



Standard Operating Procedure

SOP Name: Internet Security Policy	SOP No.: Aug-2012/ 1.1
Approved By : Management	Date of Issue : 01 st Aug 2012
Function Head : Head - IT	Effective Date : Immediate
CFO:	Next Review Due : 1 st April 2024
	Distribution : All employees, Notice Boards

1) Objective

Internet is a worldwide, publicity accessible network of interconnected computer networks. To provide guideline for acceptable usage of the Internet system and to reduce the potential risks involved in accessing the Internet.

2) Audience

This Internet policy applies to all users of **Gateway Distriparks Limited**. Internet browsing system including all permanent & temporary staff of the company, contract staff & business partners.

3) Policy Statements

For the effective and secured use of this facility, the following policy statements and clauses need to be adhered to.

A. Internet Browsing:

- i) All connections to the Internet shall pass through appropriate access control mechanism like firewall and proxy servers.
- ii) Internet browsing access shall be provided on a need to have basis only with written approval from the Functional Head + CFO / CEO + Head IT as per the approval format given in the Annexure.
- iii) All Functional Heads, CFO, CEO & CMD will have default access to the Internet.
- iv) Access to the Internet shall be granted only for HTTP, HTTPS and GRFL FTP Services. Any other request like 3rd party FTP access will require specific permission.
- v) Incoming traffic into the internal network via file downloads; file exchanges or file transfers (FTP Protocol) from the Internet of any software, executable files like .exe, .vbs, .scr etc., shall be prohibited by default.
- vi) Instant messaging solutions like, but not limited to MSN, Yahoo Messenger, Skype, G-talk, Facebook etc., are not allowed to be used due to the inherent security weakness associated with such systems.
- vii) Access to objectionable sites like hacking, pornography & other adult oriented sites, jokes, jobs, gambling, etc., is not allowed whether or not the access is blocked out by a content filtering solution.



Standard Operating Procedure

SOP Name: Internet Security Policy	SOP No.: Aug-2012/ 1.1
Approved By : Management	Date of Issue : 01 st Aug 2012
Function Head : Head - IT	Effective Date : Immediate
CFO:	Next Review Due : 1 st April 2024
	Distribution : All employees, Notice Boards

- viii) Any documents from the internet shall be scanned for viruses and malicious content.
- ix) Internet access from the servers / systems with critical data shall not be allowed.
- x) All access to the Internet may be logged and an adequate amount of information captured to assist with investigations and to detect misuse of access to the Internet.
- xi) **Gateway Distriparks Limited.**, can at any time, examine and / or monitor any Internet usage, including any email or instant messages, the content of any pages downloaded through any mechanism which record the user's usage of the Internet.
- xii) The company recognizes that there may be occasional personal use, but this shall not be excessive or unreasonable.
- xiii) The company is not responsible for any personal financial transactions such as banking, credit card, online trading etc., or consequent loss of personal information or incidental financial or other losses.

B. Usage office Internet Browsing System :

Users accessing the Internet through **Gateway Distriparks Limited.** must adhere to the following:

- i) Users shall use the system with responsibility and prudence, and shall not send any objectionable frivolous, libelous, offensive, prejudicial messages or indulge in harassment; whether racial, sexual or of any other kind or any illegal activity on the Internet, that may damage the company's business or image.
- ii) All existing company policies apply to users conduct on the Internet, especially (but not exclusively) those that deal with intellectual property protection, privacy, and misuse of company resources, information and data security and confidentiality.
- iii) The company respects all copy rights. No permanent or temporary employee, including any contractors' staff shall copy / download / install any pirated or unauthorized software in any company computer system. Any additional software required to perform company work, can be requested through the form enclosed as Annexure. Users shall be personally responsible for all consequences of installing and using any unauthorized or pirated software both to the company and any third parties against which the users will indemnify the company for all claims / damages for use of such unauthorized / pirated software. Internet facilities also must not be



Standard Operating Procedure

SOP Name: Internet Security Policy	SOP No.: Aug-2012/ 1.1
Approved By : Management	Date of Issue : 01 st Aug 2012
Function Head : Head - IT	Effective Date : Immediate
CFO:	Next Review Due : 1 st April 2024
	Distribution : All employees, Notice Boards

used to download, install or distribute pirated software or data, pornography, or other scandalous or frivolous material, to view or download audio, video or music material, games to obtain or purchase executable like *.exe or legal commitment by email on behalf of the company or play games against opponents over the Internet. Users must not attempt to bypass the security controls governing access to the internet.

- iv) Users must not utilize the Internet to disclose any company / business information without authorization.
- v) Users will make all efforts to ensure that internet bandwidth resources are not negatively affected.
- vi) Users must only access the Internet using software which has been approved by the company.
- vii) Internet facilities must not be used to deliberately propagate any virus, Trojan-horse or trap-door program codes.
- viii) Internet facilities must not be used to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another use.
- ix) Internet facilities must not be used to upload software licensed to the company or data owned or licensed by the company without authorization.
- x) Connection to the Internet through dial up modems from the systems (while connected to the LAN network) is strictly prohibited.
- xi) Internet access system should be restricted to authorized systems only and this system shall not be misused i.e. extending the system to other unauthorized systems or users.
- xii) The Internet user will bear in mind at all times that e-mail communication, however confidential, may have to be disclosed in court proceedings or investigations.

4) Violations to Policy:

Violations of this policy may subject the concerned personnel to disciplinary action, up to and including discharge from employment.



Standard Operating Procedure

SOP Name: Internet Security Policy	SOP No.: Aug-2012/ 1.1
Approved By : Management	Date of Issue : 01 st Aug 2012
Function Head : Head - IT	Effective Date : Immediate
CFO:	Next Review Due : 1 st April 2024
	Distribution : All employees, Notice Boards

5) **Withdrawal of Internet Facility :**

Immediately after resignation / termination of any permanent / temporary employee / contract staff or when such facilities are not deemed necessary for the employee, the concerned Functional Head / HR Head need to inform IT the date and time from the when the access to all IT systems including Internet and email should be withdrawn from the user. The intimation to IT Dept. should be given as per the Annexure.

5) **Acknowledgement**

Acknowledgement is required from all employees that they have read, understood and are bound by the SOP as per Annexure. This acknowledgement shall form part of the employees joining formalities which HR has to ensure.

6) **Violations to Policy:**

Violations of this policy may subject the concerned personnel to disciplinary action, up to and including discharge from employment.

6) **Exception Procedure:**

Exception to the above procedure, if requested through the concerned Functional Head shall be approved by CFO / CEO / CMD after considering impact of exception sought, the risk involved, and the compensating controls implemented to mitigate the risk.

7) **Here is a list of "dont's":**

Don't click on the "**Congratulations!** You are the Millionth Visitor! Click here to receive you FREE IPAD!" The end result will very disappointing and can mess your PC up

Don't click on the FREE; screen savers, simile central (free smiles), wall papers, freeze, mouse coursers, coupon printers, etc. Most of these will install Trojan Viruses or Malware (sometimes just poorly written software) that can cripple your computer or put a strangle hold on it.

Don't give your bank details to anyone you meet online. This includes your real name, address, bank A/c, PIN, net-banking password etc.

Don't fill out any survey, membership, or application forms asking for your personal information from an unsecured site.



Standard Operating Procedure

SOP Name: Internet Security Policy	SOP No.: Aug-2012/ 1.1
Approved By : Management	Date of Issue : 01 st Aug 2012
Function Head : Head - IT	Effective Date : Immediate
CFO:	Next Review Due : 1 st April 2024
	Distribution : All employees, Notice Boards

Don't disable any security settings, IT team have set such as antivirus, firewall, filtering, and site monitoring programs.

Don't open, reply or download attachments from spam or from unknown senders. These may contain viruses or other threats that can harm your computer.

Don't use free & downloadable peer-to-peer file sharing programs (e.g. Kazza & Grokster) ? These are spyware.

Don't download unnecessary software, songs or videos. These take up significant Internet bandwidth

Request / Withdrawal for Internet Access & Email Account		
Name	:	
Department	:	
Designation	:	
Reason for Access / Withdrawal	:	
Time Period	:	<input type="checkbox"/> Limited period of Access until : <input type="checkbox"/> Date of Withdrawal <input type="checkbox"/> On Going Access
Requirement	:	Internet
		<input type="checkbox"/> Access to all
		<input type="checkbox"/> HTTP / HTTPS
		<input type="checkbox"/> FTP
		Email
		<input type="checkbox"/> Internal Mail
		<input type="checkbox"/> External Mail
		<input type="checkbox"/> Chat / VOIP

Approval By : _____
Date: _____

_____ Head IT
Date: _____

Withdrawal Request By : _____
Head
Date: _____

_____ HR
Date: _____



Standard Operating Procedure

SOP Name: Internet Security Policy	SOP No.: Aug-2012/ 1.1
Approved By : Management	Date of Issue : 01 st Aug 2012
Function Head : Head - IT	Effective Date : Immediate
CFO:	Next Review Due : 1 st April 2024
	Distribution : All employees, Notice Boards

<u>For IT use</u>	<input type="checkbox"/> Access withdrawn & ID blocked	<input type="checkbox"/> Id's Created & Access Configured
Email ID:		
Internet ID:		
	Created By	Approved By
	Date:	Date:

Acknowledgement

I acknowledge that I have read and understood the Email security SOP issue dated 31st May 2012 containing Internet / Email Policy of the **Gateway Distriparks Limited**. I understand the requirement from me to comply with the SOP and the consequences of non-compliance.

Signature	
Name	
Designation	
Department	
Location	
Date	