National Aeronautics and
Space Administration (NASA)

NASA Shared Services Center
Stennis Space Center, MS
39529-6000

www.nssc.nasa.gov

NASA Shared Services Center Business Continuity Plan

NSBCP-1040-0006 Revision 7.0

Effective Date: **June 13, 2014**
Expiration Date: **May 5, 2015**

NSSC Information Technology Division Business Continuity Plan

REDACTED

Responsible Office: Information Technology Division

Approved by:

/s/ James A. Walker

Chief Information Officer (Acting)
NASA Shared Services Center

13 June, 2014
Date Signed

DOCUMENT HISTORY LOG

Status (Basic/Revision Cancelled)	Document Version	Effective Date	Description of Change
Basic		12/1/2006	• This document was created as a guideline for IT Department's Continuity of Operations Plan and Disaster Recovery Plan.
Revision	C	5/31/2011	• Revision A was renamed and restructured; Content updated to include current business practices, recovery guidelines, and procedures; Added section for "Ride-Out" Crew; • Document Number changed from NSSC-DP 0014 effective May, 2010; • Revision A modified the Plan's formal title and control number (May 2010); • All Tables, Figures, and Appendices were updated; • Revision B replaced the IT Division Chief name and contact information.
Revision	5.0	6/28/2012	• Document Number was changed in order to align it with NASA's Standard Document Numbering System. • Updated Appendix J SunGard Activation Plan; • Replaced SunGard MOA STEN in Appendix H; • Appendix K Modified: Oracle Representative changed; • Added Appendix Y, NSSC VOIP

Status (Basic/Revision Cancelled)	Document Version	Effective Date	Description of Change
			BCP; Updated Appendix H SunGard MOA; Updated 9.2.1.2 and 9.2.1.3 due to new BCPs from HR and PRO; • Updated Appendix H due to new SunGard Sten V6; Updated Appendix Y (NSSC VoIP BCP) due to vendor and NSSC personnel changes; Updated Table 9-1; • Replaced Appendix O (Gateway); Updated Appendix L (for KSC); Modified Figure 1-1 due to IT (SP) restructuring; Removed all references to SunGard; Added second BMC Customer Number; Updated Appendix H with ESD-A MOU (dated 4-4-2012); Replaced Appendix G; • Updated Appendix D; Replaced DC structure to NCCIPS locations; Added NSSC-NCCIPS MOU; Updated Appendix E (DR Vault); Per B&A guidance, Appendix U was deleted since its referenced documents exist in TechDoc already; and Appendix Y (VoIP BCP) was removed and created as a stand-alone BCP per B&A direction; • Replaced embedded documents with links to TechDoc or NASA per B&A direction; Updated Appendix B, Plan distribution;

Status (Basic/Revision Cancelled)	Document Version	Effective Date	Description of Change
Revision	6.0	7/26/2013	• Updated Table 1-1 for IT (SP) Manager contact; Updated personnel changes within lists/tables and loss of VoIP Contract (BCP); • Replaced Table 9-1; Updated Appendix D; Updated Table 1-1; Updated Appendix E; Updated Appendix K; Replaced Master Records Index in Appendix T; Updated Appendix E information relating to take backups; Corrected typo in Appendix J; • Modified Table 1-1 to include NICS and ACES POCs; Removed all DR related sections per DCIO Jim Walker; Added Appendix L per DCIO Jim Walker.
Revision	7.0	6/13/14	• Updated Appendix C; Updated Table 1-1; Updated Appendix C; • Updated Appendix D; Relocated Appendix K to ESC BCP (Doc_Img); Redesignated remaining Appendices; • Updated Table 6-1 replacing 'Assistant Pro' with 'DrugPak'; • Modified Expiration Date to May, [2015] in order to align with all other NSSC BCPs.

TABLE OF CONTENTS

APPENDICES

FIGURES

TABLES

1.0 INTRODUCTION

The National Aeronautics and Space Administration (NASA) Shared Services Center (NSSC) Information Technology (IT) Division Business Continuity (BC) Plan (BCP) has been re-titled and restructured to focus only on business continuity practices within IT.

Explanation of the acronyms and abbreviations used within this document is found in Appendix A – Acronyms and Abbreviations.

Below, Table 1-1 – IT Management Team Contacts, identifies the division's leadership team comprised of Civil Servants (CS), Service Providers (SP), and team support from the Agency Consolidated End-User Services (ACES) and NASA Integrated Communications Services (NICS).

Title	Contact	Office Phone (228) 81x-xxxx	E-mail
NSSC Chief Information Officer (CIO)			
NSSC Deputy CIO			
IT Security Officer (CS)			
IT DR Coordinator (CS)			
IT Manager (SP)			
Service Transition Manager (SP)			
Service Operations Manager (SP)			
Service Design/Engineering Mgr (SP)			
Service Strategy Manager (SP) [Acting]			
ESD Service Operations Manager (CS)			
ACES (Primary)			
NICS (Primary)			
NICS (Secondary)			

Table 1-1 – IT Management Team Contacts (REDACTED)

1.1 Plan Distribution

Key management personnel have been provided copies of the Plan. As needed, additional copies will be provided via thumb-drive when directed by the Senior Leadership Team (SLT) or by the NSSC Chief Information Officer (CIO)/Deputy CIO.

1.2 Recordkeeping

For record purposes, any time the NSSC's BCP is activated for annual testing or in case of an actual situation, all events and actions will be recorded in Appendix B – Activity Log with relevance to the IT division. The first entry will always be initial notification by one of the individuals identified in Table 1-1 while the final entry will always be official notification to resume normal business operations at the NSSC.

During the event, handwritten records may be kept. However, when the NSSC has been restored to regular business operations, the handwritten event records will be transcribed into the Activity Log template and saved within Appendix K – NSSC IT Division Disaster Recovery Records.

1.3 Maintaining the Plan

All questions, comments, or change requests will be submitted to the NSSC CIO identified in Table 1-1.

2.0 PURPOSE

The purpose of the IT BCP is to establish the approach for recovering from a data processing installation disaster. The most important function of this Plan is the need for continual review and updates as we encounter new situations and learn new solutions.

2.1 Responsibilities of Key Personnel

a) The Director of the John C. Stennis Space Center (SSC) exercises the authority for closing the SSC. In the event that the SSC is closed for normal operations, the NSSC Executive Director will be responsible for closing the NSSC.

b) The NSSC Executive Director has the overall responsibility for planning and ensuring that the NSSC is capable of carrying out the BCP Procedural Requirements.

c) The BC Program Manager is responsible for the activation and coordination of all BCP activities.

d) The Emergency Relocation Group (ERG) consists of personnel who are well-versed in the operation of identified NSSC functions. They are responsible to the NSSC Executive Director for the coordination, planning, and execution of the requirements outlined within the respective BCP each of the NSSC's functional areas. They also serve to share their expertise on BC planning; participate in test, training, and exercise (TT&E) events. The NSSC Executive Director, with the recommendation of the SLT, can direct the entire ERG or selected individuals to report to the Alternate Work Site (AWS) upon BCP activation.

e) Non-ERG personnel provide input on the execution of essential functions, assist in identifying and backing up vital records, and familiarize themselves with the SSC's Emergency Preparedness Plan (SPLN-1040-003) and NSSC's BCP.

2.2 Scope and Applicability

The Plan is applicable to all NSSC personnel maintaining any applications/systems within the NSSC. The recovery strategy for a business interruption/disaster is dependent upon the systems and facilities that have been damaged or lost. Actions to be implemented immediately following the event include the possible establishment and maintenance of computing operations at a backup facility. If the outage is long term, lasting more than four weeks, these procedures will provide for establishment of an alternate computing facility (Cold Site) at Marshall Space Flight Center (MSFC) in Alabama. The NSSC CIO has the primary responsibility for preparation and maintenance of this Plan. However, implementation of the Plan can only be authorized by the SLT which is described in Section 2.4.

For an extended disaster, the NSSC has an agreement with MSFC to provide 1,000 square feet of floor space for a Cold Site facility. Additionally, the NSSC is developing a plan for the procurement and installation of equipment and services to support the Cold Site at MSFC. NSSC expects to use this redundant IT computing capability as a part of its development/staging/production environment when it is not being used for disaster recovery plan (DRP) processing.

2.3 Overview

IT business continuity represents a broad scope of activities designed to sustain and recover critical IT services following a disaster or emergency. The NSSC BCP (NSBCP-1040-0001) is one of a suite of plans used by NSSC's leadership to support overall contingency planning.

Figure 2-1 – Disaster Recovery and Continuity of Operations provides a graphical depiction of the three main functions. They are:

- Protection
- Sustainability
- Recovery / Resumption of Operations

The foundations of this Plan are preparation and planning of strategic direction. Key members of each team are identified in Appendix C – NSSC Disaster Recovery (DR) Team Contacts List. In subsequent sections of this document, the team roles, responsibilities, and processes are defined. The main function of each team is to develop and coordinate the recovery plan for each individual business unit. Procedures are developed and reviewed by each team for the actions to be performed in a disaster situation. Annual testing verifies the accuracy of these procedures. Vital records and materials that must be available to meet the recovery objective are maintained and stored at an offsite repository. The contents of this repository are described in Appendix D – Offsite Vault Storage.

The Risk Assessment summary of threats categorizes severe weather, tornadoes, hurricanes, tropical storms, generalized flooding, liquid leakage, earthquake, bomb threats, fire, foundation and settlement problems, power instability, unauthorized user access, local distribution and cable plant, equipment/software failure, loss of key staff, strike/negative employee job action, and medical emergency as low risks. The preliminary Risk Assessment recommends that a DR Plan should be in place since there is a potential for disaster from these risk factors.

Figure 2-1 – Disaster Recovery and Continuity of Operations

The Escalation/Notification Procedures for NSSC operational problems describe the actions NSSC personnel follow for long-term outages. Many DR team members are the primary contacts in this procedure. The NSSC IT Management Team, using information from the national news networks and the SSC Emergency Operations Center, will alert the IT DR Coordinator who will in turn alerts members of the DR team of the potential for a disaster or that a disaster has occurred. A call tree process will alert the remaining IT DR group and provide the necessary information for activating the appropriate Cold Site services.

2.4 Senior Leadership Team (SLT)

Quoting from the NSSC BCP (NSBCP-1040-0001), "*The SLT addresses response and recovery support that will be provided at the time of disaster. During the recovery effort, the SLT provides direction and support to all affected functional areas. This is a centralized approach to ensure that recovery requirements for functional areas are met while eliminating confusion and duplication of effort. Affected functional areas will perform recovery activities based on their pre-determined strategies documented within their individual functional area BCP.*

"This concept allows for effective and timely management of the BCP activities, regardless of the magnitude of the event. A disaster is defined as any business interruption which results in the loss of a crucial information technology service, loss of access to the facility or loss of the facility." The BCP organization is depicted in Figure 2-2 – NSSC Senior Leadership Team.

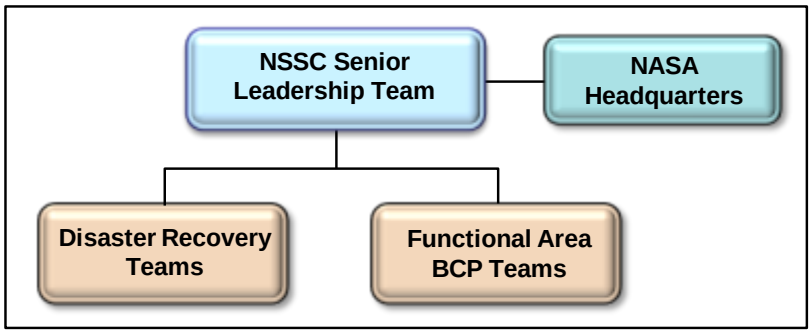

Figure 2-2 – NSSC Senior Leadership Team

2.5 Disaster/Emergency Assumptions

As soon as any data processing outage is known and a declaration is made by the NSSC Executive Director and SLT, processing would be shifted to a recovery site.

The Plan has been developed for use if some/all processing equipment supporting the NSSC has been completely destroyed or rendered inoperable and assumes the following:

a) Normally available staff members, both CS and SP employees, may be rendered unavailable by the disaster or its aftermath. Plans cannot depend on any single individual or expert being available. The Plan's documentation must be thorough enough to ensure backup (secondary) individuals can perform key tasks.

b) The Plan is not all-inclusive. Decisions regarding situations not expressly contained within this Plan, under specific control of the NSSC, are the privilege of the IT Management Team.

c) The recovery effort addressed by this Plan is limited to the service provided by the facility. It does not address the backup or recovery of associated user functions or personal computer-related programs/data. Personal computer-related programs/data are a responsibility of the End User Service Office (EUSO).

d) At the time of a disaster or emergency, the SLT of the NSSC and related SP management will handle organization-wide crisis management issues. This committee is beyond the scope of this Plan and the responsibilities handled by this committee include the following:

   1. Management of critical, ongoing functions;
   2. Personal safety.

This Plan seeks to minimize:

a) The dependence on participation of any specific person or group of people in the recovery process. Important information must be documented in this Plan, not in the mind of an individual who might not be available.

b) The need to develop, test/debug new procedures, programs, or systems during recovery. All required information should be in this Plan.

c) The adverse impact of lost data through a conscientious program of backups and testing, though recognizing the loss of some transactions is inevitable.

2.6 Crisis Identification Levels and SLT Activation (REDACTED)

The following are immediate actions for the BCP Director once notified of the incident:

- Address immediate life safety issues, if necessary;

- Record all pertinent information;
- Assess the incident based on information from the first responder; and
- Determine the appropriate Level to classify the incident. Specific instances are included within the NASA Shared Services Center Service Recovery Plan (NSPLN-1280-0002). (Double-click this link to access the document (REDACTED)).

3.0 AUTHORITY

The decision to declare a disaster is made by the NSSC Executive Director or designated alternate as outlined in Appendix E – Disaster Declaration Authorization Personnel.

3.1 Disaster Recovery Workflow Process

When a disaster is declared, the IT Management Team invokes the process to inform customers and the Cold Site.

3.2 IT Disaster Recovery Team

Notification of IT DR Team personnel is of paramount importance when an emergency or disaster is at hand. Appendix C – NSSC DR Team Contacts List identifies the members of the IT Division who would be contacted.

3.3 Cold Site Contingency (REDACTED)

With the utilization of the Cold Site, senior management can take time to appraise the disaster situation and decide upon the duration for the Cold Site.

Recovery Time Objectives (RTO) for each NSSC department are identified in Table 1-1 of the NSSC Business Continuity Plan (BCP) (NSBCP-1040-0001). (Double-click the link to access this document (REDACTED)).

3.4 Approach

Only limited NSSC functions are identified as having major impact to the daily operation of NASA. These identified functions will be performed by the NSSC ERG from within an office environment established at the MSFC. For IT operations, the NSSC intends to utilize a strategy where initial business continuity recovery begins from another NASA or federal recovery site to establish computer operation support for the ERG relocated to the AWS.

This recovery strategy is invoked if the NSSC BCP is activated due to the loss or damage of systems and/or facilities. If it is determined that the NSSC Data Center (which is now permanently in place at the National Center for Critical Information Processing and Storage (NCCIPS) facility at Stennis Space Center, MS) cannot be restored within six weeks the NSSC Executive Director will activate the requirement for the MSFC Cold Site. Additional information for NCCIPS is provided in Appendix F. The utilization of the Cold Site resources would be limited to that which is necessary to restore the services lost due to the unplanned business interruption.

Upon activation of the BCP by the NSSC Executive Director, the MSFC Facilities Management Office will provide onsite space for the AWS, if available, or coordinate procurement of off-site space with the NSSC that will provide continuity of operations and essential function recovery capability at the MSFC.

3.5 Cold Site Activation

Upon activation of the Cold Site, the IT Department's tapes, listings, manuals, and DR documentation will be retrieved from the storage facility. The most current set of monthly backup tapes are transported by SSC personnel to the NSSC's Enterprise Service Desk (ESD) Annex at Marshall Space Flight Center in Huntsville, AL (Building 4269, Room 108). Conversely, after delivery of the current tapes, the on-site tapes from the Annex are returned to the NSSC for reuse. Designated personnel will be deployed upon direction by the NSSC Executive Director via the SLT. This group will configure, restore the systems and provide ERG support. The production systems are available within 72 hours after the DR team reaches the site. If the decision that the processing cannot return to the NSSC within six weeks is made, the NSSC Executive Director will meet with the SLT and a long-term plan will be derived.

Other possible impacts to the NSSC include a Space Station disaster. From historical experience, in the event of a disaster, NASA management may require temporary suspension of part or all of the NSSC systems. The systems may experience an increased workload; however, DR should not be necessary.

4.0 IT MANAGEMENT TEAM PROCEDURES

The IT Management Team, in coordination with the NSSC BCP Program Manager, is responsible for deciding the course of action and for coordination of all activities during the DR process. Appendix C – NSSC DR Team Contacts List identifies key participants on this team.

4.1 Contacting Vendor and Hardware Maintenance Organizations

Appendix G – IT Vendor Contacts and Hardware Maintenance Organizations identifies the data recovery/salvage companies, and hardware maintenance organizations whose services/ capabilities might be required in the event of a disaster declaration.

5.0 TELECOMMUNICATIONS AND INTEROPERABLE COMMUNICATIONS

5.1 Purpose

The purpose of this section is to provide information for establishing the Transmission Control Protocol/Internet Protocol (TCP/IP) at the test site.

5.2 TCP/IP Traffic Recovery

The TCP/IP traffic uses Integrated Services Digital Network (ISDN) dialed circuits as the transport system. The TCP/IP network domain uses Cisco routers as the core backbone router of NASA Information Services Network (NISN). Border Gateway Protocol (BGP) is used to update the routing table. The NASA remote sites, through their own Local Area Network (LAN) segments, are linked to the NSSC host via mesh Cisco router connections. At the MSFC host site, each logical partition interfaces with the TCP/IP domain via dual LAN segments, dual Cisco 7200 routers for further filtering.

5.3 TCP/IP Arrangement for Disaster Recover Tests (REDACTED)

The IP path and routing are through the Premium Internet Protocol (PIP) domain to the Goddard Space Flight Center (GSFC) Cisco core router. From this core router, the path goes through an ISDN circuit to the selected site. This is a dial-on demand, 24-channel multiplexer card. The dial sequence is initiated upon reception of the first packet destined for the selected site. Filtering will be necessary at GSFC so as not to allow any other users to initiate the ISDN linkage aside from appropriate accepted IP originators. At the same time, the interfacing router at MSFC will have to do 'firewall' filtering such that except for these valid IP originators, others will not be allowed to enter into an IP session with the test proceedings at the site. This arrangement will be coordinated with the Consolidated Corporate Network Operations Center (CNOC). NSSC DR Planner, REDACTED, will supply the IP addresses allowed in the DR tests at the MSFC site.

5.4 Detailed Instructions to Establish TCP/IP Connectivity

IP traffic normally traverses the NISN until it reaches its destination. In the event of a disaster, the IP traffic will continue to use NISN; however, the traffic will re-route to the router at GSFC and then use a multiplexed ISDN line to selected site.

To complete the TCP/IP connections, it is the responsibility of the CNOC to program the “front-end” of the routers at the site.

A CNOC person can then dial in and program the router with the applicable information.

5.5 Interoperable Communications Requirements

This section will identify the required interoperable communications systems in place at the NSSC. The following communication system requirements are necessary to support emergency/contingency operations. Additional communication systems were evaluated to satisfy these requirements. Table 5-1 – NSSC Interoperable Communications Requirements identifies the requirements for the NSSC pertaining only to the IT infrastructure.

Communication Capability	Number Required for Emergency Operations	Number Required for Daily Operations	Additional Information
Landline Communications			
Non Secure Voice	25	500	
Non Secure Data	0	1	Modem line to Treasury
Non Secure FAX	1	8	
Non Secure Hardware	0	1	V.34 Data/FAX Modem
Secure Voice	0	0	
Secure Data	0	0	
Secure FAX	0	0	
Wide Area Network (WAN)	25	580	
Local Area Network (LAN)	25	580	
Radio Communications			
High Frequency (HF) Radio	0	0	
Wireless Communications			
Cellular Telephones	25	85	
Wireless Handheld Devices	25	85	
Wireless LAN	0	0	
Satellite Telephones	0	0	
Storage			
Classified Storage Containers	0	0	
Sensitive But Unclassified Storage Containers	1	6	

Table 5-1 – NSSC Interoperable Communications Requirements

5.6 Mission Critical Equipment

At present, the equipment identified in Table 5-2 – Mission Essential Equipment is on-line and operational, but houses legacy system data that will eventually be retired to a permanent-storage source.

Description of Mission Critical Equipment	Unique / One-of-a-Kind Equipment? Y/N	Available at Alternate Facility? Y/N	Current Location / Building
Astor-Intecom Automatic Call Distribution (ACD) for the Customer Contact Center (CCC)	Y	N	1201

Table 5-2 – Mission Essential Equipment

6.0 NSSC SYSTEM RESTORATION PRIORITY

As previously stated, a DR Meeting will be held in which the scope of the potential disaster/ emergency will be examined. As a result, restoration priorities will be assigned by the NSSC CIO as to which systems will be made operational if having to move off site. Table 6-1 – NSSC Business Unit Applications provides a listing of the current business applications at the NSSC for which restoration could be made.

Rebuild Priority (1-5) [5 is most important and is restored first]	Application Title	Function / Purpose
	ACaRT	Agency Cash Reconciliation Tool
	ACI	Agency Calendar Initiative
	Auto TechDoc	A Window's Service that automates the process of uploading electronic files to TechDoc. Electronic files are loaded into TechDoc by simply dragging and dropping files using windows explorer.
	Avamar	Backup Exec of Servers.
	AWMS	Accounts Payable Work Management System
	DrugPak	Drug and Controlled Substance Administration (formerly known as Assistant Pro)
	EPTS	NASA's Ethics Program and Tracking System
	ESD	Enterprise Service Desk

Rebuild Priority (1-5) [5 is most important and is restored first]	**Application Title**	**Function / Purpose**
	FCaRT	A funds check and reconciliation tool within the ESD Portal.
	Grants	Application procedures for NASA Research Announcements, Cooperative Agreement Notices, and Announcements of Opportunity.
	Inquisite	Survey/Sampling Tool
	KOFAX	Document imaging, design, and storage
	MICS	Computer Science Corporation (CSC) Metrics and Management
	NAAS	NASA Awards
	NEPS/NOPS	**NEPS** is a tool for NASA employees to view their personal data from FPPS. **NOPS** is a supervisory tool for data collection and statistical comparison to other NASA Centers.
	NetIQ	Server Monitor tool
	NRD	NASA Records Database
	OrgPublisher (OrgPub)	A COTS product showing organizational charts.
	Patchlink	Virus Protection Patch Tool
	Pay.gov Integration	An interface between the NSSC Customer Service Portal and pay.gov (related to Accounts Receivable
	Remedy	Case Tracking
	RightFAX	FAX Server
	RightNow Integration	Integration with third-party software as a service provided by RightNow Technologies.
	SATERN Training Purchases Process	A tool for processing SATERN-generated reports and creating NSRs for training purchases.
	Serena Dimensions™	A Configuration Management Tool (transitioned to TFS)

Rebuild Priority (1-5) [5 is most important and is restored first]	**Application Title**	**Function / Purpose**
	TechDoc	Electronic Document Management
	Test Tracker	Part of the NSSC Customer Service Portal used to record test cases and results.
	TFS	Team Foundation Server [Configuration Management]
	Training Purchases Status	A Web site providing the status of training purchases.
	Web Sites (applications)	Customer Information Sources

Table 6-1 – NSSC Business Unit Applications

Appendix H – NSSC Server Applications and System Software delivers a comprehensive breakdown of all Business Applications by individual server for the following environments and databases. The NSSC CIO will review the appendix during the DR Meeting to determine those systems and applications to be identified for restoration.

6.1 NSSC System Administrators (SYSADM)

6.1.1 System Administrators (REDACTED)

Following the DR Meeting, members of the SYSADM Team will identify specific technical needs based upon the NSSC CIO's restoration decisions. In order to fully identify the hardware and software assets required for restoration, the current NSSC Server Rack Layout is provided. For a visual depiction of the NSSC's hardware, and current NCCIPS location, double-click the link below.

(REDACTED)

As stated previously, the NSSC's Data Center was relocated on April 28, 2012 to the NCCIPS facility here at Stennis. To access the hardware location and identification information, click the link below to view the latest MS Visio functional diagram.

(REDACTED)

After viewing the drawing, click the "**X**" in the upper right-hand corner to exit and return to this document.

6.1.2 Desktop Support

In the event of a major disaster for which the NSSC's primary facility will be unavailable for a prolonged or unspecified period, Desktop Configurations will be provided by the ACES point of contact found in Table 1-1.

7.0 DISASTER RECOVERY PRODUCTION GOALS FOR THE IT DIVISION

7.1 Primary Responsibility

The NSSC's primary responsibility is to recover the Production [Environment] Operating Systems and Communications Network that comprise the programmatic/administrative framework of the NSSC.

There are contributing factors that must be taken into account when determining the priority with which specific systems/applications will be restored. Some of these factors are:

- How long do we anticipate the NSSC to be out of commission?
- Following an initial damage assessment, will the NSSC remain closed due to safety/health issues?
- If the facility is partially usable, which applications can continue without jeopardizing the safety of the personnel onboard and the associated hardware to run the applications? (This is especially important if having to run from generator power instead of regular power.)
- Which personnel should remain onsite to operate them?
- If subsequently the facility becomes unsafe for operations, how will we shift operation of these systems to the off site location?
- Understanding that some of our financial applications are driven by actual dates within the month, any priorities assigned must have leeway to make certain we remain in full-compliance with any Federal mandates or other lawful regulation(s).
- The priority schedule will be agreed upon and signed off before personnel begin traveling off-site. This meeting must include members from the customer's staff and the IT SP team who will be traveling.

It should be noted that every plan and strategy enacted must be robust enough to respond to change or project-grown as circumstances dictate.

7.2 Function and Component Recovery

The functions/actions identified below will ensure the orderly restoration of the Production environment.

- Restore all telecommunications.
- Perform installation verification/testing which includes the following:
  - Equipment Function
  - Software
  - Operating System
  - Telecommunications
- Activate network
- Inventory all supplies and acquire any items (such as additional tapes) that will be required at the Cold Site.
- Recover in accordance with the recovery schedule.
- Coordinate the verification of applications and databases with users.
- At this point operations at the Cold Site should be in normal processing mode and report completed and forwarded to the NSSC Management Team.
- Store backup tapes in the identified offsite storage.

8.0 IT DIVISION VITAL RECORDS (REDACTED)

The IT Division Master Records Index (MRI)/Vital Records listing provides a listing of the current records and of any other Vital Records and can be viewed at:

(REDACTED)

9.0 RIDE-OUT CREW PURPOSE, COMPOSITION, AND RESPONSIBILITIES

9.1 Purpose

The purpose of the Ride-Out Crew is to provide continuity of service for the business units and applications supported by the NSSC. During the meetings that would precede an impending disaster or known emergency, if it is determined that the best course of action would be to close down the NSSC to normal business routine and bring in a Ride-Out Crew, the individuals identified by the IT SP Manager or a designated alternate would be contacted, called in, and remain onboard. The NSSC has its own diesel-generator to provide uninterrupted power to critical systems during the ride out period. The members of the Ride-Out Crew would be authorized to bring their families to the NSSC, but must ensure they bring enough food for themselves/their family members to cover a 72-hour period.

9.2 Composition (REDACTED)

Table 9-1 – IT Ride-Out Crew Composition identifies the minimum Ride-Out Crew requirements.

IT Function	Individuals
CIO / Chief, Information Technology Division	
DCIO	
Management	
Security	
System Administration	
Database Administration	
Web Development	
Others	

Table 9-1 – IT Ride-Out Crew Composition (REDACTED)

Contact information for the above individuals is maintained separately and is considered private information.

9.3 Responsibilities

Under the guidance of the IT SP Manager or designated representative, all members of the Ride-Out Crew will continually evaluate the status of all servers and networks and immediately notify the IT SP Manager if any problems or situations arise. Written records of all events/actions undertaken by each Ride-Out Crew member will be maintained and collected when the disaster/emergency has passed and the NSSC is restored to normal operations. Please refer to Appendix I – Ride-Out Crew Responsibilities and Requirements.

9.3.1 Family Members

If authorized family members are brought onboard the NSSC with the Ride-Out Crew member, it will be the responsibility of the NSSC member to fully-explain to their family members the information contained in Appendix I – Ride-Out Crew Responsibilities and Requirements. In addition, all family members must be logged in using Appendix J – Ride-Out Family Register upon arrival. When the emergency/disaster has passed, onboard family members will be permitted to depart the NSSC after being logged out of the Register.

APPENDICES

Appendix A – Acronyms and Abbreviations

Acronym	Description
ACaRT	Agency Cash Reconciliation Tool
ACD	Automatic Call Distribution
ACES	Agency Consolidated End-user Services
ACI	Agency Calendar Initiative
AWS	Alternate Work Site
AWMS	Accounts Payable Work Management System
BC	Business Continuity
BCP	Business Continuity Plan
BGP	Border Gateway Protocol
BRP	Business Recovery Plan
CCC	Customer Contact Center
CIO	Chief Information Officer
CNOC	Consolidated Corporate Network Operations Center
COOP	Continuity of Operations
COTS	Commercial-Off-The-Shelf
CS	Customer-Staff, Civil Service (NASA employee)
CSC	Computer Sciences Corporation
DR	Disaster Recovery
DRP	Disaster Recovery Plan
DSRC	Defense Super-Computer Resource Center
EPTS	Ethics Program Tracking System [NASA]
ERG	Emergency Relocation Group
ESD	Enterprise Service Desk
EUSO	End Users Service Office
FAX	Facsimile (machine)
FCaRT	Funds Check and Reconciliation Tool
FedEx®	Federal Express (shipping & delivery service)
GSFC	Goddard Space Flight Center
HF	High Frequency
HIPAA	Health Insurance Portability and Accountability Act
IBM	International Business Machines

Acronym	Description
IP	Internet Protocol
ISDN	Integrated Services Digital Network
I3P	IT Infrastructure Integration Program
IT	Information Technology
KOFAX	The NSSC's Document Imaging, Design, and Storage System
KSC	John F. Kennedy Space Center
LAN	Local Area Network
MICS	Management Information and Control System
MRI	Master Records Index
MSFC	George C. Marshall Space Flight Center
NAAS	NASA Automated Awards System
NASA	National Aeronautics and Space Administration
NBU	Net Backup
NCCIPS	National Center for Critical Information Processing and Storage
NEPS	NASA Employee Profile System
NICS	NASA Integrated Communications Services
NISN	NASA Information Services Network
NOPS	NASA Organizational Profile System
NRD	NASA Records Database
NSSC	NASA Shared Services Center
OEP	Occupant Emergency Plan
OrgPub	Organization Publisher (a COTS product showing organizational charts)
QTY	Quantity
PIP	Premium Internet Protocol
POP	Point(s) of Presence
Rep.	Representative
RTO	Recovery Time Objective
SATERN	System for Administration, Training, and Educational Resources for NASA
SFTP	Secure File Transfer Protocol
SLT	Senior Leadership Team
SP	Service Provider (syn. Contractor)
SSC	John C. Stennis Space Center
SYSADM	System Administrator(s)
TCP/IP	Transmission Control Protocol/Internet Protocol

Acronym	Description
TechDoc	NSSC's Electronic Document System
TFS	Team Foundation Server
TT&E	Test, Training, and Exercise
VolSer	Volume/Serial
WAN	Wide Area Network

Appendix B – Activity Log (REDACTED)

The Activity Log serves as the official record of all activities associated with the DR Plan activation. Though only a template for illustrative purposes, hand-written notes will be maintained and can be placed upon this template when circumstances permit.

(When the situation has ended, all activities will be typed and linked within Appendix L for reference purposes.)

Event Date:	**6/2/2014**	**NSSC IT Disaster Recovery Plan Activity Log**
TIME OF EVENT	**REPORTED BY**	**ACTIVITY/EVENT DESCRIPTION**
3:00 pm	Charlene Thames	Received phone notification from REDACTED that the SSC has been placed under Hurricane Condition IV. Each DR Team member is to be contacted – no other actions are assigned at this time.
FOR ILLUSTRATION ONLY		

Page __ of __

Appendix C – NSSC DR Team Contacts List (REDACTED)

Name	Title	Office (228) 81-xxxx)/After Hours Phones
IT Management Team		
	NSSC CIO, IT Services Division Chief (CS) (Acting)	
	IT DR Coordinator (CS)	
	IT Manager (SP)	
IT Facilities Team		
	Safety & Security Manager (CS)	
DR Team		
	Lead System Administrator (CS)	
	NSSC IT Security Manager (CS)	
	Lead Database Administrator (SP)	
	Remedy Lead (SP)	
	Remedy Developer (SP)	
	Service Operations Manager (SP)	
	Service Transition Manager (SP)	
	System Administrator (SP)	
	Network Security Administrator (SP)	
	Manager, Service Design/Engineering (SP)	
	[Ride-Out] Web Developer (SP)	
ACES / NICS Representatives		
Please refer to Table 1-1		

Appendix D – Offsite Vault Storage

Item Description	Binder Location
NSSC Server Listing and Components; NSSC Server OS Information	Tab A
NSSC Hardware Listing	Tab B
NSSC Desktop Software Listing; NSSC Software Renewal Listing	Tab C
Two copies of the IT BCP	Tab D (on DVD)
Copies of all Lessons Learned stored electronically and placed in the Vault not later than two weeks following test completion	Tab D (on DVD)
Weekly back-up tapes and previous three months monthly back-up tapes	SSC Bldg 1100
Most recent set of monthly back-up tapes	MSFC Bldg 4629

The following personnel/teams have access to the offsite vault storage:

- NSSC IT SP Systems Administrators
- NSSC IT SP Database Administrators
- NSSC IT SP Manager
- NSSC IT DR Coordinator (CS)
- NSSC IT Support Specialist (CS)

The contents of the storage vault will be inventoried annually in consonance with the annual review of this Plan. It is imperative that the most up-to-date documentation is present at all times.

Per the NSSC DCIO, the System Administration team maintains backup tapes for:

- 14 days for backup (if recovery is necessary)
- 3 weeks (retention)
- 4 prior months

Appendix E – Disaster Declaration Authorization Personnel

The individuals listed below, as reported in the NSSC BCP (NSBCP-1040-0001) in order of precedence, are authorized to declare a disaster of the NSSC:

Position	Successor	Program Responsibility	Condition
Executive Director	Deputy Director	Full	All emergencies
Deputy Director	Director, Business & Administration	Full	If requested by the Deputy, Executive Director or in the absence of the Deputy Director
Director, Service Delivery	Service Delivery Deputy Director	Full	If requested by Director, Service Delivery or in the absence of the Director

Under normal circumstances, the SLT would convene to review the situation and make a recommendation to the Executive Director.

Appendix F – National Center for Critical Information Processing and Storage (NCCIPS)

NCCIPS is designed as a national shared-service data facility whose current Federal customers are the Department of Homeland Security, the Navy's Defense Super-Computing Resource Center (DSRC), and the Department of Transportation.

NCCIPS provides a secure data processing and storage facility on Government property with in-depth, layered security. The NCCIPS facility is currently Tier 2+ (aligned with Uptime Institute) with funding and projects underway to create a Tier 3+ facility.

The facility will have three independent, high-capacity power feeds and two Points of Presence (POP) available for routing high-bandwidth circuits. The NCCIPS facility is appropriate for sensitive and secure applications and has space available for NASA use. Some of the available space is built out in a 30-inch raised floor, but much of the space is configurable, raw square footage.

The NSSC relocated all data center hardware to NCCIPS in April 2012 in order to afford uninterrupted network connectivity and server preservations during major natural disasters that might affect the NSSC.

Appendix G – IT Vendor Contacts and Hardware Maintenance Organizations (REDACTED)

NSSC IT VENDOR CONTACTS

Oracle America, Inc.

TechDoc

Kofax

Remedy

Contacts for Hardware Maintenance Organizations (REDACTED)

Service Provider	National Telephone	Local (L) / Home (H) / Cell (C) / FAX (F)
Dell	**800-274-3355**	**http://www.dell.com/**
IBM	**800-426-7378**	**http://www.ibm.com/us/**
Oracle	**800-525-0369**	**http://www.oracle.com**

Service Provider	National Telephone	Local (L) / Home (H) / Cell (C) / FAX (F)

Appendix H – NSSC Server Applications and System Software

The current NSSC System Architecture is portrayed in a MS Visio illustration that can be viewed by clicking the icon below.

REDACTED

Appendix I – Ride-Out Crew Responsibilities and Requirements

If Ride-Out Crew personnel wish to bring their families along, the following must be made known to each employee well in advance of arrival:

- Employees must provide mattresses, bedding, essential diet/medication items, and basic hygiene items. This includes a 3-day supply of food and ice chests.
- Pets are not allowed inside the NSSC, other than Service Working Dogs.
- Each employee and family member is required to register upon arrival (see Appendix J).
- All personnel must remain inside the NSSC once they've registered.
- Family members will not be allowed to wander throughout the NSSC. The IT SP Manager will accommodate family members as much as possible to maintain privacy by keeping them together.
- Items such battery powered radio, televisions and hand-held games are authorized as long as they do not disturb others.
- Family members **are not authorized** to use any NSSC computers, peripherals or other equipment.
- Smoking or the use of tobacco products is **prohibited** within the NSSC.
- Any individuals whose medical condition(s) could require medical intervention or evacuation should not be brought onboard because there is no guarantee the SSC's Emergency Operations Department would be able to dispatch emergency medical personnel if called upon.

Appendix J – Ride-Out Family Register

Ride-Out Crew Family Register

Date: _____ Storm Name / Emergency: _____

Name of Family Member	Employee Last Name	Arrival Date/Time	Departure Date/Time	Relation to Employee	Age	Sex	Medical Conditions **
		I	I				☐ NO ☐ YES
		I	I				☐ NO ☐ YES
		I	I				☐ NO ☐ YES
		I	I				☐ NO ☐ YES
		I	I				☐ NO ☐ YES

** For reasons of personal privacy and HIPAA regulation, CHECK ONLY "YES" or "NO in this block. If there is a condition/situation the IT (SP) Manager should be aware of, please make personal notification upon arrival and NOT by electronic means.

Appendix K – IT Division Disaster Recovery Records

Activity logs, prepared per Appendix B, will be collected following the restoration of normal services at the NSSC. All documents will be formally typewritten and appended via hyperlink within this Appendix to document the events and actions directed by the SLT.