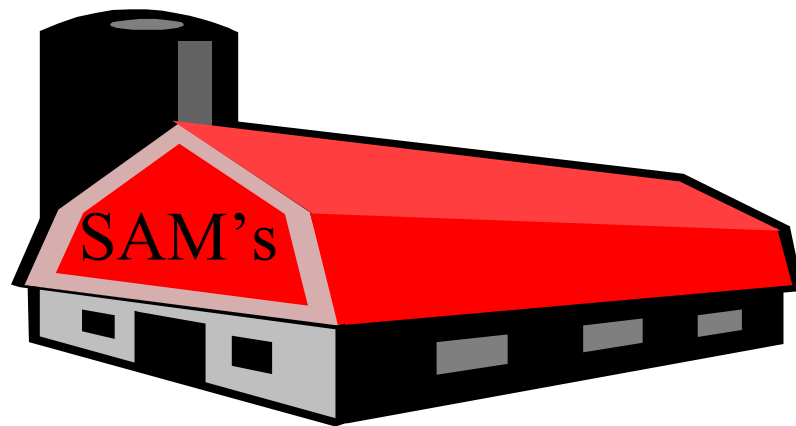












SAM's Paper Manufacturing Company Limited



Implementing Internet Access for a LAN

TABLE OF CONTENTS

Title Page	i
Table of Contents	Ii
INTRODUCTION	1
IMPLEMENTATION PLAN	3
 Background				
 Purpose				
 Project Life Cycle <ul style="list-style-type: none"> ○ Define ○ Discover ○ Design ○ Configure ○ Validate ○ Deploy 				
INTERNET SECURITY POLICY	9
 Security Policy				
 Purpose				
 Guidelines <ul style="list-style-type: none"> ○ Inappropriate Use of resources ○ Unauthorised Access ○ Physical Security ○ Backups ○ Anti-Virus Process ○ Firewall security Measures 				
INTERNET ACCEPTABLE USE POLICY		17
 Introduction				
 Policy Statements <ul style="list-style-type: none"> ○ Intellectual Property ○ Quality Control ○ Placement of Material ○ Improper Activities ○ E-Mail ○ Privacy ○ Public Representations ○ Comments ○ Access 				
 Request Procedures	21
 Consequences of Violations	22
ACKNOWLEDGEMENT FORM	23

INTRODUCTION

In our changing society as companies vie to stay alive; many have begun redefining their business strategies, so as to make accessibility to global and internal information easier for their employees. In order that business provide superior services than their competitors, Human Resource professionals strongly believe, that is closely linked to people's attitude about work, the evolution of employment-related laws and sociological trends. They must recognise the dynamic relationship between strategy, people, technology and the processes that drive organisations.

In so keeping, SAM's Paper Manufacturing Company Limited, in trying to manage the challenge facing today's organisations, change, given the rapid advances in technology, increased globalisation and the ever present need to assure quality service and contented workers, has proposed internet access for all workstation end users.

As organisations grow and develop, external and internal pressures result in changing needs. Systems and practices must be organised so that they continue to fit an organisation as its needs changes. As a result, the strategic and implementation plans are the overall blueprints that define how an organisation will deploy its capital resources, budgetary resources, and technological resources in pursuit of its goal.

In providing the Internet access, research would be carried out into the type of infrastructure that is required in providing an effective Internet access service to the employee. The types of infrastructure that need to be investigated are: -

Broadband Technology.

We would look specifically at Asymmetric Digital Subscribe Line (ADSL), which is a technology used by telephone companies to provide high band with services (faster internet and data speeds) to the home and business using existing telephone cabling infrastructure (See Appendix 1).

Routers

As its name implies the router serves as a routing switchboard. It connects two or more networks and forwards data packets between them.

Microsoft Exchange

This would facilitate internal and external e-mails

Monitoring and Managing Internet Access

Techniques and products for monitoring, controlling and managing Internet access, such as “Web use reporting” which is software used to monitor and report on how a workforce uses its access to websites.

In giving right of entry to an abundance of information, via the Internet, to all employees, management has taken into consideration the serious negative cost, which may occur, to both security and productivity of the employees. They have developed and put in place policies that take into consideration the use of firewalls to shield our Local Area Network (LAN) from unauthorised access and the use of Anti Virus products to prevent infection. And the configuration of gateways to restrict certain types of Internet traffic would reduce the possible negative affect because of the Internet access.

IMPLEMENTATION PLAN

PROPOSED INTERNET ACCESS FOR ALL WORKSTATIONS END USERS

BACKGROUND

The Internet, a public telecommunications service, was established as a cooperative effort providing worldwide networking services among educational institutions, government agencies and various commercial and non-profit organizations. High-speed networking technologies and developments have made the Internet a desirable source for expanding research interest and information dissemination and communication. The Internet has expanded to include government information, educational information systems, archives and business resources. The Internet also includes functions such as those for electronic mail (e-mail), remote computer networks, file transfers, World Wide Web (WWW) and wide area information servers.

PURPOSE

SAM's Paper Manufacturing Company Ltd is desirous of providing to all users of our workstations (computers) connected to our Local Area Network (LAN), meaningful access to the Internet for general web browsing throughout the World Wide Web, and the use of electronic mail (e-mail). This would result in:

1. Research opportunities for staff, which would result in a higher standard of product provided.
2. Monitoring what our company competitors are doing, so that we keep up to date with market facts.
3. Being able to communicate faster with our customers and suppliers, thereby bringing about greater efficiency in the company operations.

PROJECT LIFE CYCLE FOR IMPLEMENTING INTERNET ACCESS

The Project Manager works with the project team and the company owners in assessing and resolving risk and issues throughout the Project Life Cycle.

The following is an accelerated approach that ensures all critical success factors are covered. The stages are: -

1. DEFINE
2. DISCOVER
3. DESIGN
4. CONFIGURE
5. VALIDATE
6. DEPLOY

DEFINE

This initial phase identifies the stakeholders and determines the roles and responsibilities of the project team from the End Users who will be the staff to the Network Manager who would overlook the entire project.

DISCOVER

During the discover stage the project team identifies and documents the key issues before starting the design.

Research would be carried out into the type of infrastructure that is required in providing an effective Internet access service to the employee. The type infrastructure that would be looked at would be: -

DESIGN STAGE

The main objectives of the design stage are to design a solution that meets the needs of the owners and users' requirements and prepares the solution for training and tests. Deliverables are: -

- a. System Design Specifications show how users' requirements are met by the hardware, software screen definitions and business rules.
- b. User acceptance test Plan – identifies what criteria must be met and which test must run successfully before the user will accept the system.
- c. Design Review – Analyse the application architecture and design to ensure that they follow the best practices.

CONFIGURE STAGE

During the configure stage the IT department configures the system and prepares the organization for the deployment and support for Internet access for our Local Area Network (LAN). This stage includes:

Configure Software-	Software such as Microsoft Exchange, which would facilitate e-mails. Web Spy Analyser Standard, which is a powerful Internet monitoring and reporting tool.
Configuration Review-	Ensures that the configured application follows the best practices.
Application Support Plan-	The IT department would assist each officer in implementing the Internet Connection and Internet E-mail accounts.

VALIDATE STAGE

The Validate stage is a full-function of the new system. The delivery includes.

- a. Training- Implement the plan developed during the design stages. Prepares the users and run pilot testing for those who will use and maintain the system.
- b. Environment validation – Ensures that all hardware is installed and all software is loaded.

DEPLOY STAGE

The deployment stage brings all the elements of the implementation together from the production pilot to full development. During this stage the helpdesk is implemented, ongoing operational support is needed. The project team closes out the project, debriefing all stakeholders, archiving projects, artefacts and conducting user's satisfaction surveys.

PROJECT LIFE CYCLE

GHANT CHART

PROJECT TEAM

PROJECT MANAGER	IT DEPARTMENT
NETWORK SPECIALIST	CONSULTANT
SYSTEM ADMINISTRATOR	IT DEPARTMENT
END USER	MEMBER OF STAFF

BUDGET

DESCRIPTION	ESTIMATED COST
1. HARDWARE	US \$3200.00
2. SOFTWARE	US \$2800.00
3. TECHNICAL TRAINING	10 % OF SOFTWARE EXPENDITURE
4. END USER EDUCATION	US \$ 500.00 PER USER

INTERNET SECURITY POLICY

Security Policy

A policy is a documented high-level plan for organization-wide computer and information security. It provides a framework for making specific decisions, such as which defense mechanisms to use and how to configure services, and is the basis for developing secure programming guidelines and procedures for users and system administrators to follow. Because a security policy is a long-term document, the contents avoid technology-specific issues.

Purpose

The company is responsible for properly securing the data maintained in and transmitted by its computing systems and telecommunications network. In addition the company is committed to preventing the occurrence of inappropriate; unethical or unlawful behavior by any of its users.

.

GUIDELINES

The following are guidelines that should be followed in developing a security policy for the company, taking into the consideration the following.

- a) Firewalls
- b) The use of Antivirus products
- c) Configuration of Gateways

FIREWALLS

A firewall is not a single component; it is a strategy for protecting an organization's Internet-reachable resources. A firewall serves as the gatekeeper between the untrusted Internet and the more trusted internal networks.

- * They can block unwanted traffic.
- * They can direct incoming traffic to more trustworthy internal systems.
- * They hide vulnerable systems, which can't easily be secured from the Internet.
- * They can log traffic to and from the private network.
- * They can hide information like system names, network topology, network device types, and internal user ID's from the Internet.

Our policy guide

Firewall Administrator

A firewall, like any other network device, has to be managed by someone. Security policy should state who is responsible for managing the firewall. Two firewall administrators (one primary and secondary) shall be designated by the Chief Information Security Officer (or other manager,) and shall be responsible for the upkeep of the firewall. The primary administrator shall make changes to

the firewall and the secondary shall only do so in the absence of the former so that there is no simultaneous or contradictory access to the firewall.

Each firewall administrator shall provide their home phone number, pager number, cellular phone number and other numbers or codes in which they can be contacted when support is required.

Security of a site is crucial to the day-to-day business activity of an organization. It is therefore required that the administrator of the firewall have a sound understanding of network concepts and implementation. For instance, since most firewalls are TCP/IP based, a thorough understanding of this protocol is compulsory. An individual that is assigned the task of firewall administration must have a good hands-on experience with networking concepts, design, and implementation so that the firewall is configured correctly and administered properly. Firewall administrators should receive periodic training on the firewalls in use and in network security principals and practices.

User Accounts

Firewalls should never be used as general-purpose servers. The only user accounts on the firewall should be those of the firewall administrator and any backup administrators. In addition, only these administrators should have privileges for updating system executables or other system software. Only the firewall administrator and backup administrators will be given user accounts on the COMPANY firewall. Any modification of the firewall system software must be done by the firewall administrator or backup administrator and requires approval of the Network Services Manager

Data Backup

To support recovery after failure or natural disaster, a firewall like any other network host has to have some policy defining system backup. Data files as well as system configuration files need to have some backup plan in case of firewall failure. The firewall (system software, configuration data, database files, etc.) must be backed up daily, weekly, and monthly so that in case of system failure, data and configuration files can be recovered. Backup files should be stored securely on a read-only media so that data in storage is not over-written inadvertently and locked up so that the media is only accessible to the appropriate personnel. Another backup alternative would be to have another firewall configured as one already deployed and kept safely so that in case there is a failure of the current one, this backup firewall would simply be turned on and used as the firewall while the previous is undergoing a repair. At least one firewall shall be configured and reserved (not-in-use) so that in case of a firewall failure, this backup firewall can be switched in to protect the network

Trusted Networks

Trusted networks are defined as networks that share the same security policy or implement security controls and procedures that are provide an agreed upon set of common security services. Untrusted networks are those that do not implement such a common set of security controls, or where the level of security is unknown or unpredictable. The most secure policy is to only allow connection to trusted networks, as defined by an appropriate level of management. However, business needs may force temporary connections with business partners or remote sites that involve the use of untrusted networks.

THE USE OF ANTIVIRUS PRODUCTS

In terms of security, viruses are a very serious concern for computer users. According to the Information Week report, "Global Information Security 2002," 44 percent of respondents agree that computer viruses, worms, and Trojans are the number-one cited security incident. Thirty-one percent of respondents in an Information Security magazine 2002 survey cite malicious code as IT security's most important problem

Even if you have the best anti-virus software, and are running it optimally, there can still be problems. Software is just one part of the strategy system. Policies and procedures play an important role in the overall strategy

Updating Antivirus Solutions

Antivirus software is a critical component in protecting computers. Installing an effective antivirus solution is the first step, but keeping it up-to-date with the latest virus signatures is just as important. Without updated signatures, antivirus software is ineffective against new viruses.

Using and updating the latest antivirus software should protect computer files and e-mail. To help reduce the risk of a virus exploiting vulnerability, the administrator should ensure that the latest patches and updates are installed. For each new virus, antivirus vendors issue updates as inoculants against new viruses.

Anti-Virus Process

Don't open e-mail attachments from anyone you don't know, and be wary of those from people you do. Some viruses spread by mailing themselves to contacts in an infected computer's address book. If you have any doubts about the safety of an attachment, check with the source before opening it

Besides picking up a virus from an e-mail attachment, you can acquire a virus or worm from free content you download from a Web site or on a diskette someone shares with you. If your computer is not protected, once you download and install the program, the virus can spread.

Scanning For Viruses

It is important that virus protection scan be run periodically. It will find infected files automatically. It will advise whether it is able to remove viruses from every file or whether you should delete infected files.

It is important, that employees inform the IT department if they have been infected. After the viruses have been eradicated from your system, inform those that may have shared files that they may be at risk from infection.

USE OF GATEWAYS

Gateways are typically dedicated servers on a network. They can use a significant percentage of server's available bandwidth because they are doing resource intensive task such as protocol conversion.

Monitoring

The IT Administrator manages and monitor branch office gateways. Administrators can view the status of each branch office gateway; including what profile it is associated with. In addition, critical notifications about branch office gateways are also displayed that alert administrators to take appropriate action.

Efficient Management

Instead of the management server initiating communication with each of a thousand, branch office gateways individually. Dynamically addressed IP gateways periodically fetch their VPN/security policy from the management server. This reduces the load on the management server. Branch office gateways can be configured to fetch their VPN/security policy from one of multiple management servers in a single environment. This eliminates a single point of failure and ensures round the clock management availability.

A Comprehensive Logging Architecture

A comprehensive logging infrastructure to manage logs generated by hundreds of branch office gateways should be implemented. Logs can either be collected locally or be offloaded to a central log server at the corporate headquarters site. Multiple log servers may be deployed and if the designated primary log server becomes unavailable, logs can be automatically redirected to a secondary log server. Tracking logs from individual branch office gateways can become a

concern since their IP addresses change frequently. The management server assigns each branch office gateway a static, unique identifier. This makes it simple to track and analyse logs generated by an individual branch office gateway.

INTERNET ACCEPTABLE USE POLICY

OVERVIEW

It is the policy of SAM's Paper Manufacturing Company Ltd to allow and encourage the use of Internet services to support the accomplishment of the various missions of the company. Use of the Internet requires responsible judgment, supervisory discretion and compliance with applicable laws and regulations. Users must be aware of information technology security and other privacy concerns. Users must also be aware of and follow management directives for Internet usage.

Internet services provided by the company are to be used only for authorized purposes. The restrictions outlined below regarding Internet use during official working hours and employees should follow non-working hours.

SPECIFIC POLICY STATEMENTS

Intellectual Property of Others

You may not download or use material from the Internet or elsewhere in violation of software licenses, or the copyright trademark and patent laws. You may not install or use any software obtained over the Internet without written permission from the Systems Administrator.

All software downloaded via the Internet must be screened with virus detection software prior to being invoked. Whenever the provider of the software is not trusted, downloaded software should be tested on a stand-alone non-production machine. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine.

Quality Control

All information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate. Likewise, contacts made over the Internet should not be trusted with information unless a due diligence process has first been performed. This due diligence process also applies to the release of any internal information.

Placement of Material

Users must not place SAM's Paper Manufacturing Company Ltd material (software, internal memos,) on any publicly accessible Internet computer that supports anonymous File Transfer Protocol (FTP) or similar services, unless the Director of Marketing has first approved the posting of these materials. In more general terms, SAM's internal information should not be placed in any location, on the Internet, unless the persons who have access to that location have a legitimate reason.

Improper Activities.

You may not disseminate or knowingly receive harassing, sexually explicit, threatening or illegal information by use of Sam's facilities, including offensive jokes or cartoons. You may not use these facilities for personal or commercial advertisements, solicitations or promotions

E-Mail.

E-mail resembles speech in its speed and lack of formality. Unlike speech, e-mail leaves a record that is often retrievable even after the sender and recipient delete it. SAM's Manufacturing Co. Ltd strongly discourages storage of large numbers

of e-mail messages. Generally, you should promptly delete each e-mail message that you receive after you have read it. If you need to keep a message for longer than a week, save it to your hard disk, or print it out and save the paper copy. The Systems Administrator will regularly purge all messages in employee inboxes and all copies of sent messages that are older than 30 days.

Expectation of Privacy

Staff using our information systems and/or the Internet should realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, staff should not send information over the Internet if they consider it private.

At any time and without prior notice, SAM's management reserves the right to examine e-mail, personal file directories, and other information stored on our computers. This examination assures compliance with internal policies, supports the performance of internal investigations.

Public Representations

Staff may indicate their affiliation with our company in bulletin board discussions, chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for instance via an e-mail address. In either case, whenever staffs provides an affiliation, they must also clearly indicate the opinions expressed as their own, and not necessarily those of SAM's Paper Manufacturing company Ltd. All external representations on behalf of the company must first be cleared with the Director of Marketing or President. Additionally, to avoid libel problems, whenever any affiliation with our Network is included with an Internet message or posting, "flaming" or similar written attacks are strictly prohibited

Comments

Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, and related public postings on the Internet. If staffs aren't careful they may tip-off the competition that certain internal projects are underway. If a user is working on an unannounced product, a research & development project, or related confidential SAM matters, all related postings must be cleared with one's head of department prior to being placed in a public spot on the Internet.

Access

All users wishing to establish a connection via the Internet must authenticate themselves at a firewall before gaining access to our internal network. This authentication process must be done via a dynamic password system approved by the Director of Information Systems. This will prevent intruders from guessing passwords or from replaying a password captured via a wiretap.

REQUEST PROCEDURES

Internet access will be provided to users to support business activities and only as needed to perform their jobs.

As part of the Internet access request process, the employee is required to read this Internet Acceptable Use Policy. The user must then sign the statement that he/she understands and agrees to comply with the policy (located on the last page of this document). Users not complying with this policy could be subject to disciplinary action.

All users must review this policy and all changes annually, and a new Internet Acceptable Use Policy must then be signed.

CONSEQUENCES OF VIOLATION

Violations of the Internet Acceptable Use Policy will be documented and can lead to revocation of systems privileges and for disciplinary action up to and including termination. Additionally, the company may at its discretion seek legal remedies for damages incurred as a result of any violation. The company may also be required by law to report certain illegal activities to the proper enforcement agencies

Acknowledgment Form

By signing on the line below, I acknowledge that I have read, understood and agreed to comply with the foregoing Internet Acceptable Use Policy. I understand that, if I do not comply with the Internet Use Policy, I may be subject to discipline, including loss of access to SAM's Paper manufacturing Co. Ltd facilities and discharge from employment. I may also be subject to legal action against me for damages or indemnification.

Signature

Date

BIBLIOGRAPHY

www.knowledgestorm.com

www.netconcepts.com

www.itpapers.com

www.mobileplanet.com

www.pcworld.com

www.friedlnet.com

www.dtzresearch.com