National Aeronautics and
Space Administration

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

NASA Shared Services Center Work Instruction

NSWI-2810-0001 Revision 2.0

Effective Date: June 27, 2012
Expiration Date: June 27, 2017

NSSC IT Security Policies

Responsible Office: Information Technology Division

Approved by

/s/ Bruce O'Dell
Bruce O'Dell
NSSC, Chief Information Officer

August 2, 2012
Date

DOCUMENT HISTORY LOG

Status (Basic/Revision/Cancelled)	Document Version	Effective Date	Description of Change
Basic	1.0	01/03/2011	Initial release of IT Security Policies
Revision	2.0	06/27/2012	Insert Appendices O, P, Q, R, & S.

TABLE OF CONTENTS

PREFACE

P.1 Purpose

The concept of this IT Security Work Instruction is to provide a convenient collection of policy and guidance for the use of IT resources to ensure that identified essential information security levels are maintained.

P.2 Applicability

a. The provisions of this Manual apply to all NSSC NASA personnel and NSSC support service contractors.

P.3 Authority

NPR 2810.1a, §2.2.10.2b:
The Center ITSM shall develop Center-wide IT security policies and guidance for approval by the Center CIO.

P.4 Applicable Documents and References

All references are assumed to be the latest version unless otherwise specified.

a. Computer Security Act of 1987

b. NPD 2540.1g, Personal Use of Government Office Equipment Including Information Technology

c. NPR 1600.1 NASA Security Program Procedural Requirements

d. NPR 2810.1a, Security Information Technology

e. National Institute of Standards and Technology (NIST) Special Publications (SPs) 800 series

f. Federal Information Security Management Act (FISMA)

P.5 Measurement/Verification

Refer to NASA Online Action Tracking System (NOATS).

P.6 Cancellation

None

P.7 Distribution

Approved for release via NSSC's TechDoc Document Management System; distribution is limited.

INTRODUCTION

1.1 Policy

Agency regulations and requirements sometime leave gaps in specific areas of application that require treatment by additional position statements. The NASA Shared Services Center (NSSC) has identified Information Technology (IT) Security policies to address salient gaps and enhance safeguards to the confidentiality, integrity, and availability of the IT resources used by this center.

Positions stated in this document are to augment those of the agency where focus may be generic. Should agency-level policies emerge to address, and potentially conflict with, specific positions contained in this document, the agency position shall prevail.

1.2 Objective

The objective of the IT Security Work Instruction is to inform of the current IT policies and to achieve common approach of IT standards across a wide range of IT Security areas.

IT Security policies are established for:

a. Ensuring the Confidentiality, Integrity and Availability of NSSC and Agency IT resources;

b. Protecting NSSC and Agency facilities, equipment, records, and other assets; and

c. Providing organizational and operational stability.

1.3 Requirements

To accomplish these objectives, the NSSC IT Security team has drafted and compiled position statements for the guidance most frequently requested of it. Success of this effort requires management support and the awareness and compliance of all users of NSSC IT resources.

ROLES & RESPONSIBILITIES

2.1 Roles & Responsibilities

a. The **NSSC ITSM or Deputy ITSM** has the overall responsibility for implementing the NSSC IT Security Program. The Center ITSM's role is to develop Center-wide IT security policies and guidance, to coordinate and facilitate IT security awareness and training, to maintain an incident response capability, and to document, review, and report the status of the Center IT Security Program.

b. The **NSSC IT Security Team** maintains current knowledge and skills with information technologies and IT security and is comprised of NASA IT Security management, Service Provider IT Security management, and representatives from permanent IT support organizations (e.g. ACES, NICS). The team develops security standards, guidelines and procedures relative to the physical, personnel, data, communications, hardware, software and operational aspects of Information Technology systems. The team assists and collaborates with center functional areas. The team monitors and ensures the effectiveness of safeguards, and responds to incidents to contain, research, and resolve in a quick and thorough manner. The NSSC Incident Response Team (IRT) is a subset of the IT Security Team.

c. The **NSSC CIO** is responsible for establishing an effective and economical Center Information Resource Management (IRM) program. The IRM program plan defines the design and operation of the Center's information infrastructure (e.g., networks, servers, and electronic forms) and ensures alignment with the NASA IRM's vision, mission, and strategy. The Center IT security roles and responsibilities shall reside within the Center CIO office.

d. **All Employees** – It is incumbent upon all employees, as users and stewards of agency information technology resources, to recognize their potential impact on security, and to minimize risk that is associated with that potential.

e. **SOC** – The NASA Security Operations Center (SOC) is the entity for receiving convergence of IT incident reports, dispatching incident details to center response teams, and tracking incident resolution.

2.2 Delegations of Authority

Authority as specified in P.3 will not be delegated.

DEFINITIONS

3.1 Definitions

Agency Action Tracking System – NOATS (NASA Online Action Tracking System) is the agency application for issuing and tracking the closure of action-items originating within the office of the CIO.

Elevated Privileges – Logical rights of a user of information resources that are above the minimal and essential range of permission necessary for that user to perform his/her job.

IT Security Incident – A violation or imminent threat of violation of computer security policies, acceptable use policies, or a breakdown of security practices, which may adversely affect the confidentiality, availability, or integrity of agency information resources. Examples: Unauthorized access, malware, breached data, malfunction.

Network Access Control – A means to automatically assess the integrity of a computer before allowing a full data communication to be established.

NSSC Employees – NASA and Contractor personnel whose working affiliation is the NASA Shared Services Center

NSSC IT User – An NSSC employee who utilizes center IT resources. Since this includes anyone who uses a computer, telephone, or network connection, it essentially translates to all NSSC employees and, for access to NSSC internal networks, *only* NSSC employees.

Public Key Infrastructure (PKI) – NASA's Entrust-based file and email encryption method.

Sensitive But Unclassified (SBU) – Information that is of sensitive nature but does not contain national security information and, therefore, cannot be classified.

Social Media – Technologies that are applied for social interaction, also known as User-Generated Content and Consumer-Generated Media. In order for social media to be most successful it must be openly accessible, an attribute that is contrary to regulation and protection by convenient security controls. Common media are MySpace, Facebook, and Twitter.

Virtual Private Network – A method of securely extending a protected (e.g. Center Internal) network to validated remote users who must connect via otherwise unsecure means (e.g. Open Internet)

ACRONYMS

3.2 Acronyms

CCB	Configuration Control Board
CIO	Chief Information Officer
EP	Elevated Privileges
DITSM	Deputy Information Technology Security Manager
GFE	Government Furnished Equipment
IdMAX	Identity and Access Management
IMS	Incident Management System
IRM	Information Resource Management
IRT	Incident Response Team
IT	Information Technology
ITSM	Information Technology Security Manager
NAC	Network Access Control
NSSC	NASA Shared Services Center
PKI	Public Key Infrastructure
SBU	Sensitive But Unclassified
SOC	Security Operation Center
SSC	Stennis Space Center
VPN	Virtual Private Network

APPENDIX A. NSSC SOCIAL MEDIA, WEB MAIL, AND SKYPE

NSSC Social Media Policy

NSSC IT Security has determined, from incident histories and the general statistics of employees' network usage, that substantial risk exists to the center's information resources by open social media access. NSSC assumes a "default deny" posture to social media that is generally and publicly available while allowing access to NASA-maintained media. The NSSC "M86" web content controlling device will suppress access to regulated social media and webmail for those who have not received approval from their management or supervision.

Skype

The use of Skype's Business client is sanctioned for NSSC users who are authorized by supervision and file an appropriate [*NSSC Social Networking Access*] request. The Skype "consumer" client is only permitted in cases where there is not a Business client (eg. For Mac OS-X). The user is responsible for arranging for the installation of software and specific configuration settings must be in place. Elevated privileges or administrator assistance may be required.

Skype Configuration Standard
Devices which are authorized for Skype use are to only run legitimate Skype Business Version from Skype.com.
Authorized Skype users must create Skype passwords in compliance with NIST SP 800-53, Rev. 3 password strength requirements.

NOTES:

In the System Registry Modification section, the listed Registry Key values must be added to the existing Registry Key. Making incorrect changes to the Registry can render the system useless. Elevated privileges or administrator assistance may be required.

Skype software is not an end-user Tier-1 or Tier-2 item and will incur cost for ACES installation.

System Registry Modifications

Description	Setting
Disable File Transfer Feature	HKEY_LOCAL_MACHINE\Software\Skype\Phone\"DisableFileTransfer" = REG_DWORD:00000001

	HKEY_CURRENT_USER\Software\Skype\Phone\"DisableFileTransfer" = REG_DWORD:00000001
Disable Supernode Promotion	HKEY_LOCAL_MACHINE\Software\Skype\Phone\"DisableSupernode" = REG_DWORD:00000001 HKEY_CURRENT_USER\Software\Skype\Phone\"DisableSupernode" = REG_DWORD:00000001
Disable 3rd Party API Calls	HKEY_LOCAL_MACHINE\Software\Skype\Phone\"DisableApi" = REG_DWORD:00000001 HKEY_CURRENT_USER\Software\Skype\Phone\"DisableApi" = REG_DWORD:00000001

Skype Application Configuration

Description	Setting
Disable Skype AutoStart	Options -> General -> General Settings-> Uncheck "Start Skype when I start Windows"
Disable Automatic Video Sharing	Options -> General -> General Settings-> Video Settings -> Uncheck "Enable Skype Access"
Disable Commercial Skype WiFi Hotspot Access	Options -> General -> General Settings-> Skype Access -> Uncheck "Enable Skype Access"
Disable Receipt of Unsolicited Phone Calls	Options -> Privacy -> select "Allow calls from people in my contact list only"
Log Call History for as Long as Possible	Options ->Privacy -> Advanced Options-> select "Keep history for 2 weeks"
Skype Browser Cookies	Options -> Privacy -> Advanced Options-> Uncheck "Accept Skype browser cookies"
Disable Hyperlink Calling	Options -> Advanced -> Advanced Settings -> uncheck "Use Skype to call callto: links on the web"
Disable uPnP	Options -> Advanced -> Connection -> Uncheck "Enable uPnP"

APPENDIX B. NSSC IT WEBPAGE CONTENT FILTERING

There is content available from webpages on the internet that the NSSC has determined to be of detrimental nature or will consistently expose information resources to intolerable risk. The NSSC “M86” web content controlling device will suppress access to websites that fall within the below-listed categories, as defined by the device vendor. Occasionally, legitimate websites may find themselves in a blocked category and IT Security can expressly “whitelist” a website upon request bearing endorsement from management or supervision.

Categories are as named and defined by M86 Security.

Banner/Web Ads
Games
Free Hosts
ICQ & AIM
Yahoo IM
Fantasy Sports
Dating/Personals
Pornography/Adult Content
Spyware
Gambling
Phishing
Adware
Web-based Proxies/Anonymizers
Malicious Code/virus
Peer-to-Peer/File Sharing
Web Logs/Personal Pages
Web Based Email

APPENDIX C. NSSC PKI

The handling of sensitive information by IT users is frequent and commonplace within NSSC. In order to maintain control of sensitive (e.g. SBU) content, each NSSC IT user is required to have an account in the agency's public key infrastructure (PKI).

Requests for PKI are submitted using IdMAX. Since PKI requests are often submitted in conjunction with arrival of new employees, the NSSC ITSM and D/ITSM may be listed as sponsor for IdMAX requests if the supervisor or functional manager identity is not yet available.

APPENDIX D. NSSC INCIDENT HANDLING AND REPORTING

All IT Security incidents or suspected incidents shall be reported to the NASA Security Operations Center (SOC). Reports may be made to the NSSC Customer Contact Center or Enterprise Service Desk, whose response will then be to contact the SOC. The NSSC incident response team will receive notification of incident reports from SOC. If the incident involves either an ACES computer system or a lost or stolen mobile device, additional notification will be routed to appropriate technical staff.

Incidents that involve privacy information must also be communicated to the center Privacy Act Manager (PAM) and must be reported to the SOC within 1-hour of discovery by one able to file such a report.

Upon discovery of an incident, and if risk permits, affected equipment shall be left alone so that as much pertinent information can be gathered as possible. If apparent risk does not permit additional discovery, the system shall immediately be shut down by turning off the power (not a shutdown of the operating system). If a system poses a threat to the NSSC infrastructure, it must immediately be removed from the network.

All incidents at the NSSC will be addressed by the IRT who reports status to the ITSM.

The ITSM shall determine whether or not the incident involves criminal activity. Criminally-involved incidents are required to be reported to the NASA OIG.

The IRT shall seek to contain an incident within 24 hours.

Action shall be taken to return affected equipment to service as quickly as possible following the incident. ITSM approval is required for incident-related system wipe and load operations.

Complete details of the Incident Handling and Reporting guidelines are defined in NSSC Incident Reporting and Handling Procedure and NASA handbooks ITS-HBK-2810.09-01 and ITS-HBK-2810.09-02.

APPENDIX E. NSSC NETWORK CONTROLS

The interface between the NSSC's network and the agency's wide-area network (and the Internet) represents a constantly changing landscape. The NSSC adheres to a "default deny" policy regarding network traffic through its network security controls (e.g. firewall, IDS). Logical exceptions to that policy are made, and equipment configurations are periodically adjusted and updated, in order to permit necessary data flow.

The usual vehicle for carrying and documenting configurations shall be a change request to the CCB. Requests may, however, bypass CCB if supported by SOC directive or special circumstances at judgment of ITSM.

Upon the receipt of a request to modify a setting or rule, the IT Security Team will evaluate the risk and the technical feasibility of the request. Once the IT Security Team has initially approved the request, it is then sent to the ITSM for final approval. Simple requests are approved or denied by the ITSM. Otherwise, stakeholders meet with the CCB on the next scheduled meeting time. The CCB will review the request within five working days. Alternative methods may be suggested in order to best protect the health of the NSSC IT Resources.

If approved, the request will be forwarded, via PGP or Entrust encrypted e-mail, to the appropriate party (ref. below) for implementation. If rejected, the request with the reason for rejection will be returned to the requestor.

Approval and Implementation for NSSC Network Control Configurations:
(as/of ODIN-to-NICS transition completion)

Firewall:	NSSC approves	NICS implements
IDS:	NSSC approves	CSC implements
Network Access:	NSSC approves	NICS implements
Web Content Filtering:	NSSC approves	NICS Implements

Write privileges to equipment shall be exclusive to the implementing party.

APPENDIX F. NSSC GUEST WIRELESS ACCESS

NSSC permits transient access to internet resources through a guest wireless network. Users who avail of the guest network must provide nominal information to a captive portal, which captures an email address, a contact within the NSSC who is familiar with the user, and acknowledgement of the standard warning banner.

Since NSSC and Stennis Space Center (SSC) wireless territories overlap, The NSSC Guest Wireless network will be named *nasaguest* in accordance with NASA-STD-2850.2 but, to differentiate from SSC's guest wireless network, the captive portal page presented to users shall indicate that the NSSC network is being accessed. This must be done in order to facilitate troubleshooting and to assist users in making a reliable connection while within the NSSC property.

The NSSC Guest Wireless Network shall be passively monitored internally with Intrusion Detection tools. The NSSC Guest Wireless Network is also monitored externally by the SOC.

If the NSSC Incident Response Team (IRT) becomes aware of an incident on the NSSC Guest Wireless network, the team will isolate and attempt to locate the user. If reasonable attempts to locate the user fail, the team will take necessary actions to resolve the incident and protect the network.

APPENDIX G. NSSC REMOTE ACCESS

The NSSC provides information services on behalf of the agency, and maintains a high standard of care. Remote access to NSSC servers for maintenance and troubleshooting is reserved for the exclusive use of NSSC system administrators. Remote access to the NSSC network and agency campus via VPN is reserved for the exclusive use of resident NSSC employees.

Computers hosting the NSSC VPN client must be agency-provided, or “GFE”.

VPN for non-residents may be provided in accordance with a Memorandum of Agreement establishing functional area and non-resident entity. The MOA must include an external system security plan with authority to operate and prepared in accordance with agency assessment and authorization requirements wherever equipment (e.g. client hardware) will be used that is not provided by the agency (“non-GFE”). This security plan must indicate how risk to the agency by use of non-GFE, will be controlled to the satisfaction of the authorizing official. Non-resident access must be sponsored and requested by the NSSC functional representative and must be reviewed annually.

Access for remote maintenance is subject to NIST SP 800-53, Rev 3 security control MA-4 and must be approved by the ITSM. A request for access must be submitted to the NSSC IT Security Team for initial approval and must include the following information:

- Rationale why remote access is required by the vendor;
- Technical details of how the access will be used;
- Identities of those who will be using the access;
- The purpose (tasks performed) for gaining access; and
- Specific Date and Time access is needed.

All traffic will be logged and activity monitored by the NSSC IT Security Team. Each remote maintenance access request will cover one access event for the time specified.

Requests for VPN accounts are filed via IdMAX. VPN accounts also require use of an agency-issued RSA SecurilD token, also requested via IdMAX.

Users accessing the VPN system to gain remote access must have a recent patch level of the operating system and latest antivirus definitions. NAC or an equivalent technical control must be in place to ensure appropriate patch levels and antivirus definitions exist.

APPENDIX H. NSSC PHYSICAL ACCESS TO IT RESOURCES

Access to NSSC Building 1111 is controlled as a part of the agency's badging and access control system. Additionally, areas deeper within Building 1111 are subject to further control. All individuals seeking access to physically-controlled NSSC IT Resources such as the NSSC Data Center, Switch Rooms must submit an "SSC Physical Card Access" request in IdMAX .

APPENDIX I. NSSC IT APPROPRIATE USE OF IT RESOURCES

NASA document NPD2540.1g, “Personal Use of Government Office Equipment Including Information Technology”, shall be the foundation for determining appropriate use of NSSC IT resources.

APPENDIX J. NSSC ELEVATED PRIVILEGES

Background: NASA has implemented a managed approach for users requiring Elevated Privileges (EP) to perform their job functions. This reduces the risk of running or installing unauthorized applications and vulnerabilities being exploited by malware and malicious users.

NSSC follows handbook ITS-HBK-15-02a to implement the directives of NITR 2810-14a in regulating a computer user’s privilege level.

All Users requiring EP must take the appropriate training in SATERN and then submit an IdMAX request. This request must be sponsored by the user's supervisor or manager and is validated by IT Security prior being provisioned by end-user services.

Elevated privileges may be granted for a period not to exceed one year, renewable upon review of need and qualifications, or for a non-renewable 30-day period, once a year. As of 1 February, 2012, recurrent training is required for all renewals of EP.

NSSC does not grant administrator privileges for the day. For spontaneous need there is provision to call the end-user services helpdesk for an escorted warm hand-off to NSSC Technical Support for temporary elevation of user privileges.

APPENDIX K. NSSC DESKTOP AND SERVER PATCHING

NSSC minimizes vulnerabilities to its IT resources by ensuring that operational software is current.

NSSC Data Center

- All routine and critical/urgent patches to NSSC Data Center servers must be tested in a test and development environment before being released into a production environment. Once a patch is installed in test and development, it must be actively monitored by the system administrator for any system irregularities.

- Routine patches must be installed in within 7-9 calendar days from the date of release and do not require CCB approval prior to implementation.

- Critical/urgent patches or any patches that are outside of the typical patching schedule are to obtain CCB approval prior to implementation. Vendor Security patches shall be treated as critical/urgent.

- A risk assessment is to be conducted to determine the schedule for installation in the production environment.

Desktops

- End-user services desktop patching must be in compliance per delivery order.

APPENDIX L. NSSC VOICEMAIL DATA REQUEST

NSSC policy regarding requests for voicemail transcripts and call detail reports does not require treatment as targeted monitoring unless it is known that the product of the request requires chain-of-custody. Non-chain-of-custody requests shall be submitted on an SSC or NSSC IT Report Request form and have concurrence of physical security and IT security. Requests that require chain-of-custody shall follow the targeted monitoring process of ITS-HBK-09-03. Targeted monitoring requests, if originating within the center, may only be initiated by NSSC legal counsel, HR, or others specified in ITS-HBK-09-03.

APPENDIX M. ELECTRICAL CIRCUIT BREAKER OPERATION

In order to maintain a safe and organized approach to controlling the electrical power circuits in the NSSC Data Center, the following guidelines apply to the manipulation of circuit breakers in the distribution panels of Room 197.

Circuit breakers may be operated by System Administrators in order to isolate equipment from electrical power.

Circuit breakers that are observed to have tripped require attention to determine presence of an overload before attempting a reset, and reset may then be attempted no more than twice without success. Upon tripping a third time, the overload must be reported to the electrical contractor’s trouble desk and the NSSC facilities office.

Covers and panels which provide a barrier against the electrical hazards within an enclosure are not to be removed by NSSC personnel.

APPENDIX N. FIPS 140-2 USB MEMORY STICK DEVICES

Background: NASA has established encryption requirements for its information technology resources that store and process Sensitive But Unclassified (SBU) data. In accordance with NPR 2810.1, Security of Information Technology, "NASA management shall comply with NIST FIPS Publication 140-2, Security Requirements for Cryptographic Modules, FIPS Publication 46-3, Data Encryption Standard and NIST SP 800-77, Guide to IPSec VPNs."

In order to ensure the safeguarding of NASA Financial and Human Resource data that may be stored or processed, no NSSC personnel may store or process any data on a memory stick device that is not compliant with FIPS 140-2 encryption requirements. When obtaining memory stick devices, NSSC personnel must purchase memory stick devices that are FIPS 140-2 compliant and interoperable with computers (PC+Mac) found within the NSSC environment. Memory devices must encrypt their entire storage capacity.

APPENDIX O. VULNERABILITY NOTIFICATION, REMEDIATION, AND ELEVATION

Day Zero (0)
The systems are scanned and vulnerabilities are identified, remediation tickets are issued to the McAfee Vulnerability Manager (MVM) Remediation Managers. The Remediation Manager has three (3) calendar days to verify that the ticket issued is in his or her assigned area of responsibility or needs to be addressed by another Remediation Manager.

Day Three (3)
All remediation tickets must be reassigned if needed.

Day Thirty (30)
All tickets must be completed, verified, and closed.

Day Thirty-One (31)
When a vulnerability remediation ticket has exceeded 30 days from the creation date, a Plan of Action and Milestone (POA&M) item is created and reported to the Agency via the NSSC IT Security Manager (ITSM) with completion date not to exceed (15) fifteen days.

Day Forty-Five (45)
If resolution has not yet been accomplished, the vulnerability remediation ticket holder must show cause daily to the ITSM as to why the vulnerability still exists, and commence preparation for system isolation.

Day Sixty (60)
When a vulnerability remediation ticket has exceeded 60 days from the creation date, it is escalated to the NSSC ITSM with the request to remove the system from the network.

Remediation Managers are assigned to leads over specific areas of responsibilities.
It is the responsibility of the Remediation Manager to continue the remediation process while absent or on travel. The role may be delegated to an alternate member during times of absences that would interfere with meeting the performance of the process.

Performance metrics will be collected and reported to the NSSC ITSM and functional area management.

APPENDIX P. NSSC TRAINING ROOM

The computers in the NSSC training room will be attached to a network VLAN configured specifically to isolate them from all other NSSC assets. This VLAN will be connected to a separate interface on the NSSC firewall.

The default configuration for this VLAN will block access to all services except those required for the maintenance of the desktop computers in the training room. Required services includes patch management, anti-virus, log management, and systems administration.

Hard drive images for the standard load required for training computers will be maintained by the contractor responsible for the maintenance of the desktop computer.

After each training class has concluded, the training desktop computers will be wiped and the standard image load will be reapplied.

The training department will determine the needs for the connectivity requirements for any training classes, which may require a consultation with the group requesting use of the training assets as well as NSSC IT Security. If internal or agency network connectivity is required, it will be implemented as needed provided proper justification has been provided along with the connectivity requirements.

ACL requests must be submitted a minimum of 5 business days prior to required implementation.

For new NSSC employees who have not yet received their full NASA clearance and are not yet approved to operate NSSC computer assets, http and https connectivity will be provided only to NASA SATERN.

The concept of least privilege will be applied in regards to training computers access any NASA resources. This includes physical security, internal network resources and network file shares.

The training room manager will provide the daily schedule for any training activities which require a deviation from the default network configuration. Any access controls will be implemented with based on this schedule. This includes after hours. An example of this requirement would be “Monday September 12, 2011 through Thursday September 15th, 2011 from 7:30 a.m. until 6:30 p.m. each day.”

The standard NSSC IT Webpage content filter policy defined in NSWI-2810-0001, *NASA Shared Services Center Work Instruction,* Appendix B, will be applied to the training room network.

The training room network and computers will be monitored in accordance with all current NSSC and NASA agency policies.

The training room will be physically secured when not in use.

APPENDIX Q. MEDIA SANITIZATION

Sanitization of all data storage media at NSSC shall conform to ITS-HBK-0035.

Removable, non-electronic media may be placed into contracted shredder boxes for disposal.

Electronic media, if functional, must be erased in accordance with ITS-HBK-0035. Non-functional electronic media must be given to the NSSC property custodian for proper disposal.

NSSC computers that are being reassigned across corporate or organizational boundaries may be screened and purged of any information sensitive to the departure organization. It is incumbent on the departure organization to be diligent in knowledge of sensitive information and subsequent purging before the computer's scheduled removal.

Sanitization or disposal of media that contains sensitive information may be documented on forms available from, and retained by, the NSSC IT Security Manager.

APPENDIX R. SEPARATION OF DUTIES

In order to effectively implement NIST control AC-5 (separation of duties) and mitigate risk of conflict due to overlapping jurisdiction, it is necessary to define and separate key data center administrative roles.

Privileged roles identified:

- System Administrator
- Database and Application Administrator

Responsibilities:

System administrators shall be responsible for -

- Implementation and maintenance of security controls at the system level, defined as operating system, hardware, and network connectivity but excluding the network, databases and applications
- Availability of the system
- Performance and risk mitigation of the system
- Managing system access by others
- Controlling server processes
- Implementation of system configuration changes.

Database and Application Administrators shall be responsible for -

- Implementation and maintenance of security controls for databases and applications
- Availability of databases and applications
- Performance and risk mitigation of databases and applications
- Defining hosting requirements for supporting database and application functionality
- Controlling database and application processes
- Implementation of database and application configuration changes.

APPENDIX S. DATA AT REST PROTECTION

There is high probability of sensitive information being contained on NSSC computers and reasonable means shall be taken to protect this information from unauthorized access. No NSSC computer may be taken outside the gates of SSC, nor be left unattended when outside the NSSC workplace, unless it is equipped with a functioning means of encrypting its contents.