

REQUIREMENTS	SENSITIVITY LEVEL 0	SENSITIVITY LEVEL 1 (All Level 0 Requirements Plus)	SENSITIVITY LEVEL 2 (All Levels 0 and 1 Requirements Plus)
ACCREDITATION			
ACQUISITION OF IT RESOURCES	<ul style="list-style-type: none"> • A clause requiring delivery of virus-free products. • Comply with functional security requirements of Computer Security Act of 1987 (PL 100-235) and OMB Circular A-130, APP III. 	<ul style="list-style-type: none"> • Contracting and Technical Officers must ensure that ITS requirements are included in RFPs. 	
AUDIT TRAIL		<ul style="list-style-type: none"> • Review audit trails periodically. • Record all access failures to systems, files, objects, and resources. • Record all systems privilege use. 	<ul style="list-style-type: none"> • Review audit records weekly. • Retain audit records for 1 year.
AUTHORIZATION TO PROCESS (systems/networks)	<ul style="list-style-type: none"> • DPI Management's written authorization for any system or network to process: <ul style="list-style-type: none"> - Before operations begin - After significant change • Reauthorization every 3 years. 		<ul style="list-style-type: none"> • Reauthorization every 2 years.
CERTIFICATION/RECERTIFICATION		<ul style="list-style-type: none"> • DPI-ITSO Certification <ul style="list-style-type: none"> - Prior to use - After significant change • Recertification every 3 years prior to Management reauthorization to use. 	<ul style="list-style-type: none"> • DPI-ITSO recertification every 2 years prior to Management reauthorization to use.
COMMUNICATIONS SECURITY (COMSEC)			<ul style="list-style-type: none"> • Data encryption compliant with NIST standards. (Justification for non-use requires GSO approval). • No uncontrolled dial-up access or unauthorized connections to external networks.
COMPUTER SECURITY AWARENESS TRAINING (CSAT)	<ul style="list-style-type: none"> • A DPI designee must provide initial training to all new employees within 60 days of employment. • A DPI designee must provide training whenever there is a significant change in the ITS environment or procedures. • A DPI designee must conduct refresher training as frequently as determined necessary (at least biennially). • The DPI-ITSO must maintain signed acknowledgement of training for 2 years. 	<ul style="list-style-type: none"> • A DPI designee must conduct system or network-specific security training for users. • A DPI designee must provide training whenever an employee enters a new position which deals with sensitive information. 	

CONFIGURATION MANAGEMENT (hardware, software and procedures)	<ul style="list-style-type: none">• Annual inventory of hardware.• Maintain current hardware listing.• Maintain licenses for all copyrighted software.• Maintain current network and system configuration diagrams.	<ul style="list-style-type: none">• Maintain a process that controls changes to all software, hardware, or procedures in the system.• Maintain a listing of all licensed software.• Maintain a complete inventory of system software and applications.• Full backup every 3 months.• Incremental backups as determined by owner.• Most recent incremental backup stored on-site.• Other backup on-site storage in different building.	<ul style="list-style-type: none">• Annual inventory of all software.• Maintain a current listing of all software.• Monthly full backup.• Weekly incremental backup.• All backup storage in a separate location except weekly incremental.
--	--	---	--

REQUIREMENTS	SENSITIVITY LEVEL 0	SENSITIVITY LEVEL 1 (All Level 0 Requirements Plus)	SENSITIVITY LEVEL 2 (All Levels 0 and 1 Requirements Plus)
CONTINGENCY PLAN/DISASTER RECOVERY		<ul style="list-style-type: none"> • Develop and document a plan that covers emergency response, recovery and return to normal operations. <ul style="list-style-type: none"> - Approval by DPI Management. • Test, review and update the plan annually. • Plan must meet the requirements of FIPS PUB 87. 	
DESTRUCTION OF INFORMATION TECHNOLOGY (printouts, film, ribbons, etc.)		<ul style="list-style-type: none"> • Destroy by shredding (tearing 6 times minimally acceptable): <ul style="list-style-type: none"> - Designated Sensitive Data - Risk Assessments. 	<ul style="list-style-type: none"> • Destroy per established procedures <ul style="list-style-type: none"> - For Official Use Only (FOUO) - Privacy Act Data - Proprietary Data - Procurement Sensitive Data - Source Evaluation Board (SEB).
DISPOSAL OF INFORMATION TECHNOLOGY RESOURCES (hardware/media)	<ul style="list-style-type: none"> • Remove data and Federal records from computer data storage as required by GSFC CIO Notice 98-01. 		
ELECTRONIC MAIL (e-mail)	<ul style="list-style-type: none"> • For official business only. • U.S. Government credit card numbers cannot be transmitted via e-mail. 	<ul style="list-style-type: none"> • Information which cannot be transmitted via e-mail: <ul style="list-style-type: none"> - Designated Sensitive Data - Risk Assessments. 	<ul style="list-style-type: none"> • E-mail use for the following requires GSO approval: <ul style="list-style-type: none"> - For Official Use Only (FOUO) - Privacy Act Data - Proprietary Data - Procurement Sensitive Data - Source Evaluation Board (SEB).
ENVIRONMENTAL CONTROLS	<ul style="list-style-type: none"> • Install adequate dust, water, temperature, humidity and ventilation controls. • Install surge protection on all resources. • Install a fire suppression system. 	<ul style="list-style-type: none"> • Emergency power-off switch. • Emergency power-down procedure. • Plastic sheeting to protect from overhead liquid discharge. • Humidity warning system. • Temperature warning system. • Water detectors under raised floor. 	<ul style="list-style-type: none"> • UPS or Power Distribution Unit (PDU) for minicomputers, servers and mainframes.
IDENTIFY INFORMATION CATEGORIES AND SENSITIVITY LEVELS	<ul style="list-style-type: none"> • Assign an information category and sensitivity level to each system, network, and application. <ul style="list-style-type: none"> - Concurrence of DPI-ITSO required 	<ul style="list-style-type: none"> • DPI-ITSO maintains current inventory of DPI systems and networks. 	
INCIDENT REPORTING AND HANDLING	<ul style="list-style-type: none"> • Report security incidents per Enclosure 14. • Forward GSFC Form 24-10 (Incident/Investigative Report) to the DPI-ITSO and Center ITS Manager. • DPI-ITSO should: <ul style="list-style-type: none"> - Maintain a file of security incidents and - Retain copy for 2 years. 	<ul style="list-style-type: none"> • Retain copies until the next independently-conducted ITS Compliance Review. 	

INDEPENDENT COMPLIANCE REVIEW		<ul style="list-style-type: none">• GSO Compliance Review every 3 years.	<ul style="list-style-type: none">• GSO Compliance Review every 2 years.
LOGOFF AND TIMEOUT		<ul style="list-style-type: none">• Suspend a user ID after 5 consecutive unsuccessful access attempts.	<ul style="list-style-type: none">• Log off or pause workstations or terminals that have not had keyboard activity for a fixed period of time not to exceed 30 minutes.

REQUIREMENTS	SENSITIVITY LEVEL 0	SENSITIVITY LEVEL 1 (All Level 0 Requirements Plus)	SENSITIVITY LEVEL 2 (All Levels 0 and 1 Requirements Plus)	SEN (All Plu
LOGON BANNER	<ul style="list-style-type: none"> Install logon banner as required in NASA CIO letter dated October 10, 1997, subject, "Guidance on Implementation of Information Technology (IT) Security Warning Banners." 			
MAINTENANCE AND REPAIR (Government owned)	<ul style="list-style-type: none"> Permission of the Property Custodian and a property pass are required to remove equipment from a Government or Government Contractor-controlled facility. Delete licensed software from fixed storage media before property is removed from Government or Government Contractor-controlled facility. 	<ul style="list-style-type: none"> Delete or remove information from fixed storage media (if technically possible) before property is removed from a Government or Government Contractor-controlled facility. 		
MARKING OF INFORMATION		<ul style="list-style-type: none"> Identify all media with an external and/or internal label 	<ul style="list-style-type: none"> Provide a visual means of identification for all media containing Privacy Act Data, Proprietary Data, SEB and For Official Use Only (FOUO) data. 	
MEDIA DECLASSIFICATION				
MEDIA AND MEMORY CLEARING	<ul style="list-style-type: none"> Follow procedures detailed in Enclosure 9 for clearing, when required. 			
MEDIA STORAGE	<ul style="list-style-type: none"> Protect media from theft, vandalism, and natural disasters. 	<ul style="list-style-type: none"> Store media in an environmentally controlled area. Secure diskettes in a lockable container or area. Ensure only authorized personnel can access the media. Maintain an inventory accounting system for media entering and departing storage facility; verify inventory annually. 		
NETWORK AND SYSTEM ACCESS CONTROL		<ul style="list-style-type: none"> Single-user networked and multi-user computers and workstations must implement user identification (USERID). Maintain log of all accesses to multi-user systems. 	<ul style="list-style-type: none"> Provide measures that ensure: <ul style="list-style-type: none"> identification and authorization of individual users restriction of functional capabilities of individual users written authorization for system interconnection. 	<ul style="list-style-type: none"> Pr ar sy de Au re fil DI

NETWORK AND SYSTEM ADMINISTRATION	<ul style="list-style-type: none">• DPI-ITSO must be assigned in writing.• A system or network administrator must be assigned in writing.			
--	--	--	--	--

REQUIREMENTS	SENSITIVITY LEVEL 0	SENSITIVITY LEVEL 1 (All Level 0 Requirements Plus)	SENSITIVITY LEVEL 2 (All Levels 0 and 1 Requirements Plus)
PASSWORD		<ul style="list-style-type: none"> • All accounts must be password protected. • Preferably 8 alphanumeric characters (minimum of 6). • Change at least every 180 days, upon termination of employment or reassignment of any person having knowledge of a system password, or whenever the password is suspected to have been compromised. • Are not to be displayed on the system monitor. • Should not be a word appearing in a dictionary. • Vendor-provided and default passwords must be changed prior to system use. • Are not to be stored in batch files or keyboard macros. • Individual users are not to share, write down or electronically store passwords. • Single-user networked and multi-user computers and workstations must implement passwords. 	<ul style="list-style-type: none"> • DPI-ITSO approval for the use of group passwords.
PERSONNEL SECURITY		<ul style="list-style-type: none"> • National Agency Check (NAC) screening prior to being granted access, for all individuals who are authorized to bypass significant technical and operational security controls. • Assign a position sensitivity rating to each Federal employee and each Non-Federal position. • Reevaluate position sensitivity ratings annually. • Complete Foreign National Access Request (Enclosure 7) for foreign national users of ITS resources prior to use. 	<ul style="list-style-type: none"> • National Agency Check (NAC) screening on all personnel who have access. • Screening shall occur prior to individual being granted access.
PHYSICAL SECURITY	<ul style="list-style-type: none"> • Secure IT resources in a locked area or container when not in use. • Annual unannounced fire drill. 	<ul style="list-style-type: none"> • Control access to facility containing IT resources. 	<ul style="list-style-type: none"> • Control NASA Resource Protection (NRP) areas per Chapter 28 and Appendix H of NHB 1620.3C.

REPRODUCTION OF CLASSIFIED MATERIALS			
---	--	--	--

REQUIREMENTS	SENSITIVITY LEVEL 0	SENSITIVITY LEVEL 1 (All Level 0 Requirements Plus)	SENSITIVITY LEVEL 2 (All Levels 0 and 1 Requirements Plus)
RISK MANAGEMENT	<ul style="list-style-type: none"> • Implement a process to: <ul style="list-style-type: none"> - Measure risk (Risk Assessment) - Select appropriate controls to reduce risk to an acceptable level (risk mitigation). - Document residual risk for management acceptance. • Document the process in a Risk Management Plan. • Assess the risk <ul style="list-style-type: none"> - Before operation of new facility, system or network; - Upon significant change or every 3 years, whichever is sooner; - Review and update Risk Management Plan every 3 years. 	<ul style="list-style-type: none"> • Review and update the Risk Management Plan every 2 years. 	<ul style="list-style-type: none"> • Review and update the Risk Management Plan annually.
SECURITY IN THE SYSTEM DEVELOPMENT LIFE CYCLE (SDLC)	<p>Initiation Phase</p> <ul style="list-style-type: none"> • Identify Information Categories and Sensitivity Levels. 	<p>Development/Acquisition Phase</p> <ul style="list-style-type: none"> • Develop Security Plan that meets the requirements of OMB Circular A-130, App III. <p>Implementation Phase</p> <ul style="list-style-type: none"> • Implement security per Security Plan. 	
SECURITY PLAN		<ul style="list-style-type: none"> • Develop a Security Plan that meets the requirements of OMB Circular A-130, App III. • Review and update <ul style="list-style-type: none"> - Upon significant change - Every 3 years 	<ul style="list-style-type: none"> • Review and update every 2 years.
SOFTWARE PROTECTION	<ul style="list-style-type: none"> • Check all software for malicious or unauthorized code prior to its installation. • Install anti-viral software on all file servers, microcomputers and portable computers. 	<ul style="list-style-type: none"> • Protect NASA Computer Programs per NMI 2210.2B. 	

<p>SYSTEM RULES OF BEHAVIOR</p>		<ul style="list-style-type: none"> • A DPI designee must develop “rules of behavior” for each system and network. - Provide in writing to each user. - Maintain on file an acknowledgment of receipt. - Include in DPI-conducted periodic security awareness training. - Include all subjects listed in OMB Circular A-130, APP III. - Clearly delineate responsibilities and expected behavior of all users who access the system as well as the consequences of behavior not consistent with rules. 	
<p>TRANSMISSION (electronic)</p>			<ul style="list-style-type: none"> • FOUO information may be transmitted over FAX provided the recipient will immediately protect it in accordance with FOUO guidance. • FOUO information may be transmitted over telephone lines without encryption.