? Who does it? How often? What are the resources used?>

## Service Desk

<What do system users do if they have problems? Who do they call or email? How do calls get triaged and tracked? How do system problems get sorted out from network/desktop issues (TSC)? How is service quality monitored and improved?>

<Describe the typical requests that are handled by the application support service desk and the TSC service desk. How are the requests triaged and responded? If this information is better described elsewhere, remove this table and reference the document.>

|  |  |  |
| --- | --- | --- |
| Service Desk Request | Received By | Request Response |
| <The nature of the request> | <Application Support Team> | <What does the support team do to respond to this request?> |
|  | <TSC Service Desk> |  |

## Troubleshooting

<How are problems diagnosed, tracked and solved? How are issues resolved with the vendor? What tools are used for this, such as a bug-tracking system or a knowledge center (like a wiki)?>

## Planned Outage

<This section should answer the question: When is the planned outage for this system and what should be done routinely during this time? This can covering routine activities, processes, checks, as well as staffing and overtime issues. Explain if the outage must be coordinated with the TSC. If your department has a general approach to planned outage, it should be referenced here.>

# Security Processes

<This section answers the question: What does the operational team need to do to keep information secure and the system available? It should describe the security mechanisms, but not divulge critical pieces of information, like passwords.>

## Certificates, Credentials & Algorithms

<Describe any security certificates, 3rd-party credentials, authentication schemes or encryption algorithms used by the system that the operational team should be aware of. For instance, if passwords are salted and encrypted, give the salting algorithm and encryption type. (For information on protecting the information in this manual, see Section 9.5 below.>

## Incident Response

<This section should answer the question: How are security incidents handled for this system? How are incidents logged? Who is the contact for incidents? Refer to documents such as the Threat Risk Assessment, Disaster Recovery Plan, departmental incident response plans, etc…

## Disaster Recovery

<This section should answer the question: How is the system recovered in an emergency? Also, how can we be sure that our disaster recovery plan is valid? Describe the people involved, the process, the test plan and so on. Do not duplicate anything already in other documents, unless you absolutely need it in this document in an offline/paper scenario. Wherever possible refer and link to documents, such as the Disaster Recovery Plan.>

## Business Continuity

<This section should answer the question: How will the business that the application supports continue in the event of a prolonged outage? Describe what the operational team needs to do to coordinate with the business units before, during and after outages. It is unlikely that a complete business continuity plan is best addressed on a system-by-system basis (it’s usually per government program), so the details here should mostly relate how this system fits into the larger plan. Likewise with the DRP, do not duplicate any details better presented elsewhere – refer and hyperlink to other documents.>

## Documentation Security

<This section should answer the question: How are sensitive operational documents, such as this manual, kept secure and available? For instance, the manager might keep an original copy on a personal drive and only make a password-protected encrypted PDF available to the team, the password being shared only offline. Contact the OCIO Security Group for more options.>

# Administrative Processes

<This section answers the question: What does the operational team need to routinely do in order to keep the system running? This involves patching, back-ups, system shut-down and start-up, batch processes and much more. The structure and grouping of the various processes will depend on your system but an example is given below.>

## Shut-Down and Start-Up

<Consider using a common structure for each process, such as the following.>

### Purpose

<State the purpose of the process, when it is uses, what it is intended to do, what the effect is, etc…>

### Process Steps

1. <List each step in the process. Replace with a flowchart, or link to a Visio diagram, if preferred. Include how you check to see if the process was successful.>

### Exceptions

1. <List exceptions to this process, if the above section does not cover exceptions.>

## Patching

## Back-up Validation

## Batch Processing

## On-Boarding New Users

## Off-Boarding Departing Users

## On-Boarding New Administrators

## Off-Boarding Departing Administrators

## Desktop Client Installation

# Appendix A

<Use the appendices for extra information, charts, tables, diagrams, etc… but also consider keeping those in external documents and hyperlinking to them. The only lengthy details that should be in this document are those that are vital in a full emergency, where the network is seriously impaired (where a local or paper copy may be the only resource).>