GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Configurable Basic Service Agreement

For

Army

Network Support Centers

by
Harold P. Jensen Jr.
GSNA
version 2.1 Option #2 practical

© SANS Institute 2003, Author retains full rights.

12/19/03
© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

ABSTRACT

One of the most important issues in dealing providing IT services are who will do what, and what is authorized. Civilian ISP's (Internet Service Provider) for example have agreements with their customers on what is allowed and what is not. In the different military branches they have units that provide ISP like services to their community. Often the tasking of these ISP like units conflict with the actions their customers are taking. This is usually caused by a misunderstanding on whom can do what, who will do what, and whom ultimately owns the computers.

This SLA was designed to cover the many areas that a Military IT provider, in this case a Network Support Center (NSC) might need to discuss with their customers. It was designed to be quickly configurable, and could easily be a 2-3 page document or a full 38 page or longer document based upon the needs of the customer.

This SLA could also be used by a customer to establish a relationship with their Military IT provider to help the IT provider better understand what the customer needs.

The Checklist provide at the end of the SLA will provide the IT Provider and the customer a better understanding of how their network actually exists, and may point out areas that need improvement. This checklist could also be used as a self inspection checklist or to help complete a computer network accreditation package.

When completed this document will provide all parties concerned a basic contract on what will be provided, support required, and paths to resolve any conflicts.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

PREFACE

The information for this SLA has been gathered from several regulations, (DOD, Army, Navy, and Air Force) and several civilian resources. This SLA is designed to follow current Army Knowledge Management (AKM) goals and objectives. This SLA is not intended to supercede any higher level guidance but to give the Network Support Centers (NSC) and their customers an understanding of their relationships and to establish a common background structure. In developing this SLA I treat computer systems and their supporting infrastructure as a weapon system.

This SLA was created by GS-12 Harold Jensen and may be used as needed by all DOD entities. Any suggestions would be greatly appreciated.

General Instructions for the BASIC SLA:
This is a basic SLA for all uses. Certain sections may not apply to your customers, and should be deleted if not applicable

When modifying this SLA to reference any regulations, try to list all applicable regulations under the introduction only. Do not put them in the body of the text as this makes this document extremely long. When necessary provided copies of applicable regulations to your customers as a separate attachment.

Certain Services are always considered CORE (NSC-ONLY) services, and will be annotated with **(NSC-ONLY)** after the title. I.e.3.1a **NETWORK BACKBONE (NSC-ONLY) :** Do not delegate away your responsibilities without approval from your command and proper review.

NON-CORE items are marked with **(NSC/Customer)** which indicates that it is either an NSC function, customer function, or shared.

By default all services supported by an NSC are listed in section 3, FUNCTIONAL RESPONSIBILITIES OF THE NETWORK SUPPORT CENTER, and are assumed to be the function of the NSC. After meeting with your customer, and identifying which NON-CORE services he will take over, move the applicable items to section 4.
Some NON-CORE items might be shared by both the (NSC) and (Customer) and could be in both areas.

To customize quickly,

Find and Replace (NSC) with your own NSC.

Find and replace (Enter Signal Command Here) with your MAJCOM Signal command.

Find and Replace (Customer) with your customers name.

Find and Replace (Battalion) with yours.

Find and Replace (BASE) with yours.

Find and Replace all XXX-XXXX with correct phone numbers.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

You can use the checklist in Section 10 to help you identify the customers network for developing this SLA. The checklist is also a valuable tool for developing the customers DITSCAP accreditation package.

Review all areas, delete those that do not apply move those items that the NSC will do (section 3) or the Customer (Section 4) will do. It is possible that this SLA can be reduced to a few pages for you simple customers.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

INDEX

Section 1 Introduction

Section 2 Purpose

Section 3 Services supported by the (NSC)

Section 4 Services to be taken over by the (Customer)

Section 5 Miscellaneous agreements.

Section 6 Escalation procedures

Section 7 Agreement Summary

Section 8 Acronyms

Section 9 Recommend Setups.

Section 10 Auditing checklist.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

SERVICE LEVEL AGREEMENT (SLA)

BETWEEN THE

(NSC) and the (Customer).

12/19/2003

1. INTRODUCTION:

This Service Level Agreement (SLA) implements DoD Directive 8500.1, "Information Assurance (IA), DoD Instruction 8500.2, "Information Assurance (IA) Implementation Army Regulation 25-1, Army Information Management (AIM); AR 380-19, Information Systems Security; AR 380-5, Department of the Army Information Security Program; and USAREUR PAM 25-1, Army Information Management, and the Army NETOPS program.

2 PURPOSE:

The purpose of this SLA is to state the relationship between the Network Support Center (NSC) and the (Customer). It specifies the services and commitments of the (NSC) as well as the expectations and obligations of the (Customer).
For the purposes of this SLA, the (NSC) is considered a service provider of all services listed below. Several of the services listed are provided by (Enter Signal Command Here), but the NSC will be the local Point of Contact (POC) for any information regarding these services. Current Army directives are seeking to centralize network operations at the NSC Level, and this SLA will follow this guidance.
This SLA is designed to conform to the Army Knowledge Management (AKM) program, and maps the attempt of the (BATTALION) to conform to Army's strategy to transform itself into a network-centric, knowledge-based force.

Funding for any hardware, software, and infrastructure issues is outside the scope of this SLA and should be treated as a separate issue. Please note that certain agreements might create funding issues for you unit. I.e. Helpdesk support or any required training should be addressed by the unit requiring the training. Who will pay for the replacement hardware? Who will pay for the training cost? …etc

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

Network Support Center: (NSC)

i) Point of Contact:

ii) Location or office symbol:

iii) Telephone numbers:

Commercial:

iv) E-mail Address:

v) NSC help Desk:

B. END USER: (Customer)

i) Point of Contact:

ii) Location or office symbol:

iii) Telephone numbers:

Commercial:

iv) E-mail Address:

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

3 FUNCTIONAL RESPONSIBILITIES OF THE NETWORK SUPPORT CENTER, (NSC):

The (NSC) agrees that it will execute the functions identified in the above regulations, to include:

3.1 GENERAL SERVICES:

The (NSC) is the provider of all network infrastructure services for the (Battalion) at (NSC). These services are divided into CORE **(NSC Only)** and NON-CORE **(NSC/Customer)**. Some NON-CORE services may be delegated/ shared with the customer who would then act as a representative of (NSC). User organizations may request NON-CORE services to be performed by the (NSC). The (NSC) manages and requires access to all network devices and closets in which they reside.

The (NSC) will provide proactive and reactive management of resources by monitoring and managing available bandwidth, hardware, and distributed software resources. They will respond to detected security incidents, network faults (errors) and customer reported outages at the time of Help Desk referral. The (NSC) will provide network monitoring and management, 8-hours/day 5-days/week (8X5). The 39th NOSC will provide 24-hours/day 7-days/week (24X7) coverage. On-Call service (2-hour response) is provided when requested by a customer.

3.1.1 CONFIGURATION CONTROL

The (NSC) is the local Point of Contact (POC) for the DA USAREUR initiative to acquire and implement Enterprise Systems Management. The (NSC) will be the local POC to review, approve, and manage all Information Technology (IT) requirements, and implementation IAW Department of Defense (DoD), DA, USAREUR, DISC4, and local standards based architecture (Defense Information Infrastructure (DII) Common Operating Environment (COE), JTA-AF). The (NSC) will coordinate requirements with (Enter Signal Command Here)and CCB.

The (NSC) will develop technical solutions where necessary, review and approve acquisitions to ensure that the base network will not be impacted while customer performance requirements are met. The (NSC) will ensure that all designs and equipment conform to approved system architecture. All Computer Systems Requirements Documents shall be processed within a 2 to 4 week time frame based upon their complexity.

3.1.2 FAULT MANAGEMENT

The (NSC) will detect, identify, isolate, and correct abnormal operations or fault situations of network components. The (NSC) will direct fix actions for all trouble tickets.

3.1.3 PERFORMANCE MANAGEMENT

The (NSC) will be aware of the current and previous performance of the network, including Metropolitan Area Network (MAN), subnets, routers, switches, base firewalls and border systems. The (NSC) will identify potential areas of improvement and potential network faults based on performance analysis.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

3.1.4 ACCOUNT MANAGEMENT

The (NSC) will have management control or oversight for all user accounts that have access to the (NSC) Domain.

3.1.5 ASIPRNET:

The (NSC) is the local POC for all customers requiring access to the ASIPRNET. This includes connectivity, system administration, hardware and software maintenance, upgrades, e-mail, DMS, and ASIPRNET web hosting services.

The (NSC) will establish connectivity to the ASIPRNET. Any quality of service (QOS) issues may be outside the scope of the (NSC), but will be tracked in NSS for comment to USAREUR. AISPERNET problems will be elevated first to the (NSC) who will create an NSS trouble ticket. It will then be tracked by the (NSC) to resolution.

3.2 NETWORK SERVICES:

3.2.1 NETWORK BACKBONE (NSC-ONLY):

The (NSC) provides responsive mission support by managing the (BATTALION) Local and Wide Area Network (LAN/MAN/WAN) infrastructure which provides the Customer with the communications and information resources needed to achieve its operational objectives.

Network services provided by the (NSC) are available 24 x 7 except for planned outages.

Network Trouble tickets will average (to be negotiated with customer) hours or less from ticket submission to return to service. The (NSC) serves as the single focal point for (NSC) Network Management and problem resolution and is the single delivery point for all communications traversing the ANIPRNET/ ASIPRNET.

All communications and information services entering and exiting (NSC) fall under the operational control of the (NSC). The (NSC) will identify, acquire, upgrade and maintain the physical components necessary to support the base network. The (NSC) is the manager of all network components that comprise the network backbone.

The (NSC) will support the customer's bandwidth requirements (10/100Mbps to the desktop) by configuring existing network infrastructure or designing and acquiring required infrastructure components to meet approved requirements.

3.2.2 Base Routers (NSC-ONLY):

The (NSC) has responsibility for the base routers located in all buildings behind the (Enter Signal Command Here) routers. All service to these routers will be provided by the (NSC). Customer owned routers will allow administrative access to their routers for security, configuration, and monitoring purposes. This includes router software upgrades and maintenance.

Performance for all components is measured by the metrics compiled by the (Enter Signal Command Here) and will be available upon request.

3.2.3 Building Switch/Hubs (NSC/Customer):

The (NSC) has responsibility for all building switches and hubs. All service to these devices will be provided by the (NSC). Customer owned devices will allow the (NSC) Administrative access to their devices for security, configuration, and monitoring purposes. This includes device software upgrades and maintenance.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

3.2.4 Firewalls (NSC-ONLY):

The (NSC) has second level responsibility for all Firewall's located behind (Enter Signal Command Here)'s firewalls. This includes upgrades, changes, and maintenance. The (NSC) will configure second level security into the organizations network based on their requirements and above regulations. This includes device software upgrades and maintenance.

All changes required of First Level Firewalls ((Enter Signal Command Here)) will be coordinated though the NSC).
The (Customer) will not install any firewalls, or firewall like programs or devices.

3.2.5 Network Management (Spectrum) (NSC-ONLY):

The (NSC) has responsibility for all network performance management. All service and performance monitoring at the Network level and below is a shared effort with the customer organization. The (NSC) requires that all standards and operational procedures be adhered to as designated by the (NSC). Performance reports will be available to the **(Customer)** upon request.

3.2.6 SERVERS:

3.2.6.1 Enterprise (NSC/Customer):

Enterprise services (Authentication, E-mail, Intranet, and file and print services) is responsible (NSC) for all hardware, software maintenance and upgrades in support of these applications. These servers include, but are not limited to; Domain controllers (PDC, BDC), Intranet Web Servers, E-mail servers, The (NSC) will ensure that the services that run on these servers be available to the customer organization, and that the latest versions of the OS are made available for customer based equipment. In the event that the customer runs their own Enterprise services, the (Customer) agrees to setup an administrative account for the (NSC) to insure proper operation and upgrades are applied to the system.

3.2.6.2 Application and Non-Enterprise (NSC/Customer):

All servers that are application specific (STAMIS,I.E Library Catalog, AWRDS et al), and are Non-Enterprise are the sole responsibility of the (NSC) (Customer) organization. The area of responsibility includes the day-to-day administrative functions as defined in the accreditation package. The (NSC) will periodically review the customer's accreditation package to ensure adherence to DA standards. . In the event that the customer runs their own Enterprise services, the (Customer) agrees to setup an administrative account for the (NSC) to insure proper operation and upgrades are applied to the system.

3.2.6.3 Customer Specific Servers (NSC/Customer):

The (NSC) has overall responsibility for securing the connectivity and safety of any customer's server(s) residing in the (NSC). Day to day operations and administration is solely the responsibility of the customer organization. All service and support to the server(s) is the responsibility of the customer

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

organization. The (Customer) will provide access to the server by authorized (NSC) customer personnel when needed.

3.2.6.4 NORTON ANTIVIRUS SERVERS (NAVSRVR) (NSC-ONLY):

The NSC will host a Community Anti-virus Server that will push all antivirus updates to all systems connected the (NSC) AOR. The (NSC) will ensure that the latest versions of AV software are made available for all (Customer) equipment.

3.2.6.5 UPDATE EXPERT (Patch Management):

Update EXPERT is a hotfix and service pack security management utility that helps Helpdesk, systems administrators (SA), and Information Assurance Officers (IAO) keep their hotfixes and service packs up-to-date by analyzing which service packs and hotfixes are installed on the Windows 2000/NT/XP, which ones are not installed and which ones are available. Update EXPERT facilitates locating, downloading and installing the latest service packs and hotfixes. Update Expert eliminates the confusion and labor of maintaining hotfixes.

3.2.6.5.1 UPDATE EXPERT Master and Leaf servers:

The NSC will be responsible for all UPDATE EXPERT master servers and leaf servers. The (NSC) will provide all required updates to the (Customer) leaf servers.

The NSC Helpdesk, IAO, and SA will use UPDATE EXPERT (UE) to manage all Microsoft systems in the AOR. The (NSC) will ensure that the latest patches are made available for all (Customer) equipment. The NSC IAO will have access to all UE systems in AOR to check for IAVA Compliance. All customer Microsoft based systems will be connected to the UPDATE EXPERT SERVER

3.2.7 INTERNET PROTOCOL ADDRESS MANAGEMENT (NSC-ONLY):

The (NSC) will control all base IP address space. The (NSC) will allocate a block of IP addresses for use on designated LANs. All static network devices (Servers, routers, switches, printers etc) will be set up by the (NSC) for the customers. All private address spaces must be registered and approved by the (NSC). The (NSC) will retain capability to monitor and block any individual IP address or subnet, both private and public. Network devices will be installed in a set range common to the AOR for easy identification. For security reasons the NSC will set the customer up with DHCP IP address with MAC address reservation. This feature prevents anyone just bringing in a computer and getting on the network. They will have to contact the NSC helpdesk for connection.

3.2.8 DOMAIN NAME SYSTEM (DNS) & WINS SERVERS:

3.2.8.1 DNS:

(Enter Signal Command Here) will maintain the base external and internal DNS servers. (Customer) issues with DNS will be coordinated though the (NSC) using NSS. (Customer) DNS servers will act as _____ servers and always point to a

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

5th Command DNS server. Customers DNS servers must be prepared for Dynamic DNS (DDNS) when the Army AD domain is rolled out.

3.2.8.2 WINS:

The (NSC) will maintain and support all WINS servers. (Customer) issues with WINS will be coordinated though the (NSC) using NSS.

3.2.8.3 Active Directory (AD):

(Enter Signal Command Here) is currently working on an AD deployment plan. (Customer) agrees to Follow NETCOM AD policy guidance. POC for all AD questions will be (NSC) Network Branch, who will track AD issues with an NSS ticket to resolution.

3.2.9 REMOTE DIAL-IN / DIAL-OUT COMMUNICATIONS (RAS) (NSC-ONLY):

By DA regulation RAS is not authorized. For Dial in Access see Terminal Service Access Control System (TSACS). 3.2.1

3.2.10 Terminal Service Access Control System (TSACS) (NSC-ONLY):

The (NSC) will provide a Terminal Server Access Control System (TSACS). (Customer)'s needing TSACS access will request an account with the (NSC) Helpdesk. All services for TSACS, including device software upgrades and maintenance. will be provided by the (NSC).

3.2.11 NETWORK TIME PROTOCOL (NTP) (NSC-ONLY):

The (NSC) will establish policies and procedures to ensure the integrity of the Network Time Protocol.

3.2.12 WEB HOSTING SUPPORT SERVICES:

Public access web servers will be hosted only by (Enter Signal Command Here), currently done at ASB/ O6 level. The (NSC) will establish policies and procedures, develop, manage, and maintain the systems for hosting internal (Intranet) Web servers. The (NSC) is not responsible for (Customer) content of pages. The (customer) will ensure that their information is approved for public display by coordinating with the base Public Affairs Office (PAO).

3.2.13 WebCache/ Proxy:

3.2.13.1 WEBCACHE:

(Enter Signal Command Here) will establish and maintain WebCache Proxy services. Statistics will be available by request through the (NSC).

3.2.13.2 PROXY:

The (NSC) is responsible for all hardware, software maintenance and upgrades in support of these Proxy servers. (Customer) owned proxy servers will allow the (NSC) Administrative access to their proxy servers for configuration, security, and monitoring issues. The (NSC) will ensure that the latest versions are made available for customer based equipment. Customers will not set up and install proxy servers to segregate them from (NSC) security monitoring or management.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

3.2.13.3 Virtual Private Network (VPN)

Customers requiring VPN configuration will coordinate all such requests with the (NSC). The (NSC) will track all VPN requests in NSS up to (Enter Signal Command Here) for resolution. VPN will not be set up in such a way as to deny the (NSC) oversight of the network using VPN.

3.2.14 BASE SHARE

The (NSC) will provide the server(s) based storage of base wide data. All information that is enterprise in nature and requires sharing will be stored on the appropriate file server. The (NSC) will provide connectivity and access to the server. The (NSC) will maintain and ensure that sufficient storage exists for all BASE SHARES. The (NSC) will be responsible for backup and restoring of user data as prescribed the regulations above.

IMO's may provide their users additional data backups as needed.

The (NSC) will develop and use login scripts to control all mappings to required base shares. Custom login scripts may be developed as needed to support the mapping requirements of (Customer).

(Customer) will use BASE SHARE for file sharing, and not engage in client to client file shares. Peer to Peer (Client) shares are highly discouraged because of vulnerability issues, backup issues, and security issues. The (NSC) IAO will do routine scans for client to client shares.

3.2.15 MESSAGING SERVICES:

The (NSC) provides organizational and individual core messaging services. Core messaging services offered include, but are not limited to, Defense Messaging System (DMS) and the DA standard electronic mail (e-mail) services (Exchange).

3.2.15.1 DMS

The (NSC) is responsible for all DMS connectivity, configuration, management, security, and server administration. (Customer) IMO's are responsible for administration of their users at the client workstation. The (NSC) will ensure that the centralized management of the system is maintained and that connectivity and access to the DMS systems are available. The (NSC) will maintain and ensure that sufficient storage exists for all base-wide data. The (NSC) will be responsible for backup and restoring of user data as prescribed in the TTP. IMO's may provide their users additional data backups as prescribed in the E-mail CONOPS.

3.2.15.2 Exchange

The (NSC) is responsible for all e-mail connectivity, configuration, management, security, and server administration. (Customer) IMO's are responsible for administration of their users at the client workstation. The (NSC) will ensure that the centralized management of the system is maintained and that connectivity and access to the e-mail systems are available. The (NSC) will maintain secure e-mail access over HTTPS and IMAP 4 for customers that require Internet access to the Exchange mail system. The (Customer agrees

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

The (NSC) will be responsible for backup and restoring of user data as prescribed in the TTP. IMO's may provide their users additional data backups as prescribed in the E-mail CONOPS.

3.3 CABLE PLANT:

3.3.1 Internal building:

The (NSC) has responsibility for all cabling within the customers building(s). Any upgrades (new drops) and or changes need to be coordinated with the (NSC) . All design and engineering requirements will be from the (NSC) .

3.3.2 Intrabuilding (NSC-ONLY):

(Enter Signal Command Here) has overall responsibility for all cabling throughout the (Customer) campus (LAN, MAN). Any upgrades and or changes need to be coordinated with the (NSC) through the Digital Communication Officer (DCO) and tracked with an NSS trouble ticket. All design and engineering requirements will be from the (NSC). All work will be reviewed by the (NSC) DCO/Networking branch for compliance to the Army network infrastructure architecture.

3.4 DEDICATED COMMUNICATIONS LINES (NSC-ONLY):

The (NSC) will maintain dedicated lines for base centralized dial-in and remote access system. Customer dedicated point-to-point data circuits will be acquired IAW DA policy, paid for by customer and acquired through the (NSC). All circuits will be Designated Approval Authority (DAA)/CMB certified. The (NSC) has responsibility to ensure that all LAN/MAN links dedicated to the customer organization shall remain fully operational on the Army side of the commercial connection. Problems that are identified to be on the commercial supplier's side will be transferred to their service desk for resolution. The (NSC) will ensure that connectivity from the dedicated commercial connection to the base entry point is maintained.

3.5 INFORMATION ASSURANCE:

The (NSC) Information Assurance Officer (IAO) at (BASE), will be the IAO responsible all IA issues in the (NSC) Area of Responsibility (AOR). The IAO will conduct Information Assurance Operations according to referenced regulations as previously described, and provide IA services to support the (Customer)'s needs.
(Customer) IA's (IAO, IAS etc) will coordinate with the (NSC) IAO, and incidents will be tracked in NSS to resolution. The (Customer)'s IA's, IMO's, and SA's will work closely with the (NSC) IAO for all IA Issues, and act a representative of the (NSC) IAO. The (NSC) IAO will have overall oversight responsibility to all aspects of IA in the AOR.

3.5.1 Network Vulnerability Scans:

The (NSC) IA will perform vulnerability assessments to test and validate security of networks and systems. If vulnerabilities are discovered, they will provide appropriate IMO's, systems administrators, commanders, DAA, MAJCOM IA offices, NOSC, and RCERTE with test results and recommendations. The IAO will attempt to coordinate scans to have minimum network impact, with the understanding that random scans are required to detect network vulnerability issues. (Customer) IA's will provide vulnerability scans results to the (NSC) IAO

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

as required. High vulnerability found during scans will be resolved by the IAO by working with the (Customer)'s IMO, SA, the (NSC) Helpdesk or network staff.

3.5.2 Information Assurance Vulnerability Alert (IAVA) Reporting:
The (NSC) IAO will perform IAVA reporting for (Customer) to the Information Assurance CRD database. The IAO may work with (Customer) IMO's, SA's etc to achieve IAVA compliance.

3.5.3 Accreditations:
The (NSC) IAO is the local POC for Accreditation issues in the (NSC) AOR.
In the development of (Customer) Accreditation packages, the (NSC) IAO will act as the Certifying Authority (California) for the (Customer)'s package.
It is the responsibility of the (Customer) to do the majority of the accreditation package development. The (NSC) IAO will provide guidance, review and support in accreditation development.
The IAO will insure that the (Customer) has a valid Accreditation prior to connecting to either the (NSC) ANIPRNET or ASIPRNET.

3.5.4 Accreditation Package Changes: The (Customer) will provide the IAO copies of all events that result in accreditation package changes. This includes Software changes, Hardware Changes, and Network Architecture changes that happen at the (Customer) site.

3.5.5 NETWORK CHANGE PROPOSALS (NCP):
The NSC IAO will review all (Customer) NCP's for IA issues, All NCP requests will be generated at the NSC Help Desk.

3.5.6 IA Related Training:
The NSC IAO will provide IA related training to the (Customer)'s representatives as requested.

3.6 HELP DESK SERVICES:

NSC/NSC Help Desk (DSN XXX-XXXX) is the focal point for all problem resolution. They will provide a central repository for technical advice, tracking history, and solutions for network systems, software applications assistance, automatic data processing support, hardware exchange, and repair service support, IA issues, telephone issues, etc.
The (NSC) Automation Branch receives all service requests and processes them to the appropriate NSC technical staff for resolution.
Service Desks in (Customer) organizations act as agents for the (NSC) Automation Branch and will coordinate with the (NSC) Helpdesk.

3.6.1 NSS NETOPS Support System (REMEDY) (NSC-ONLY):
The (NSC) Automation branch is responsible for the overall management of the NSS trouble ticketing generating system. Its functions include centralized reporting which relies on data gathered from the (Customer) organization. The (NSC) Helpdesk will provide the centralized NSS as well as its distributed

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

components to be utilized by customers. All updates for the system will be managed by the (NSC) Helpdesk. All customer trouble calls will be logged and tracked using NSS.

3.6.1.1 NSS TROUBLE TICKETS:

All requests from the (Customer) will be tracked in the NSS system. These inputs can be generated by the IMO, (Via the NSS webpage), by telephone, or by e-mail. The preferred method of generating NSS tickets is via the NSS Web interface. The (NSC) helpdesk will provide NSS training to the (Customer).

The (NSC) will ensure that the Help Desk is manned from 0800-1630. After normal hour's inquiries will be on an on-call basis with a 4-hour response upon initial contact. A trouble ticket will be generated and followed through resolution for each incident. The following are the customer personnel who will assist users with their problems:

3.6.2 TIER SUPPORT:

The following is a list of the Tier support structure. Personnel in this structure can appear at all levels, from Customers site or the NSC level.

Tier I - Workgroup Managers (IMO) or contracted personnel will assist users in OS and application questions provide hardware diagnosis with simple repair or replacement of components or system or connecting a system to the wall jack. They will elevate problems to the SA.

Tier II – System Administrators (SA) ensure servers, workstations, peripherals, communication devices and software are on-line and available. The (Customer) SA's will contact the NSC Help Desk if they cannot resolve a problem.

Tier III – Network Hardware that require intervention by the (NSC) /vendor in order to correct.

3.6.3 WORKSTATION SETUP:

The **(**NSC) Help Desk (phone) is the focal point for workstations setup. (Customer)'s should contact the helpdesk prior to attempting to connect to (NSC) LAN, to insure baseline and security issues are met.

3.6.4 SOFTWARE INSTALLS/ SUPPORT: The (NSC) Help Desk (phone) is the focal point for software install/ support. (Customer)'s must contact the help desk prior to attempting to connect to (NSC) LAN, to insure software is correctly installed. Licensing issues are the responsibility of the (Customer). The (NSC) Helpdesk will provide software support to the (Customer) to correct any issues. (Customer) agrees only to use software approved by the DA. For questions concerning approved software contact the NSC IAO.

3.6.5 COMPUTER USER TEST: No user accounts will be issued until the user has completed the computer user test, verified by the NSC Helpdesk. After 3 years all personnel are required to take retake the computer user test.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

3.6.6 ACCOUNT CREATION: The (NSC) Helpdesk will be the focal point for all Networks, e-mail and TSACS system accounts requests. A Computer user test is required before the account information is given to the user.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

4 RESPONSIBILITIES OF THE (Customer) :

The (NSC) and (Customer) representatives are the focal points for identifying, obtaining and maintaining the (Customer) communications and information requirements to meet the (Customer) objectives. The following items will be performed by the (Customer) in agreement with (NSC) policy.

4.1 GENERAL RESPONSIBILITIES OF the (Customer)

4.1.1 USE OF NSS (REMEDY):

The (Customer)'s IMO agrees to use NSS trouble ticket system to request and track all trouble tickets to resolution. NSS Tickets will be sent by the (NSC) Helpdesk to appropriate section for resolution. In the event the NSS system is down, the (Customer) will call the (NSC) Helpdesk XXX-XXXX to have a ticket opened for them.

4.1.2 MAINTENANCE SCHEDULE:

The (Customer) will support the (NSC) maintenance schedule of (every other Thursday after 1800 hours). The (NSC) shall schedule the (second weekend of every month for out-of-cycle maintenance). (Customer)'s wishing to participate in out-of-cycle maintenance must identify their needs two weeks in advance in order to ensure (NSC) personnel availability.

4.1.3 INFRASTRUCTURE AND SERVICE CHANGES:

The (Customer) agrees to implement all infrastructures (Cabling, router/ switch configuration, etc) and service changes as defined by the (NSC) per USAREUR/ DA guidance. Once these changes are agreed to, the (Customer) will implement these changes so as not to impact the (NSC)'s or the (Customer)'s daily operations as early as possible.

4.1.4 NEW EQUIPMENT:

(Customer) agrees to coordinate through the (NSC) the setup of all new devices (workstations, printer, servers, routers, etc.).
The (Customer) agrees that no new equipment will be installed until the (NSC) has prepped it for set up.

4.1.5 CORE EQUIPMENT PASSWORDS:

Core equipment passwords (BIOS, IOS, and OS) will be maintained by the (NSC). The (Customer) will not disable the core equipment passwords.

4.1.6 NETWORK ARCHITECTURE:

(Customer) agrees to coordinate all planned changes to the network with the (NSC), using NSS, before implementation. (Customer) understands that a Network Change Proposal (NCP) must be generated in the NSS before any changes can be implemented. Customer should contact the NSC Helpdesk for all NCP request.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

4.1.7 ADPE INVENTORY

The (Customer) is responsible for managing their ADPE inventory per current Army Regulations.

4.1.8 SOFTWARE INVENTORY:

The (Customer) is responsible for managing their software inventory. The (NSC) can help provide inventory information to the customer upon request to help them determine their software license issues.

4.1.8.1 APPROVED SOFTWARE:

The (Customer) agrees to only use DA approved COTS/GOTS and IA software. The (Customer) can request this information from the (NSC). In the event unapproved software is identified, the (Customer) agrees to migrate to approved software as soon as feasible. Software currently used that is not on the approved Software list will be annotated on the users accreditation and in the audit checklist at the end of this document.

4.1.9 FIREWALLS:

The (Customer) will not install any firewalls, or firewall like devices.

4.1.10 ACCREDITATIONS:

4.1.10.1 COPIES:

The (Customer) will provide completed soft and hard copies of their ANIPRNET and ASIPRNET Accreditations to the (NSC) IAO, prior to being connected to the ANIPRNET or ASIPRNET.

4.1.10.2 DEVELOPING:

It is the responsibility of the (Customer) to complete the development of their accreditation packages. It is recommended that the (Customer) appoint at least two of his staff in accreditation development. In the development of (Customer) Accreditation packages, the (NSC) IAO will act as the Certifying Authority (CA) for the (Customer)'s package. The (NSC) IAO will also provide guidance, review and support in accreditation development.

4.1.10.3 REACCREDIDATION:

The (Customer) will complete a reaccredidation every 3 years, as per regulation, or upon a major network change as recognized by the (NSC) IAO.

4.1.11 COMSEC:

The (Customer) is to comply with Army COMSEC procedures as listed in the above regulations.

4.1.12 RAS:

Customer will not attempt to install any form of RAS. For Dial in Access see Terminal Service Access Control System (TSACS). All workstations and laptops

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

connected to the ANIPER/ ASIPRNET will have internal modems disabled per USAREUR baseline guidance.

4.1.13 BASE SHARES:

The (Customer) will use BASE SHARE for file sharing, and not engage in client to client file shares.

4.1.14 PROXY SERVICES:

The (Customer) will not set up and install proxy servers with the intent to segregate them from (NSC) security monitoring or management. (Customer) will provide copies of proxy logs to the (NSC) upon request.

4.1.14 Wireless (WIFI):

Current DA regulations do not approve the use of wireless. As Wireless becomes acceptable to USAREUR, the (Customer) agrees to coordinate all WIFI requests with the NSC, who will open an NSS ticket, aid in the development, and track the project to resolution.

4.2 NSC DELEGATED NETWORK SERVICES:

The (NSC) and the (Customer) agree the following responsibilities are delegated to the (Customer) for all equipment located in (Customer) building(s), as identified in the following subparagraphs.

The (Customer) understands that delegation means acting on behalf of the (NSC),and the (Customer) will set (NSC) requests for action as a priority and provide operational data and statuses as a priority.

The (Customer) agrees to follow the directions of the (NSC) and higher headquarters directives, policies, processes, and standards when managing the day-to-day operations for this equipment. In the event of a conflict with above regulations, the (Customer) agrees to apply the more restrictive of the directives.

Enter subparagraphs here: If none so state

5 MISCELLANEOUS AGREEMENTS:

5.1 SECURITY:

The (Customer) shall implement a Network Security program to effectively manage and protect Network Infrastructure as defined by the (NSC). Services and network connectivity of local systems and networks may be terminated if the (Customer) fails to maintain compliance with DA and (NSC) security policies, standards, and practices.

5.2 (CUSTOMER) PLANNED OUTAGES:

The (Customer) shall notify all (Customer)'s personnel and the (NSC) at least one weeks prior to all planned service outages. The (Customer) shall ensure that planned outages do not impact its customer's needs and shall occur during Non Core hours, (after 1800 during the week and anytime during weekends). Unplanned outages must be taken care of on a case by case basis; however; the (Customer) will create a ticket in NSS for these outages. These tickets can be used to track trends and incidents that may lead to the cause of these outages.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

5.4 SERVICE DEGRADATION AND FAILURES

Network trouble notification shall be provided to The (NSC) Help Desk via a NSS Trouble ticket as soon as the (Customer) is aware of a problem.

5.5PROCESSES, STANDARDS AND POLICIES

The (Customer) agrees to implement all approved processes, standards and policies, as they relate to (NSC) Network services, which deal with system requirements gathering, procurement, installation, maintenance and operations.

This section left intentionally
left blank.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

6 ESCALATION PROCEDURES:

The (NSC) and the (Customer) agree to use the following procedures if it becomes necessary to escalate/elevate a problem that is not satisfactorily resolved:
For Helpdesk issues, to the (NSC) Helpdesk Chief;
For Network issues, to the (NSC) Network Chief,
For IA issues, to the IAO,
For any of the above then the (Customer) will elevate the problem to the NSC Chief, then to the Battalion commander.

A. For normal problems the (Customer) will use the base standard trouble ticketing system, NSS, to post a ticket to the (NSC) Help Desk, who will track the problem through resolution. The (NSC) will ensure the ticket is assigned, worked and closed using the agreed upon problem notification procedures. If a problem is not satisfactorily resolved (falls outside of the agreed performance levels continuously) or unsatisfactory service has been performed by the (NSC) personnel, it will be escalated to the next Logical level;

B. If a Helpdesk resolution cannot be performed, escalation should be to the (NSC) Automation Chief:
NAME:
Phone:
E-mail:

C. If a Network resolution cannot be performed, escalation should be to the (NSC) Network Chief:
NAME:
Phone:
E-mail:

D. If an Information Assurance resolution cannot be performed, escalation should be to the (NSC) IAO:
NAME:
Phone:
E-mail:

E. If none of the above result in a resolution then, escalation should be to the (NSC) NSC Chief:
NAME:
Phone:
E-mail:

F. If none of the above result in a resolution then, escalation should be to the (BATTALION) Commander (NSC)/CC:
NAME:
Phone:
E-mail:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

7.0 AGREEMENT SUMMARY:

A. The (NSC) and (Customer) agree that the terms of this SLA will remain in effect for three (3) years and may be modified or amended at that time if necessary. For additions, an addendum may suffice without renegotiating this SLA.

B. The (NSC) and (Customer) agree that in the event an out-of-cycle SLA review is deemed necessary, due to changing organizational situations or other factors, the (NSC) POC or (Customer) POC for this document will notify their counterpart in the other organization. At that time, the notifying POC will clearly identify the circumstances surrounding their contention that the existing SLA needs out-of-cycle review in order to quickly resolve the situation.

Service levels and procedures established herein were agreed to by the (NSC) and (Customer) Network Services represented by the undersigned.

FOR (NSC) : (Customer) :

_____ _____

Signed Signed

Date: _____ Date: _____

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

Section 8 Acronyms

(Enter Signal Command Here)	Major Signal Command (Network owner)
AD	Microsoft Windows 2000 Active Directory
AEI	Army Enterprise Infrastructure
AFN	American Forces Network
AKM	Army Knowledge Management
AOR	Area of Responsibility
ASC	Army Signal Command
ASG	Area Support Group
ATMIS	Automated Telephone Management Information System
BTN	Battalion
CA	Certification Authority
CAN	Campus Area Network
CAT5	Category 5 Cabling OR without cabling (Page 4-5)
CD	compact disk
CD-ROM	Compact Disk – Read Only Memory
CEG-E	Combat Equipment Group - Europe
CIO	Chief Information Officer
CL	Clerical
COM	Computer Output Microfilm
CONOPS	Concept of Operations
CONUS	Continental United States
COTS	Commercial Off-the-Shelf
CPU	Central Processing Unit
DA	Department of the Army
DCA	Directorate of Community Activities
DCO	Dial Control Office
DMA	Defense Messaging Systems
DNS	Domain Name System (or Service)
DoD	Department of Defense
DPW	Directorate of Public Works
DSN	Defense Switching Network
EIS	Enterprise Information Systems
E-Mail	Electronic Mail
FAQ	Frequently Asked Questions
FAX	Facsimile

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

FTP	File Transfer Protocol
FY	Fiscal Year
HDQA	Headquarters Department of the Army
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletins
IIS	Internet Information Services
IMO	Information Management Office(r)
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MACOMS	Major Army Commands
MAN	Metropolitan Area Network
NATO	North Atlantic Treaty Organization
NAV	Norton Anti-Virus
NDS	Novel Directory Services
NETCOM	Network Enterprise Technology Command
NETOPS	Network Operations
NIC	Network Interface Card
ANIPRNet	Army Non-classified Internet Protocol Router Network
NOSC	Network Operating Center
NSC	Network Service Center
NT	New Technology (Windows)
NTFS	NT File Systems
OEM	Original Equipment Manufacturer
OS	Operating System
PDA	Personal Digital Assistant
PEO	Program Executive Office
PKI	Public Key Infrastructure
PMO	Provost Marshall's Office (Army Unit)
RAM	Random Access Memory
SHAPE	Supreme Headquarters Allied Powers Europe
SHN	Schinnen
SIG	Signal
ASIPR	Army Secure Internet Protocol
SLA	Service Level Agreement
SME	Subject Matter Expert
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

STAMIS	Standard Army Management Information Systems
TCO	Telephone Control Office OR Total Cost of Ownership
TDY	temporary duty
TECHCON	Technical Control
USAREUR	United States Army Europe
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wireless Application Protocol
WIFI	Wireless networking
www	world wide web

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

Section 9 Additional Recommended Setups:

1. Have the NSC IAO provide you an ISS or Harris Stat scan of your system to identify areas needing improvement.

2. The following additional steps are recommended for enhancing your computer security beyond the RCERTE baseline, and are totally optional. These vulnerabilities often show up in a Harris Stat Scan.

NOTE: The RCERTE baseline is the bare minimum setup requirements for all systems. The baseline instructions for all systems can be found at https://iassure.usareur.army.mil/security/ Any questions concerning the RCERTE baseline should be directed to the (NSC) Helpdesk or the (NSC) IAO.

9.1 WORKSTATIONS			
ITEM	**STEP**	**JUSTIFICATION**	**EFFECT**
9.1.1	Password Protect BIOS on all computers	Locks Users out of BIOS preventing system changes	Protects BIOS, and makes it harder for intruders to affect system.
9.1.2	Set Bios to boot with HDD 0 only or First	Keeps intruders from booting a floppy or CD	Speeds up the boot up process, and prevents intruders for breaking into the system.
9.1.3	Disable DCOM service on NT Machines	DCOM (Distributed Component Object Model) is a set of Microsoft concepts and program interfaces in which client program objects can request services from server program objects on other computers in a network. http://www.iss.net/security_center /static/176.php	Mitigates this vulnerability, unused in most areas, Speeds up systems.
9.1.4	Disable Automatic Updates	Allows computer to download updates from Microsoft. Some systems require user have admin rights for updates to work, ties up network bandwidth, site redirect could allow hacker to exploit this service and send out Trojan files as an update.	Frees up network bandwidth, Prevents OS problems, tightens security on workstation.
9.1.5	Disable background intelligent transfer service (BITS)	Part of Automatic Updates service	Frees up network bandwidth, Prevents OS problems, tightens security on workstation.
9.1.6	Disable SSDP Discovery Service	Enables discovery of UPnP devices on your home network	Mitigates this vulnerability, unused in most areas, Speeds up systems.
9.1.7	REGEDIT associated with Registry files	Regedit.exe is associated with registry files. Anyone could open a *.reg file and modify a registry when the file is run. Regfile associations can be changed by non-administrators. By default if you double-click on a file with a '.REG' extension the file will be imported into the system registry. Changing the registry could cause serious problems that may cause a denial of service or require you to reinstall the operating system.	Some hacker attempts use e-mail attachments can modify the registry files. This change would mitigate this vulnerability.
9.2 PRINTER SETUPS			

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

9.2.1	Update Printer BIOS/IOS	Newer BIOS for many of the printers have enhanced security	Increase security to printer.
9.2.3			
9.3 Server Setups			
9.3.1	Password Protect BIOS on all computers	Locks Users out of BIOS preventing system changes	Protects BIOS, and makes it harder for intruders to affect system.
9.3.2	Set Bios to boot with HDD 0 only or First	Keeps intruders from booting a floppy or CD	Speeds up the boot up process, and prevents intruders for breaking into the system.
9.3.3	Disable Automatic Updates	Allows computer to download updates from Microsoft. Some systems require user have admin rights for updates to work, ties up network bandwidth, site redirect could allow hacker to exploit this service and send out Trojan files as an update.	Frees up network bandwidth, Prevents OS problems, tightens security on workstation.
9.3.4	Disable background intelligent transfer service (BITS)	Part of Automatic Updates service	Frees up network bandwidth, Prevents OS problems, tightens security on workstation.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

Section 10. Auditing Checklist

CUSTOMER POC INFORMATION
Location
Building Number(s)
Office Symbol
POC Phone

CUSTOMER CONFIGURATION INVENTORY:
NUMBER OF:
OS 98:
OS NT4:
OS 2000:
OS XP:
Other (please state)
Total Workstations

Users:

Servers:
OS Used:

Protocols Used:

IP Address ranges:

Networked
Printers:
Routers:
Switches:
Hubs:
Public Web server (either hosted by self or others):
If Yes address:

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

Auditing Checklist for SLA Between (Customer) and the (Organization) NSC.

Item

Stan.

Standard Description

Comply

Comments

LEGEND

Implementation Standard:
N = not applicable
O = optional
R = recommended
M = mandatory

Compliance:
X = no protection/not implemented
W = needs work
A = adequate; meets or exceeds standard

1. General

1.1

M

Accreditation Package complete and accurate?

X W A

1.2

M

All IMO's and SA's properly trained in IACND?

X W A

1.3

M / R

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

Backup plan developed for servers (M) and staff workstations (R)?

X W A

1.4

R

DA security policy briefed detailing rights and responsibilities of staff, patron, and contract users of the network?

X W A

1.5

M

Internal Acceptable Use Policy (IAUP) developed for patrons and staff; includes consequences of misuse of equipment or services?

X W A

1.6

R

Workstation security plan developed

X W A

1.7

M

Staff trained not to reveal system passwords to anyone.

X W A

1.8

M

Train staff not to allow anyone access to systems and network equipment without prior authorization

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

X W A

1.9

M

Monitor anyone performing maintenance/ configuration and do *not* to disclose any network configuration information to any third-party without prior authorization.

X W A

2. Physical & Data Security

2.1

M

Dead bolt locks on all building entrances/exits

X W A

2.2

M

All servers and network equipment (Router etc) in staff-only area, preferably locked (alternatively, in locked equipment cabinet)

X W A

2.3

R

Data cables/data jacks (public areas) are secured from patron access, if possible, and not connected if not used.

X W A

2.4

R

Locked storage is used for backup media and emergency recovery disks/CDs

© SANS Institute 2003, Author retains full rights.
© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

X W A

2.5

R

Rotate one backup set offsite regularly and store in a secure location

X W A

2.6

R

Store backup of router, firewall configuration file, if applicable, in a secure location

X W A

2.7

R

Keys used in securing equipment or media are stored in a controlled location

X W A

2.8

M

All workstations and servers follow local Naming standard.

X W A

2.9

R

All workstation power cords connected to surge protectors.

X W A

12/19/03
© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

2.10

M

No modems enabled on workstations connected to LAN.

X W A

2.11

R

Serial numbers and physical asset numbers (if applicable) are recorded for all workstations, servers, and network equipment

X W A

2.12

M

All workstation have correct security labels for level authorized. (SF-710)

X W A

3. Password Security

3.1

M

Follow DA/USAREUR written password policy and brief to all staff and patrons using specific user logons

X W A

3.2

M

Document passwords for all network equipment, servers, and workstations

X W A

12/19/03
© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

4. Hardware Security

4.1

R

BIOS: public workstation: boot order, set primary hard drive first

X W A

4.2

R

BIOS: server (locked staff-only access): boot order, either setting

X W A

4.3

R

BIOS: server (when locked staff-only access is not possible): boot order, set primary hard drive first

X W A

4.4

R

BIOS: workstations: supervisor password set

X W A

4.5

R

BIOS: servers: if servers can restart automatically with password set, set one

X W A

4.6

12/19/03
© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

O

BIOS: anti-virus protection enabled

X W A

4.7

O

BIOS: public workstations: floppy drive(s) disabled if IAUP specifies no patron access to floppy disks

X W A

4.8

R

BIOS: servers (when locked staff-only access is not possible): disable floppy drive

X W A

4.9

R

BIOS: public workstations: setup message hidden/ disabled, if available

X W A

4.10

R

BIOS: all computers: record setup configuration parameters

X W A

4.11

O

Servers and workstations: use small padlocks to secure case covers where possible

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

X W A

4.12

O

Public workstations (or all computers in a very insecure environment): secure CPU, monitor, keyboard, and mouse to table/desk with hardware security cables/devices.

X W A

4.13

R

All servers: protect with UPS (400va or higher), preferably having auto shutdown software

X W A

4.14

R

Network equipment (hubs or switches): protect with UPS (250va or higher)

X W A

4.15

M

Router/firewall: protect with UPS (250va or higher)

X W A

5. Workstation Security

5.1

M

Configure ALL Workstations by RCERTE Baseline.

X W A

12/19/03
© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

5.2

M

Disable Auto login on all workstations

X W A

5.3

M

If individual patron local accounts are implemented, develop a written password policy with training documentation for patrons to follow. (LAPTOP COMPUTERS)

X W A

5.4

R

Remove unnecessary/unused files/programs from hard drive

X W A

5.5

R

Deny Users local administrator rights to workstation.

X W A

5.6

M

Install “managed” anti-virus software on all workstations

X W A

5.7

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

M

Update virus signatures on weekly schedule for stand alone machines.

X W A

5.8

M

Document software and security settings for future use in configuring new workstations

X W A

5.9

R

Schedule periodic download and installation of operating system patches or Schedule

X W A

5.10

M

Create and maintain current Emergency Repair Disks, and store in a controlled location

X W A

5.11

M

Use NSS NETOPS Support System to log and record maintenance problems and patron misuse of workstation

X W A

5.12

R

File all workstation component documentation (papers/manuals/disks) for use by service technicians

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

X W A

6. LAN/Domain Server Security

6.1

M

Configure all NT Servers with RCERTE Baseline.

X W A

6.2

R

Configure separate operating system and data partitions (both NTFS)

X W A

6.3

R

Mirror server drives (or implement RAID), if funding allows, for redundancy

X W A

6.4

M

Remove unnecessary services

X W A

6.5

M

Remove unnecessary files/programs

X W A

12/19/03
© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

6.6

M

Configure file system with proper file/folder access permissions (Specifically, restrict access to system files and executables)

X W A

6.7

R

Create alternative Administrator account (with new name) with full privileges

X W A

6.8

R

Disable default Administrator account

X W A

6.9

R

Use different account names and passwords for domain/server accounts than for local workstation accounts, or

X W A

6.10

M

Restrict access permissions for the Everyone group

X W A

6.11

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

M

Create appropriate user and group accounts

X W A

6.12

M

Set appropriate group access permissions

X W A

6.13

R

Document software and security settings for future use in reconfiguring servers

X W A

6.14

M

Develop and implement procedure for monitoring audit logs on a routine basis

X W A

6.15

R

Install software for the server's UPS that automatically shuts down the server

X W A

6.16

R

Implement procedures for file backups according to backup plan

X W A

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

6.17

R

Rotate one backup set offsite regularly

X W A

6.18

M

Schedule periodic download and installation of operating system patches

X W A

6.19

M

Create and maintain current Emergency Repair Disks, and store in a controlled location

X W A

6.20

R

Implement paper log to record maintenance problems, attempts at unauthorized access, and other server problems

X W A

6.21

M

File all server component documentation (papers/ manuals/disks) for use by service technicians

X W A

7. Network Equipment Security

12/19/03
© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

7.1

M

Set appropriate network management protocol (SNMP) passwords/community strings

X W A

7.2

M

Record and secure any password settings created by staff or contractors

7.3

M

Configure audit logs properly, if available

X W A

7.4

M

Implement procedure for monitoring audit logs

X W A

7.5

M

Schedule periodic installation of firmware updates

X W A

7.6

M

Document equipment settings for future use in reconfiguring equipment; make backup copy

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

of router configuration file, if possible, and store in secure location

X W A

7.7

M

File all network equipment documentation (papers/ manuals/disks) for use by service technicians

X W A

8. Router Security

8.1

R

Configure router to deny inbound access to unused ports (unless specific library services require them); for example, FTP on port 21, Telnet on port 23, etc.

X W A

8.2

M

Document router settings for future use in reconfiguring router; make backup copy of router configuration file, if possible, and store in secure location

X W A

8.3

M

Schedule periodic installation of firmware updates

X W A

8.4

M

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

File all router documentation (papers/ manuals/disks) for use by service technicians

X W A

9. Web Server Security

9.1

M

Follow Web server baseline from RCERTE

X W A

9.2

M

Document settings for future use in reconfiguring web server, and store in secure location

X W A

9.3

M

Implement procedure for creating/monitoring audit logs

X W A

9.4

R/M

Have PAO review for webpage's for content (Mandatory for Public web pages)

X W A

9.5

M

File web server documentation (papers/manuals/ disks) for use by service technicians

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

X W A

10. Virtual Private Network (VPN) Security

10.1

M

Supports RCERTE guidance for VPN

X W A

10.2

R

Document all server changes required to support the VPN

X W A

10.3

R

Document firewall configuration changes required to support the VPN

X W A

11. Software Currently used not on Army Approved software list.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003. As part of GIAC practical repository. Author retains full rights.