

# **Fantastic Information Security Contingency Plan (ISCP)**

## Change Record

Date	Version	Author	Changes Made / Section(s)
15 Feb 2021	1.0	HCoS Durkaj	Initial Document

## Table of Contents

1.	OVERVIEW
2.	INTRODUCTION
3.	CONCEPT OF OPERATIONS
4.	ACTIVATION AND NOTIFICATION
5.	RECOVERY
6.	RECONSTITUTION
7.	SIGNATURE
APPENDIX A – PERSONNEL CONTACT LIST	
APPENDIX B – DETAILED BACKUP AND RECOVERY PROCEDURES	
APPENDIX C – ALTERNATE PROCESSING PROCEDURES	
APPENDIX D – SYSTEM VALIDATION TEST PLAN	
APPENDIX E – TEST AND MAINTENANCE SCHEDULE	
APPENDIX F – LESSONS LEARNED / AFTER ACTION REPORTS	
APPENDIX G – BUSINESS IMPACT ANALYSIS	
ENCLOSURE 1 – CONTINGENCY PLAN TEST REPORT TEMPLATE	
ENCLOSURE 2 – AFTER ACTIONS REPORT TEMPLATE	
ENCLOSURE 3 – TRAINING RESOURCES	

## 1. OVERVIEW

There is a subtle difference between an ISCP and a COOP. These difference will not be outlined and for all intents and purposes, this document shall act as both ISCP and COOP.

Information systems are vital elements in most mission/business processes. Because information system resources are so essential to an organization's success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption. Contingency planning is unique to each system, providing preventive measures, recovery strategies, and technical considerations appropriate to the system's information confidentiality, integrity, and availability requirements and the system impact level.

This document does not address facility-level information system planning (commonly referred to as a disaster recovery plan) or organizational mission continuity (commonly referred to as a continuity of operations [COOP] plan) except where it is required to restore information systems and their processing capabilities. Nor does this document address continuity of mission/business processes

Information system contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption. Contingency planning generally includes one or more of the following approaches to restore disrupted services:

- 1) Restoring information systems using alternate equipment;
- 2) Performing some or all of the affected business processes using alternate processing (manual) means (typically acceptable for only short-term disruptions);
- 3) Recovering information systems operations at an alternate location (typically acceptable for only long-term disruptions or those physically impacting the facility); and
- 4) Implementing of appropriate contingency planning controls based on the information system's security impact level.

This document complies with the following requirements from NIST Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations". A detailed compliance matrix can be found in the Fantastic System (FS) eMASS Artifacts.

## 2. INTRODUCTION

Information assets are vital to FANTASTIC SYSTEM (FS)'s mission/business processes; therefore, it is critical that services provided by FANTASTIC SYSTEM (FS) are able to operate effectively without excessive interruption. This Information System Contingency Plan (ISCP) establishes comprehensive procedures to recover FANTASTIC SYSTEM (FS) quickly and effectively following a service disruption.

### a. Background

This FANTASTIC SYSTEM (FS) ISCP establishes procedures to recover FANTASTIC SYSTEM (FS) following a disruption. The following recovery plan objectives have been established:

- 1) Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - a. Activation and Notification phase to activate the plan and determine the extent of damage;
  - b. Recovery phase to restore FANTASTIC SYSTEM (FS) operations; and

- c. Reconstitution phase to ensure that FANTASTIC SYSTEM (FS) is validated through testing and that normal operations are resumed.
- 2) Identify the activities, resources, and procedures to carry out FANTASTIC SYSTEM (FS) processing requirements during prolonged interruptions to normal operations.
- 3) Assign responsibilities to designated FANTASTIC SYSTEM (FS) personnel and provide guidance for recovering FANTASTIC SYSTEM (FS) during prolonged periods of interruption to normal operations.
- 4) Ensure coordination with other personnel responsible for FANTASTIC SYSTEM (FS) contingency planning strategies. Ensure coordination with external points of contact and vendors associated with FANTASTIC SYSTEM (FS) and execution of this plan.

#### **b. Scope**

This ISCP has been developed for FANTASTIC SYSTEM (FS), which is classified as an **Availability = LOW** impact system, in accordance with Federal Information Processing Standards (FIPS) 199 – Standards for Security Categorization of Federal Information and Information Systems. Procedures in this ISCP are for Low- Impact systems and designed to recover FANTASTIC SYSTEM (FS) within 5 DAYS. This plan does not address replacement or purchase of new equipment, short-term disruptions lasting less than 5 DAYS; or loss of data at the onsite facility or at the user-desktop levels. As FANTASTIC SYSTEM (FS) is a low-impact system, alternate data storage and alternate site processing are not required.

#### **c. Assumptions**

The following assumptions were used when developing this ISCP:

- FANTASTIC SYSTEM (FS) has been established as a low-impact system for Availability purposes, in accordance with FIPS 199.
- Alternate processing sites and offsite storage are not required for this system.
- The FANTASTIC SYSTEM (FS) is inoperable and cannot be recovered within 5 days.
- Key FANTASTIC SYSTEM (FS) personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the FANTASTIC SYSTEM (FS) Contingency Plan.

The FANTASTIC SYSTEM (FS) ISCP does not apply to the following situations:

- Overall recovery and continuity of mission/business operations. The Business Continuity Plan (BCP) and Continuity of Operations Plan (COOP) address continuity of mission/business operations.
- Emergency evacuation of personnel. The Occupant Emergency Plan (OEP) addresses employee evacuation

### **3. CONCEPT OF OPERATIONS**

The Concept of Operations section provides details about FANTASTIC SYSTEM (FS), an overview of the three phases of the ISCP (Activation and Notification, Recovery, and Reconstitution), and a description of roles and responsibilities of FANTASTIC SYSTEM (FS)'s personnel during a contingency activation.

#### **a. System Description**

FANTASTIC SYSTEM (FS) is a terrible, indescribable thing vaster than any subway train - a shapeless congeries of protoplasmic bubbles, faintly self-luminous, and with myriads of temporary eyes forming and un-forming as pustules of greenish light all over the front that bore down upon the System Administrators, crushing the frantic users and slithering over the glistening floor that it and its kind had swept so evilly free of all litter.

**i. Essential Mission**

The FANTASTIC SYSTEM (FS) system encompasses many modules that perform specific functions in the eldritch abyss. Each module has varying restrictions on access privileges.

**ii. Essential Business Function**

The FANTASTIC SYSTEM (FS) system is developed for and sponsored by the High Chancellor of Security to act as multi-purpose terraforming and colonization tool for elder things.

**b. Overview of Three Phases**

This ISCP has been developed to recover and reconstitute the FANTASTIC SYSTEM (FS) using a three-phased approach. This approach ensures that system recovery and reconstitution efforts are performed in a methodical sequence to maximize the effectiveness of the recovery and reconstitution efforts and minimize system outage time due to errors and omissions. The three system recovery phases are Activation and Notification, Recovery, and Reconstitution.

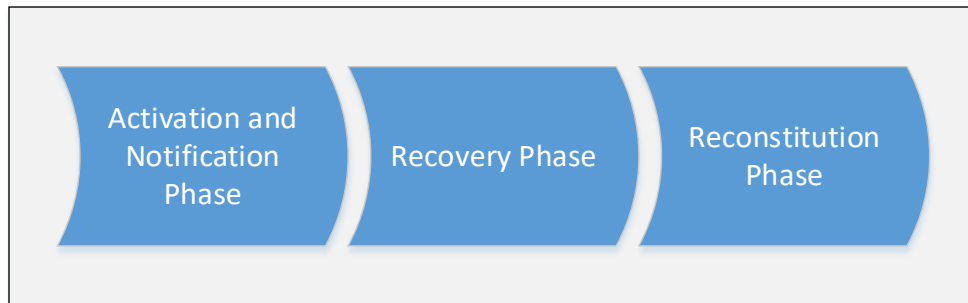


Figure 1 – The Three Phases

**c. Roles and Responsibilities**

The ISCP establishes several roles for FANTASTIC SYSTEM (FS) recovery and reconstitution support. Persons or teams assigned ISCP roles have been trained to respond to a contingency event affecting FANTASTIC SYSTEM (FS).

- i. System Owner / Program Manager:** This individual is a Senior Manager is responsible to Executive Management for all facets of contingency planning and exercises, as well as for recovery operations.
- ii. ISCP Coordinator / Project Manager:** This individual is responsible for managing the total recovery effort; for ensuring that other personnel perform all checklist items and for coordination and overall communications.
- iii. Technical Recovery Lead:** This individual has a full understanding of the technical aspects of the system.

**4. ACTIVATION AND NOTIFICATION**

The Activation and Notification Phase defines initial actions taken once a FANTASTIC SYSTEM (FS) disruption has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the ISCP. At the completion of the Activation and Notification Phase, FANTASTIC SYSTEM (FS) ISCP staff will be prepared to perform recovery measures.

**a. Activation Criteria and Procedure**

The FANTASTIC SYSTEM (FS) ISCP may be activated if one or more of the following criteria are met:

- 1) The type of outage indicates FANTASTIC SYSTEM (FS) will be down for more than 5 days;
- 2) The facility housing FANTASTIC SYSTEM (FS) is damaged and may not be available within 5 days; and

The following persons or roles may activate the ISCP if one or more of these criteria are met:

- System Owner
- ISCP Coordinator
- Technical POC

**b. Notification**

The first step upon activation of the FANTASTIC SYSTEM (FS) ISCP is notification of appropriate mission/business and system support personnel. Contact information for appropriate POCs is included in Appendix A, "Personnel Contact List".

For FANTASTIC SYSTEM (FS), the following method and procedure for notifications can be used:

- Phone Call
- Email
- In-person

As stated previously, any role within the process can execute initial notification.

**c. Outage Assessment**

Following notification, a thorough outage assessment is necessary to determine the extent of the disruption, any damage, and expected recovery time. Assessment results are provided to the ISCP Coordinator to assist in the coordination of the recovery of FANTASTIC SYSTEM (FS).

The following procedures will be followed:

- Determines if there has been loss of life or injuries
- Assesses the extent of damage to the facilities and the information systems
- Estimates the time to recover operations
- Determines accessibility to facility, building, offices, and work areas
- Assess the need for and adequacy of physical security/guards
- Advises the ISCP Coordinator that physical security/guards are required
- Identify salvageable hardware
- Maintain a log/record of all salvageable equipment
- Estimates levels of outside assistance required
- Report updates, status, and recommendations to the ISCP Coordinator

**5. RECOVERY**

The Recovery Phase provides formal recovery operations that begin after the ISCP has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. The following Recovery Objectives have been identified:

- 1) restore system capabilities
- 2) repair damage
- 3) resume operational capabilities at the original location

At the completion of the Recovery Phase, FANTASTIC SYSTEM (FS) will be functional and capable of performing the functions identified in Section 3.a of this plan.

**a. Sequence of Recovery Activities**

The following activities occur during recovery of FANTASTIC SYSTEM (FS):

- 1) Identify recovery location (if not at original location);
- 2) Identify required resources to perform recovery procedures;
- 3) Retrieve backup and system installation media;
- 4) Recover hardware and operating system (if required); and
- 5) Recover system from backup and system installation media.

**b. Recovery Procedures**

Recovery procedures are outlined in Appendix B, “Detailed Backup and Recovery Procedures” and will be executed in the sequence presented to maintain an efficient recovery effort.

**c. Recovery Escalation Notices/Awareness**

During the Recovery Process, it is extremely important to keep both senior management and the general user population aware of all activities and status. The ISCP Coordinator is responsible for communicating status through either phone, email or in-person to the general user population. If the outage escalates and potentially causes outages to other systems or networks, the ISCP Coordinator will up-channel reporting to the CIO so that other teams are notified.

## **6. RECONSTITUTION**

Reconstitution is the process by which recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. A determination must be made on whether the system has undergone significant change and will require reassessment and reauthorization. The phase consists of two major activities: validating successful reconstitution and deactivation of the plan.

**a. Validation Testing**

Validation data testing is the process of testing and validating data to ensure that data files have been recovered completely at the permanent location and the system is ready to return to normal operations. Updated procedures are maintained by System Administrators within the Technical POS’s office and will be recorded via copy of the System Validation Test Plan outlined in Appendix D.

**b. Recovery Declaration**



Upon successfully completing testing and validation, the FANTASTIC SYSTEM (FS) will formally declare recovery efforts complete, and that FANTASTIC SYSTEM (FS) is in normal operations. FANTASTIC SYSTEM (FS) business and technical POCs will be notified of the declaration by the ISCP Coordinator.

**c. Notifications (Users)**

Upon return to normal system operations, FANTASTIC SYSTEM (FS) users will be notified by the System Owner or ISCP Coordinator using predetermined notification procedures (e.g., email, phone calls, etc.).

**d. Data Backup**

As soon as reasonable following recovery, the system should be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup is then kept with other system backups. The procedures for conducting a full system backup are located in Appendix B, "Detailed Backup and Recovery Procedures".

**e. Event Documentation**

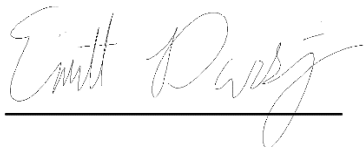
It is important that all recovery events be well-documented, including actions taken and problems encountered during the recovery and reconstitution effort, and lessons learned for inclusion and update to this ISCP. It is the responsibility of each ISCP team or person to document their actions during the recovery and reconstitution effort, and to provide that documentation to the ISCP Coordinator. The process contained within Appendix F, "Lessons Learned and After Action Reports" will be followed.

**f. Deactivation**

Once all activities have been completed and documentation has been updated, FANTASTIC SYSTEM (FS) will formally deactivate the ISCP recovery and reconstitution effort. Notification of this declaration will be provided to all business and technical POCs

**7. Policy Review**

This Contingency Plan for FANTASTIC SYSTEM (FS) must be reviewed annually by (at a minimum) the ISSM, ISSO, Project Manager, and Technical Recovery Lead. Changes to this document must be routed to the BCOM commander for signature.



High Chancellor of Security (HCoS),  
Emmitt Durkaj  
555-555-5555

DURKAJ.EM  
MITT.ALLEN.  
12345678

Digitally signed by  
DURKAJ.EMMITT.AL  
LEN. 1234567890  
Date: 2021.02.21  
18:08:30 -05'00'

## APPENDIX A – PERSONNEL CONTACT LIST

ISCP Key Personnel		
Key Personnel		Contact Information
<b>System Owner / Program Manager</b>	Work	555-555-5555
Gerard Way	Email	Gerard.Way@Hotmail.com
<b>ISCP Coordinator / Project Manager</b>	Work	555-555-5555
Frank Lero	Email	Frank.Lero@PBS.org
<b>User Representative</b>	Work	555-555-5555
Mikey Way	Email	Micheal.Way@gmail.com
<b>ISSM</b>	Work	555-555-5555
Ray Toro	Email	Babble inconsistently
<b>ISSO</b>	Work	555-555-5555
Bob Bryar	Email	Travis.Barker@yahoo.com
<b>Technical POC</b>	Work	555-555-5555
Tracy Phillips	Email	Ucandanceifyouwantto@navy.gov
<b>Service Desk</b>	Work	555-555-5555
After Hours – Contact Key Personnel via Service Desk	Work	555-555-5555

## **APPENDIX B – DETAILED BACKUP AND RECOVERY PROCEDURES**

### **Recovery Process Overview**

#### **Contact Order**

### **Priority of Storage System Restoration**

#### **System A**

#### **System B**

#### **System C**

### **Database Server Restoration**

#### **Contact these guys**

### **Application Server Restoration**

#### **Recovery Process Summary:**

Once the application servers and, database server, and networking capabilities have been restored, Administrators and FANTASTIC SYSTEM (FS) team members will verify the restoration from backup, connectivity to the databases, background services, and FANTASTIC SYSTEM (FS) web application functionality. Test data loads will then be conducted to verify that the tools and all connectivity are functioning as expected.

Full information system restoration without deterioration of the security safeguards is a goal of the recovery process. ACAS scans and recovery steps completed by the Administrators and FANTASTIC SYSTEM (FS) team will confirm functional and security posture restoration.

Full system backups will back up all the data on a system to media on a different system than the system or volume being backed up. Full backups will be performed once a week and the data retained for 30 days per basic services or as specified in a signed Service Level Agreement (SLA). A copy of the full volume backup will be made for offsite storage at either a commercial approved or government site. Unless otherwise specified within a customer Service Level Agreement (SLA), the established standard offsite facilities are established per the Offsite Backup MOA dated September 2018.

## APPENDIX C – ALTERNATE PROCESSING PROCEDURES

This section identifies alternate manual or technical processing procedures available that allow the business unit to continue some processing of information that would normally be done by the affected system.

### Information System Disruption

Maintaining Essential Mission. FANTASTIC SYSTEM (FS) is not considered Mission Essential. During a Contingency Event, unaffected assets will continue work as before. For affected assets, if they are a higher priority than the currently operational assets then operational assets will be re-purposed to prioritize continuing mission. In the event the full system is impacted for more than 5 DAYS, the System Owner will contact the Program sponsor to activate the overarching Business Continuity Plan, which is outside the scope of this document.

Maintaining Business Functions. During a Contingency Event, unaffected assets will continue work as before. For affected assets, if they are a higher priority than the currently operational assets then operational assets will be re-purposed to prioritize continuing mission. In the event the full system is impacted for more than 5 DAYS, the System Owner will contact the Program sponsor to activate the overarching Business Continuity Plan, which is outside the scope of this document. All documentation, meetings and face-to-face communications will continue to occur.

### Information System Compromise

Maintaining Essential Mission. FANTASTIC SYSTEM (FS) is not considered Mission Essential. During a Contingency Event, unaffected assets will continue work as before. For affected assets, if they are a higher priority than the currently operational assets then operational assets will be re-purposed to prioritize continuing mission. In the event the full system is impacted for more than 5 DAYS, the System Owner will contact the Program sponsor to activate the overarching Business Continuity Plan, which is outside the scope of this document.

Maintaining Business Functions. During a Contingency Event, unaffected assets will continue work as before. For affected assets, if they are a higher priority than the currently operational assets then operational assets will be re-purposed to prioritize continuing mission. In the event the full system is impacted for more than 5 DAYS, the System Owner will contact the Program sponsor to activate the overarching Business Continuity Plan, which is outside the scope of this document. All documentation, meetings and face-to-face communications will continue to occur.

### Information System Failure

Maintaining Essential Mission. FANTASTIC SYSTEM (FS) is not considered Mission Essential. During a Contingency Event, unaffected assets will continue work as before. For affected assets, if they are a higher priority than the currently operational assets then operational assets will be re-purposed to prioritize continuing mission. In the event the full system is impacted for more than 5 DAYS, the System Owner will contact the Program sponsor to activate the overarching Business Continuity Plan, which is outside the scope of this document.

Maintaining Business Functions. During a Contingency Event, unaffected assets will continue work as before. For affected assets, if they are a higher priority than the currently operational assets then operational assets will be re-purposed to prioritize continuing mission. In the event the full system is impacted for more than 5 DAYS, the System Owner will contact the Program sponsor to activate the overarching Business Continuity Plan, which is outside the scope of this document. All documentation, meetings and face-to-face communications will continue to occur.

## APPENDIX D – SYSTEM VALIDATION TEST PLAN

Example outlined in row 1.

[illegible]

## APPENDIX E – TEST AND MAINTENANCE SCHEDULE

The ISCP is reviewed and tested yearly or whenever there is a significant change to the system. For low-impact systems, a yearly tabletop exercise is sufficient.

FISMA testing is completed yearly for Contingency Testing, Controls Testing, and Annual Review of plan and procedure documentation. FANTASTIC SYSTEM (FS) coordinates with all roles to schedule and participate in yearly FISMA testing. Disaster Recovery Plan (DRP) testing may or may not be conducted, based upon direction and availability.

A test of the FANTASTIC SYSTEM (FS) incident response capability will be conducted in accordance with FISMA and validation of this Contingency Plan. Per direction from the High Chancellor of Security, an incident will be reported by an appointed user. The details of this incident will be communicated to the High Chancellor of Security.

Standard incident reporting procedures will be enacted per the Fantastic Incident Response Plan and recorded on the approved incident reporting form for lessons learned after the incident has been resolved.

## APPENDIX F – LESSONS LEARNED / AFTER ACTION REPORTS

### LESSONS LEARNED

One of the most important parts of contingency planning is also the most often omitted: learning and improving. The FANTASTIC SYSTEM (FS) contingency planning team will evolve to reflect new threats, improved technology, and lessons learned. Holding a “lessons learned” meeting with all involved parties after a major contingency, and optionally periodically after lesser contingencies as resources permit, can be extremely helpful in improving security measures and the contingency planning process itself. Multiple contingencies can be covered in a single lessons learned meeting. This meeting provides a chance to achieve closure with respect to a contingency by reviewing what occurred, what was done to intervene, and how well intervention worked. The meeting should be held within several days of the end of the contingency. Questions to be answered in the meeting include:

- 1) Exactly what happened, and at what times?
- 2) How well did staff and management perform in dealing with the contingency? Were the documented procedures followed? Were they adequate?
- 3) What information was needed sooner?
- 4) Were any steps or actions taken that might have inhibited the recovery?
- 5) What would the staff and management do differently the next time a similar contingency occurs?
- 6) How could information sharing with other organizations have been improved?
- 7) What corrective actions can prevent similar contingency in the future?
- 8) What precursors or indicators should be watched for in the future to detect similar contingencies?
- 9) What additional tools or resources are needed to detect, analyze, and mitigate future contingencies?

Small contingencies s need limited post- contingency analysis, with the exception of contingencies s performed through new attack methods that are of widespread concern and interest. After serious attacks have occurred, it is usually worthwhile to hold post-mortem meetings that cross team and organizational boundaries to provide a mechanism for information sharing. The primary consideration in holding such meetings is ensuring that the right people are involved. Not only is it important to invite people who have been involved in the contingency that is being analyzed, but also it is wise to consider who should be invited for the purpose of facilitating future cooperation.

The success of such meetings also depends on the agenda. Collecting input about expectations and needs (including suggested topics to cover) from participants before the meeting increases the likelihood that the participants’ needs will be met. In addition, establishing rules of order before or during the start of a meeting can minimize confusion and discord. Having one or more moderators who are skilled in group facilitation can yield a high payoff. Finally, it is also important to document the major points of agreement and action items and to communicate them to parties who could not attend the meeting.

Because of the changing nature of information technology and changes in personnel, the contingency planning team will review all related documentation and procedures for handling contingencies s at designated intervals.

### AFTER ACTIONS REPORTS

The After Actions Report (AAR) provides evaluation criteria based on the exercise objectives and a means to evaluate how well exercise objectives were met, and identify areas where additional exercises might be necessary. Evaluating the exercise is a critical step to ensuring success of the contingency response program. After the test or exercise is complete, the participants will conduct a debriefing to discuss observations for things that worked well and things that could be improved. The comments that surface during the debriefing, along with lessons learned documented during the exercise, will be captured in the AAR. The AAR will also document observations made throughout the exercise and participants during the exercise and recommendations for enhancing the IR plan that was exercised.

## **METRICS**

The FANTASTIC SYSTEM (FS) contingency planning team will collect the below data, which will be used to measure the success of the contingency team.



## ENCLOSURE 1 – CONTINGENCY PLAN TEST REPORT TEMPLATE

Test Information	Description
<b>Name of Test</b>	
<b>System Name</b>	
<b>Date of Test</b>	
<b>Team Test Lead and Point of Contact</b>	
<b>Location Where Conducted</b>	
<b>Participants</b>	
<b>Components</b>	
<b>Assumptions</b>	
<b>Objectives</b>	Assess effectiveness of coordination among recovery personnel  Assess effectiveness of procedures  Assess effectiveness of notification procedures
<b>Methodology</b>	
<b>Activities and Results (Action, Expected Results, Actual Results)</b>	
<b>Post Test Action Items</b>	
<b>Recommended Changes to Contingency Plan Based on Test Outcomes</b>	

## ENCLOSURE 2 – AFTER ACTIONS REPORT TEMPLATE

### 1.0 Introduction

On {DATE}, FANTASTIC SYSTEM (FS) participated in a tabletop exercise designed to validate their understanding of the FANTASTIC SYSTEM (FS) Information Systems Contingency Plan.

### 2.0 Objectives

The exercise objectives are as follows:

- Validate the team's ability to respond to contingencies
- Validate the accuracy of procedures documented in the FANTASTIC SYSTEM (FS) Information Systems Contingency Plan
- Identify areas of the FANTASTIC SYSTEM (FS) Information Systems Contingency Plan that need to be revised.

### 3.0 Agenda

Date	{DATE}
Location	{LOCATION}
Exercise Name	{EXERCISE NAME}
{TIME}	Welcoming Remarks and Introductions
{TIME}	Exercise Briefing (Objectives, Rules of Engagement, etc.)
{TIME}	Scenario Discussion
{TIME}	Debrief/Hotwash

### 4.0 Discussion of Findings

The {EXERCISE NAME} provided information on the FANTASTIC SYSTEM (FS) Information Systems Contingency Plan. An important benefit of the exercise was the opportunity for participants to raise important questions, concerns, and issues. The discussion findings from the exercise along with any necessary recommended actions are as follows:

	Subject	Observation	Recommendations
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			

