

E-circular dt June 04, 2010



Rajive Chawla
President, FSIA



Sangeet Kr Gupta
Hon. Consultant, FSIA

I T Policies for FSIA Member Business units

Preface

During our interaction with the FSIA members, we have found that, on one hand most of them has started or already have a good level of computation. But a glaring gap is in the level of knowledge towards I T Security. MSME units specially are susceptible to risks, like Data loss, Virus Attack, Data leakage, Server collapse, poor I T infrastructure.

As a **FSIA initiative**, we have prepared a **set of I T policies**, especially for our members Some of these Discussion papers / I T policies we have made for FSIA members are on

1. Security Policies
2. Password Policy
3. Remote Access Policy
4. Internet Connection Policy
5. Approved Application Policy (unauthorized software not allowed)
6. Asset Control Policy (who controls which laptop)
7. Mobile Computer Policy
8. Computer Training Policy
9. Wireless Use Policy
10. Anti-Virus Policy
11. System Update Policy
12. User Privilege Policy
13. Application Implementation Policy (how to implement a software)
14. System Lockdown Policy
15. Server Monitoring Policy
16. IT Equipment Purchase and Failure Prevention Policy
17. Incident Response Plan
18. Intrusion Detection Policy
19. File Backup and Restore Policy
20. Network Documentation Policy
21. Server Documentation Policy
22. Network Scanning Policy
23. Network Risk Evaluation

We **shall circulate the same** to you in next two months, **as a part of our weekly E-circulars.**

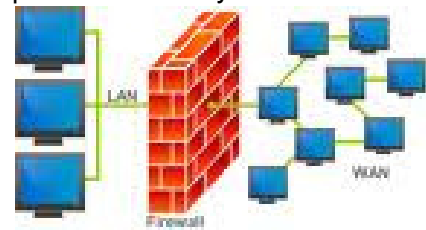
FSIA members are today already in the Powerful world of <u>Information Technology</u>		
	 <i>Future-ready</i>	
We at FSIA empower them to next secure level		

Internet Connection Policy

1.0 Overview

This internet connection policy has components of a user compliance policy and an internal IT policy. The user compliance section specifies how users are allowed to connect to the internet and provides for IT department approval of all connections to the internet or other private network. It **requires all connections** such as connections by modems or wireless media to a private network or the internet **be approved by the IT department** and what is typically required for approval such as the operation of a **firewall to protect the connection**.

This internet connection policy requires users **to use the internet for business only** and requires users to avoid going to malicious web sites which could compromise security. It informs the users that their internet activity may be logged and monitored and defines whether user activity on the network will be logged and to what extent. It specifies what system will be used to prevent unauthorized viewing of sites and what system will log internet usage activity. Defines whether a proxy server will be used for user internet access. It defines how the network will be protected to prevent users from going to malicious web sites.



2.0 Purpose This policy is designed to **protect** the organizational resources **against intrusion by malware** that may be brought into the network by users as they use the internet. It is also designed to prevent unauthorized and unprotected connections to the internet which may allow a host of unsafe content to enter the organizational network and compromise data integrity and system security across the entire network.

3.0 Physical Internet Connection : All physical internet connections or connections to other private networks shall be authorized and approved by the IT department. Most users will access



the internet through the connection provided for their office by the IT department. Any additional connections must be approved by the IT department. These additional connections include but are not limited to:

1. Modem connection from a computer or communication device which may allow a connection to the network.
2. Any multipurpose printing and FAX machines which have both a phone and network connection must be examined and approved for use by the IT department.
3. **Wireless access points** or devices with wireless capability **are not allowed** unless approved by the IT department. If any computers or other devices have wireless capability, the wireless capability must be turned off before connecting to the network unless it is approved for wireless operation by the IT department when connected to the network.

Any additional internet connections not provided by the IT department must be reviewed and approved by the IT department. Typically any additional connections from the organizational network to the internet or other private network will require.

1. An IT department approved firewall operating at all times and properly configured.
2. Some communications through the connection may require encryption subject to a review of data to be transmitted by the IT department.

4.0 Use of the Internet

1. All employee use of the internet shall be for business purposes only.
2. Employee use of the internet **may be monitored and logged including all sites visited**, the duration of the visits, amount of data downloaded, and types of data downloaded. The time of recorded activity may also be logged.
3. Employees are urged to use **caution when visiting unknown internet sites** and through user training set and keep their browser configured to IT approved standards in order to protect against infections of malware. Employees will be trained in the latest IT approved standards to protect against malware when appropriate.



5.0 Internet Control and Logging System:

A system will be required to operate on the network with the following capabilities:

1. The ability to prevent users from visiting inappropriate, pornographic, or dangerous web sites. It will have its database of categorized websites updated regularly.
2. The ability to log user internet activity including:
 1. Time of the internet activity.
 2. Duration of the activity.
 3. The website visited.
 4. Data and type of data downloaded
 5. Whether the system will cache web pages to increase the internet connection speed. This requires a proxy server.



Future-ready

3. The system should ideally, require a login ID or it will use the current network login to identify users.


The system used to prevent users from visiting inappropriate, pornographic, or dangerous web sites shall be specified (Say, CISCO, or SONICWALL) or any other Firewall. This same system will not require an additional login ID and will use Active Directory to identify internet users. The system shall be able to log the time of internet activity, duration of the activity, the website visited, any data downloaded and the type of data downloaded. The system will cache web pages.

6.0 Enforcement

Since improper use of mobile computers can bring in hostile software which may destroy the integrity of network resources and systems and the prevention of these events is critical to the security of the organization and all individuals, **employees that do not adhere to this policy** may be subject to **disciplinary action** up to and **including dismissal**.

Source: for text of other IT Security Policies, worth implementing at your company, Please do visit, www.finsys.co.in/ITpolicies.htm

For queries, suggestions and feedback , you can e-mail us at :

<p><u>Sangeet Kumar Gupta</u> FCA, ICWA, PGDMM, B.Com(Hons) Honorary Consultant, Faridabad Small Industries Association 93126-08426 groupmlg@eth.net Camp Off : SCF no 70, Sector-16A Market, Faridabad FSIA Off : FSIA Park, Opp. Plot No.23, Sector- 24, Faridabad-121005</p>	
--	--

Subscription

Please send your details, and request e-mail to groupmlg@eth.net

for Discontinuation of this E-mail

To discontinue receipt of e-mails from the author, please reply mentioning "Discontinue" in the Subject.

Notes & disclaimer

For private circulation. Intended for recipient only. This is only for personal information of the members. Based on information & interpretations available as on Friday, June 04, 2010. Please contact your Consultant / Chartered Accountant / counsel for his final opinion, if deemed fit.

For Trade Enquiries for Finsys ERP, you may contact : Finsys Infotech Limited : Faridabad (93112-78881 Puneet Gupta), Okhla office (Sanjay 9312136464), Gurgaon(Sunil Bedi – 9312608426), Kaleamb(Rajan – 93109-75518)

