Acceptable Usage Policy for IT Systems

Document Control

Document Title	Acceptable Usage Policy
Document ID	Wockhardt_ISMS_POL_AU_V1.0
Document Version	1.00
Effective Date	18th January 2018

Document Details

Description	Name	Designation	Date	Signature
Prepared by	Biju John	General Manager - IT	15.01.2018	
Reviewed by	Prem Singh	President Global –HR	18.1.2018	
Approved by	Venkat Iyer	Group Global CIO	18/01/2018	

Document Revision Control

Version	Description	Change Author	Change Approver	Revision Date

Document Distribution List

S. No	Name	Organization	Purpose
1	Chief Information Officer	Wockhardt India	Internal Compliance
2	IT HODs	Wockhardt India	Internal Compliance
3	MIP team (Internal Audit)	Wockhardt India	Internal Compliance
4	Employees	Wockhardt India	Internal Compliance
5	Human Resource	Wockhardt India	Internal Compliance

Table of Contents

1 Introduction

Information Technology (IT) team is committed to protecting Wockhardt's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly by implementing various security controls at all levels of the IT infrastructure.

Internet / Intranet related systems, including but not limited to computer equipment, software, operating systems, storage media & networks providing electronic mail and web browsing, etc., are the property of Wockhardt. These systems are to be used for business purposes in serving the interests of the company and our customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Wockhardt employee and affiliates who deals with information and / or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

The intention of publishing an Acceptable Use Policy is not to impose restrictions that are contrary to Wockhardt' s established culture of openness, trust and integrity.

2 Objective

The purpose of this policy is to outline the acceptable use of computing equipment at Wockhardt Ltd and its group Companies. These rules are in place to protect the employee and Wockhardt. Inappropriate use exposes Wockhardt to risks such as virus attacks, compromise of network systems and services and legal issues.

3 Policy Statement

Acceptable Use IT Policy is a User centric policy that covers basic user related information security awareness and best practices to be followed while conducting daily business operations.

4 Scope

The Policy applies to

1. All employees of Wockhardt– permanent, temporary, trainees, employees on probation and retainers.
2. Employees of suppliers/ service providers / service receivers / other contractors
3. All equipment owned or hired by Wockhardt.

5 Abbreviation

1.	CIO	- Chief Information Officer
2.	HOD	- Head of Department
3.	IT	- Information Technology
4.	MIP	- Management Improvement Process
5.	NDA	- Non Disclosure Agreement
6.	LTO	- Linear Tape Open

6 Responsibility

Designation	Role
Chief Information Officer (CIO)	• Owns the policy
HOD / Designee	• Ensure that this policy is effectively implemented. • Enforce the policy
Human Resource	• Create information security awareness among the user.
Employees	• Adhere to the policy

7 Policy

7.1 End Computing Devices

1. A Desktop/Thin Client shall be provided to the user by the IT department based on the user's role.
2. A Laptop shall be allocated, based on their designation (DGM and above) or based on user's role, duly approved by the Head of the Department. An existing laptop within the department shall be allocated if there is one in Stock; else HR/HOD shall seek Capex approval from MD/Chairman.
3. Desktop/thin client/Laptop installation, troubleshooting and maintenance shall be undertaken only by the IT department.
4. USB Ports shall be in block mode (Read/Write) for all types of USB based storage devices.
5. All CD/DVD drives shall be in block mode. (Read/Write)
6. Read and Write access to USB Drive and CD / DVD facility shall be provided as an exception, for business purposes only. The request shall be validated by the respective HOD, who shall then forward the request to MIP department for purpose of compliance. MIP shall assess the business requirement and conduct an impact analysis. Post the assessment, the approval shall be forwarded to the Corporate Information Technology department for provisioning the access. MIP department reserves the right to reject the request with valid reasons. The HOD shall ensure the proper usage of this facility and remains accountable for its proper use.

7. Users shall not attempt to install any software on any IT resource.
8. If the user requires software for business purpose, same shall be approved by the HOD and then shall log a request with IT, provide details of business need, software functionality details and necessary CAPEX / OPEX approval.
9. Users shall not try to access any PC other than the one allocated to them or any other IT equipment, unless authorized to do so by the IT department.
10. User shall not share Desktop / Laptop / Thin Client with anyone unless specifically told by IT department.
11. IT Resources shall not be moved from one location to another within the premise / between offices without prior approval from IT.
12. Every system must have a password protected screen saver that automatically activates after 10 minutes of system inactivity. If your system does not have this feature, report this to local IT personnel
13. Usage of the IT resources shall be monitored by the IT department / Top Management in case there is a need for the same.
14. All the data, information and any other material found on a computer or any other IT resource shall be the sole property of Wockhardt. Users shall not copy / store / transmit information in any form outside of Wockhardt if it is not for business purpose.
15. Users shall not use IT resources for personal gain including commercial / social / cultural purposes.
16. Users shall not copy / store / transmit any form of obscene, vulgar, inappropriate material, jokes, pictures, chain mails or any other material, which are not meant for the business activities of Wockhardt.
17. Users are personally responsible for protecting the data and information on the IT resources being used by them. Users shall not switch off any tools / services from the IT resources set up by the IT department like anti-virus, firewalls etc.
18. If the users observe anything unusual in the IT resources, they shall immediately bring the same to the notice of the IT department with full details.
19. Users shall switch-off their desktops / thin client / laptops at the end of the day and also when they are away from their work station / cabin for a longer period of time.
20. Intimation of employee resignation shall be forwarded by the concerned Function/Department /Business Head to HR & IT on the same day without fail so as to facilitate the onward processes.
21. Resigned employee shall surrender all IT resources issued to them to the IT department and get a clearance from the IT department to this effect. A documented clearance certificate or via online portal (https://wire.wockhardt.com => click E-Exit link) from the IT department shall be the required documents by the HR Department to clear the terminal dues of the user.

7.2 Laptop Security

1. User shall be responsible for protecting the laptop from physical damages, loss or theft
2. User shall backup the laptop data on their respective network drive before travelling for an extended period of time.

3. Use a cable lock, wherever possible, to restrict physical movement of the laptop.
4. When travelling – Be aware of your surrounding and do not leave the laptop unattended in public place.
5. When travelling by car –Lock the laptop in the car's boot and never leave the laptop in a vehicle where it is clearly visible to passers-by.
6. While staying in a hotel - If the laptop is kept in the hotel room anchor it securely to a metal post or fixed object. When not in the room, consider locking the laptop up in the hotel's safe. (Make sure a receipt is given).
7. Ensure laptop security when attending conventions and conferences
8. Users shall immediately inform their respective HOD and IT Department in case of loss or theft of their Laptop. They shall also take further prompt action as desired by Wockhardt including lodging complaints with Police / any other authority. Maintain all data on laptop in encrypted form as far as practicable.

7.3 Mobile Devices - Mobile Phones / Tabs

1. Users provided with Mobile devices by Wockhardt shall protect it from damage, loss or theft. Always use a lock screen which every smartphone and tablet provide. Users shall be solely responsible to Wockhardt for any expenses incurred by Wockhardt on repairs due to damage caused by any of their actions / inactions.
2. Users shall immediately inform Wockhardt in case of loss of theft of their mobile phones provided by Wockhardt. They shall also take further prompt action as desired by Wockhardt including lodging complaints with Police / any other authority.
3. Users shall be responsible for any action against them for any misuse / unauthorized use of the mobile phones.
4. User shall not respond to a text messages from stranger to avoid getting victimized by lottery or such kind of scams and to avoid visiting the malicious links received from those messages.
5. Users shall not use the public USB charging stations that are found in airports, malls or at any public place to avoid "Juice Jacking" attack in which same charging cable can be used to extract/load data/malicious software into the mobile. Always use mobile charger/own power bank for charging.
6. Even in respect of mobile phones provided by Wockhardt to its employees, Wockhardt shall not be responsible for any misuse / unauthorized use of such mobile phones. Users shall be solely responsible for any action against them for misuse / unauthorized use of such mobile phone.
7. Users shall exercise caution while communicating with people over the phone since there exist a possibility of the recipient preserving / reproducing (including in a Court) / transmitting to others the conversations on phones. On the other hand, the users / Wockhardt may have no record of any of these communications. It is recommended that any commitments made on behalf of Wockhardt and requires to be documented then the same may be communicated via emails and retain such emails so that the same are available for future references.

7.4 Storage Device Security

1. All removable media including CD / DVD / USB / LTO / External hard disk shall be labelled with the contents
2. Media carrying confidential information shall not be left unattended and shall be stored with appropriate physical security. The Storage media shall be encrypted as far as practical.

7.5 Password Security

Users are responsible and accountable for all use and security of the electronic resources they own or use, including but not limited to computer account(s), passwords, personal computer(s), electronic data, and network access. Users shall protect the confidentiality of their accounts / User IDs / Passwords through good password management and shall not allow anyone else to operate. Each new user must have their unique login id and a secret password issued by the IT department prior to being permitted to use Wockhardt's computers and network resources.

7.5.1 Password construction

Users shall choose passwords which are difficult to guess. Some of the guidelines for password constructions are-

1. Do not use own name, short form of own name, own initials, names of family, friends, co-workers or popular characters
2. Do not use personal information like date-of-birth, address, telephone numbers, brand of vehicle, favourites, department / group name etc.
3. Do not use password which are same as User ID or Log in ID
4. Do not use common words found in English dictionary.
5. Do not use word or number patterns like aaabbb, qwerty, zyxwvuts, 12345, 123321,etc
6. Do not use any of the above preceded or followed by a digit (e.g., secret1, 1secret)
7. Strong passwords have a minimum length of 8 characters and can be constructed through a mix of numerals (1,2,3 etc.), special characters (!,@,#,$ etc.) and capital letters (A,B,C etc.).
8. One way to create complex but easy to remember passwords is to take a known word or phrase and convert it using numerals, special characters and capital letters. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

7.5.2 Password Protection

1. Users shall not share their passwords with anyone including colleagues and IT staff. Users shall also not ask others to share their passwords. All passwords shall be treated as sensitive and confidential information.
2. The system shall force the user to change their password once in 60 (sixty) days. The system shall alert the user via email about the need to change their password seven days in advance before the actual expiry of the password. User shall change their password before the expiry.

3. Users shall ensure that they are not observed while entering password nor observe others while inputting the password into the system. If user suspects that someone has compromised their account, they shall change the password immediately.
4. User shall take utmost care not to save passwords in browser especially while using cyber cafes.
5. User shall not maintain a written copy in the form of sticky notes or in diary or any other paper form of their passwords. Users shall not display .password on a sticky note or on whiteboard in their workstation area.
6. Users shall change their password regularly. While some applications shall enforce password change and complexity on users automatically, it may not be feasible to enforce it for all accounts and for all applications. Users shall change their passwords under any of the following circumstances-
   a. As enforced by system (applications and operating system)
   b. After you suspect that a password has been compromised.
7. All operating systems as applicable shall be configured to lock out the accounts after 5 bad password attempts. User shall report if the login account is locked out before 5 attempts. If the account gets locked out before 5 attempts, this could be because someone else or mobile active sync was trying the password.
8. After the user changes his Windows passwords, make sure that the new password is updated on their mobile devices for email syncing. Failing to do so will result in account lock out.
9. Users who have been authorized to use the VPN tokens or private keys shall safeguard them carefully.
10. Wherever applicable use two factor authentication methods like hard token, soft token, PIN via email or mobile to enhance the security level further.

7.6 Network and File Services

1. Users can access their files on the servers / applications by authenticating with their user IDs only. All users shall note that they shall be solely responsible to Wockhardt for any misuse of their password/s by anyone inside / outside Wockhardt.
2. Users shall always keep all business related documents on the File server.
3. Users shall not directly share with other users their files / directories on the server. If sharing of the files / directories is necessary for coordination / effective functioning, he/she shall seek written permission from their supervisor, giving full details of the files / directories, name/s of person/s and reasons for sharing such files / directories.
4. The Contents of Common_to_all, drive on the File Server shall be deleted automatically every 24 hours. This common folder shall not be used for storage of official sensitive information. However, if certain information is required to be internally transmitted within or across departments, employees shall ensure that the files are password protected and copied / viewed immediately by the intended recipient.
5. The Contents of the Scan Folder on Common drive on the File Server shall be deleted automatically every 24 hours as applicable. Users shall remove sensitive information immediately from the scan folder.

7.7 E-mail Services

1. Users shall not use the e-mail service facility to send / receive / store / transmit any e-mails which are obscene, vulgar, inappropriate, jokes, pictures, chain mail, Phishing letters or any such material, in any form. If any such mails are received by the users, they shall immediately delete the same from their computer system.
2. Users shall not give out their corporate email id on any web sites, other than the ones relevant to Wockhardt' s business requirement. If there is a need to register, provide an alternate external email address. This will help to keep your official mailbox free from spam.
3. Users shall not use scanned hand rendered signatures in emails.
4. Users shall not auto-forward their emails to any external / personal mailbox.
5. Emails shall be marked only to intended recipients on a need-to-know/need-to-do basis. Unconnected departments in relation to the subject/matter shall not be marked mails without reason.
6. Personal/Private email ids shall not be marked in Bcc copy for any official mails except for business purposes. If required, the emails shall be forwarded to the required person separately on a need-to-know/need-to-do basis.
7. Users shall not send any computer programs as attachments.
8. Users shall not directly open any web links embedded in a body of the email without checking the authenticity of the web link.
9. If the User receives an email with file attachments from unknown sender, the same shall be deleted without opening the attachment. Repeated occurrence shall be informed to the IT department
10. Users shall not use the e-mail service for spamming. Spamming includes, but is not limited to:
    a. Bulk sending of unsolicited messages or the sending of unsolicited emails.
    b. Posting any kind of content to any kind of news groups or e-mail groups like Yahoo groups/ Usenet.
    c. E-mail harassment of other Internet User/s including but not limited to, transmitting any threatening, libellous or obscene material, or material of any nature which could be deemed to be offensive and against the interests of Wockhardt.
11. Users shall not use any third-party private e-mail service from within Wockhardt offices, unless specifically allowed to do so by their HOD and duly approved by the MIP department
12. Users accessing e-mails from outside Wockhardt through the web shall ensure that they do not leave the browser open after accessing their emails and shall immediately log-off once their e-mail usage is over. Users shall take utmost care not save their password in browser while accessing email from public shared computer facilities like internet cafes, hotels, airport etc.
13. Users shall ensure that the laptop/Desktop/Smart phones used by them to access their mails via browser have an updated antivirus installed on their system.
14. Users shall not access other User's mail files / directories.

15. In order for an immediate superior to be able to access the e-mails of a User (including a user who has left Wockhardt), he / she shall take the approval of the HOD and HR department before forwarding the request to the IT department
16. Users shall not send any confidential data outside Wockhardt without the written approval of their HOD.
17. The terms of non-disclosure and confidentiality agreements shall be strictly complied with.
18. Use of Email facilities for incidental (limited) personal use is permitted as long as it does not impact business needs and is not a violation of Wockhardt policies.
19. Users have no right of personal privacy in any matter stored in, created, received or sent over the electronic communication systems. Wockhardt reserve right to access and inspect information transmitted and/or stored on Desktop and/or on any other devices and media.

7.8 Internet Services

1. Wockhardt employees as per their functional requirement have been provided with Internet access for business purpose only.
2. Users shall not download any shareware or freeware or any other software from the Internet.
3. User shall not use Wi-Fi that user doesn't own and which is available without password.
4. Users shall use the Internet service judiciously in connection with official work.
5. Users shall not download audio or video files onto Wockhardt network since this may cause congestion in the internet traffic.
6. Users shall not attempt to access pornography, violence, gaming, gambling, jokes, hate, racism, hacking, chat sites.
7. Before entering any personal information or doing any financial transactions users shall look for the green lock icon (i.e. secure web link 'https') present before the URL (website address).
8. No employee shall represent Wockhardt on Internet discussion forum and public forum without special authentication.
9. Private Emails (Gmail, Rediffmail, Hotmail, Yahoo mail, etc.), social networking and stock trading sites shall be blocked.
10. There shall be restrictions on certain sites being accessed from within Wockhardt. As an exception to the above, any website which needs access for business purpose, the user shall approach the HOD for approval. The request shall be validated by the respective HOD, who shall then forward the request to MIP department for purpose of compliance. MIP shall assess the business requirement, and conduct an impact analysis. Post this assessment, the request approval shall be forwarded to the Corporate Information Technology department for provisioning the access. MIP department reserves the right to reject the request with valid reasons. The HOD shall ensure the proper usage of this facility.
11. Users shall not use the Internet service to enter or attempt to enter any network in an unauthorized manner.

12. Use of chat software to the user shall be permitted only if approved by the user's department head and MIP department. Users shall use all chat facilities for Official purposes only.
13. The IT Department reserves the right to monitor all Internet traffic to ensure that no inappropriate, abusive or unethical use of the Internet facility is being carried out.
14. All history along with caches and cookies should be deleted from the browser on definite intervals to ensure the deletions of the malicious cookies and unwanted redirections to malicious websites.
15. Use of internet facilities for incidental (limited) personal use is permitted as long as it does not impact business needs and is not a violation of Wockhardt policies.

7.9 Document Security

1. Each Department Head shall identify and classify information / data pertaining to his / her function in line with the information classification policy. The same shall be communicated to the concerned respective team members, selectively. The Department Head shall ensure/induct appropriate measures/systems for its administration, usage, central storage and dissemination of all such sensitive information, thus classified.
2. All documents containing sensitive information shall be marked as "confidential" both in electronic and print format. Care shall be taken to ensure confidentiality while these documents are transmitted over email, other communication media or during printing and photocopying of documents.
3. Confidential documents shall not be kept unattended in the user's work area, near printers, fax machines or photocopiers and shall be stored with appropriate physical security.
4. Users shall adopt a clean desk policy in order to reduce the risks of unauthorized access, loss of and damage to information outside business hours or when left unattended.
5. Unnecessary documents / papers shall be destroyed using shredder machine and in case of non-availability of a shredder machine, every sheet shall be torn off manually in such a manner that no one can read / access information from such documents. Expired and bad storage media shall be destroyed before disposal.
6. Users shall keep a backup copy of important documents. The backup shall be taken on the backup media.
7. The media shall be protected from environmental hazards like heat, electromagnetic fields, dust, smoke, etc.
8. Sensitive / Confidential information shall not be discussed in the presence of external personnel who do not 'need to know' that information.
9. Patient's Personal Health information (PHI) shall not be shared with anyone who does not need to have access to the same.
10. Employee's Personally Identifiable information (PII) shall not be shared with anyone unless there is a need for the same.
11. Sensitive information may get revealed unintentionally due to unsafe practices. Care shall be exercised in the following scenarios to protect sensitive information-
    a. Reading confidential documents in public places

b. Discussing confidential information in public places
c. Working on laptops in public places
d. Answering to queries over phone to unverified persons
e. Providing information to vendors / suppliers
f. Leaving confidential information unattended

7.10 Confidential Agreement

1. The employee shall not, either during or after his / her employment, divulge or utilize any confidential information belonging to Wockhardt. This includes and is not limited to confidential information on;
   a. Processes
   b. Business Projects – Completed, current and expected
   c. IT infrastructure setup

   This may be gained during their employment. They shall take all reasonable precautions to keep all such information confidential.
2. Except as may be necessary for the purpose of their duties, the employee shall not, without the consent of their managers, make copies of Wockhardt's confidential information
3. Employees shall not
   a. access
   b. read
   c. copy
   d. divulge to others
   e. delete or destroy

   Any type of information not in his scope of work, belonging to other employees without the consent and signed approval of appropriate authority.
4. Employees who have been assigned Wockhardt's assets e.g. laptops, PDA, mobile for internal or external use shall comply with the statements of confidentiality mentioned above.
5. If on the termination of his / her employment, the employee is in possession of any originals or copies of confidential documents, he / she shall return the same to Wockhardt.
6. Employees with access to privileged information shall not divulge that information even to other employees or third party.
7. Failure of any employee to comply with the confidentiality required above shall give the right to take action as deemed appropriate, including legal action.

7.11 Information Exchange Security

1. All departments shall ensure that a NDA (Non-Disclosure Agreement) is signed before sharing any sensitive information to third party or any vendor. Department head written approval is required prior to sharing such information is mandatory.
2. A list of all the documents shared to third party or vendor as part of any project shall be maintained and signed by both the parties.

3. All documents shall be shared in non-editable format (in PDF) with password protection.
4. Documents shall be shared using Internal FTP Server (xfiles.wockhardt.com) with password protection and FTP link validity. By default the FTP link shall be valid for 7 days only. If there is a need to extend the validity beyond 7 days, same shall be approved by the HOD. However the validity cannot be extended beyond one month. Files stored on the FTP server will be removed after the validity period.
5. Exchange of sensitive information through email shall be secured (e.g. Word/Excel/PDF can be password protected)
6. Each department head is required to identify and classify information/data pertaining to his/her function into sensitive information/data. Department head with the help of IT department shall ensure/induct appropriate measures for administration, usage, central storage and dissemination of all such sensitive information.
7. Critical and confidential information exchanged between departments shall be secured. The recipient shall ensure that the information is not modified.
8. For remote access requirement to the Wockhardt network, user needs to contact IT department.

7.12 Clear Desk and Clear Screen

The following controls shall be implemented by all the users

1. Paper used during work hours shall be either locked away in the lockers or be shredded at the end of the day.
2. Paper and computer media shall be stored in suitable locked cabinets and/or other forms of secured area when not in use and after office hours.
3. Sensitive or critical business information shall be locked away (ideally in a fire-resistant safe or cabinet) when not required, especially when the office is vacated.
4. Desktops, thin clients, laptops or any other computing device shall not be left logged on when unattended. Wherever applicable, these computing devices shall be timeout if the system is inactive for more than 10 minutes.
5. Photocopiers shall be protected from unauthorized use.
6. Sensitive or classified information, when printed, shall be cleared from printers immediately, prints of such documents shall not be left unattended on the printer/fax machine. Printer and fax machine shall be manned while printing confidential documents. Wherever applicable, secure print option (Password Protected) shall be used to print Sensitive information.
7. Computer screens shall be kept clear of sensitive information when unattended.

7.13 Antivirus

1. All computing device shall have antivirus software installed on it.
2. Users shall ensure that the Anti-virus software is active on their system (Check for the antivirus icon status). If the anti-virus software is not active, user shall inform the IT and get the same rectified immediately.

3. The antivirus computer local agent automatically updates the virus signatures from the antivirus orchestration Server. If the user finds that the antivirus is not getting updated from server, user shall inform the IT and get the same rectified immediately. (Right click on the antivirus icon and find the status of the update).
4. All the files received from the external sources shall be scanned for virus before opening the same. This includes files in removable media like CD's / DVD's, external hard disks, pen drives and email attachments.
5. Any virus detection shall be informed to the IT team immediately.

7.14 Social Engineering

User shall not share any official information on call or on internet chat or personally with any stranger.

7.15 Physical Security

1. Users shall ensure that the visitors are escorted within the workstation area if required
2. Visitors shall not be allowed to access Data Center, network communication rooms, UPS rooms, etc.
3. Piggyback is not allowed in access controlled area.
4. All servers shall be hosted in the server room only and the access to the same shall be restricted.

7.16 Procurement and Asset Management Services

1. All purchases of IT resources shall be done / coordinated by the IT department.
2. Requirement requests for a new Computer / IT resource / IT service shall be referred to the IT department at least four weeks in advance.
3. All original software and licenses shall always be maintained in custody of the IT department.
4. The IT department shall procure appropriate IT resources as per the user's requirement.

7.17 Incident Reporting

Users shall report any security incidents identified on the IT systems to the IT department / HOD / Designee. Incidents could result in un-authorized access, disclosure of information, corruption of information or denial of service. Users can follow these guidelines to identify an incident:

1. Abnormal system resource usage - If the CPU, memory utilization on a system is very high compared to normal usage in past, the system could have been compromised. Attackers use compromised systems for spreading viruses or attacking other machines leading to high resource utilization.
2. Abnormal, slow response for application - Users may experience extremely slow response times if the application servers or the network has been compromised and is being used for malicious purposes. Virus or worm outbreak could lead to network congestion that

would in-turn cause application responses to be slow and unstable. Report instances where the response is extremely slow as compared to past usage.

3. Data corruption - If the user finds that data or files stored on the desktop has been either deleted or modified without their knowledge this could be sign of a compromised system.
4. Change in desktops - If the desktop configuration looks different from normal days in terms of applications installed, screen savers or icons on the screen or the desktop is misbehaving in terms of opening up new screen / applications without any input command and these changes have been done without the user's knowledge, it could be an indication of someone else using your desktop.
5. Changes in passwords - Users shall report if they find their passwords have been changed or their account has been locked without their knowledge. Any changes in user passwords could be indications of system compromise. A user shall also raise an alarm in case they suspect someone else of using their account.
6. Virus infection - Users shall report any virus or worm that infected one or more hosts at their site. However viruses or worms that are detected and cleaned by anti-virus software need not be reported; only those which are not getting cleaned and infecting the system needs to be reported.
7. Changes in applications – If the applications accessed looks different from its normal appearances or the user's level of access in the application appears to have been modified (either increased access or decreased access); the application may have been compromised.
8. Security weakness detected - If any weakness has been detected in the applications accessed that can cause unauthorized access or modification or lead of any kind of compromise, such weaknesses shall be reported to prevent any loss.
9. Violation by others - If a user encounters any instance of security violations committed by others like running of malicious tools, trying to break into system or committing IT frauds or thefts, copyright or license agreement violations, they shall report the same. Care shall be taken not to report minor or unsubstantiated activities.
10. Phishing attacks - In case of receipt of a phishing mail, the employee shall immediately report the matter by email / telephone to Information Security team. Employee shall forward the original email sent by phisher to the Information Security team.

While reporting incidents users shall provide their identity and contact details for effective follow up. Anonymous reporting may or may not be addressed at the discretion of the information security team.

7.18 Security Violations

Certain categories of activities, which have potential to harm, or actually harms the information assets are defined as security violations and are strictly prohibited. All security violations shall entail disciplinary action. A security violation is any attempt to breach the security of applications, network and IT devices, whether or not it results in actual damage or financial loss. The following are examples of security violations-:

1. Connecting modems to machines without approval
2. Connecting wireless devices such as smart phones, memory sticks, USB devices
3. Unauthorized use of remote access software
4. Use of peer to peer applications
5. Use of Instant messaging applications
6. Introducing virus
7. Sniffing on the network
8. Doing password guessing
9. Computer impersonation
10. Erasing or modifying data on central systems without authority
11. Downloading or transmitting objectionable content (through e-mail or Internet)
12. Running scans or attack tools
13. Bypassing access control mechanisms
14. Exploiting any system vulnerability
15. Installing or distributing unlicensed software
16. Vandalism
17. Computer fraud or theft
18. Unofficial audio video files

7.19 Spot Checking

1. All third parties / contractors/ vendors / visitors shall cooperate while the security guard conduct a spot check (e.g. checking the laptop bags at the gate / badge)

7.20 Copyrights and Licenses

1. All IT Users at Wockhardt shall respect copyrights and licenses to software, published and unpublished documents, and any other legally protected digital information.

7.20.1 Copying

1. Any material protected by copyright shall not be copied except as specifically stipulated by the owner of the copyright or otherwise permitted by copyright law. Protected material may not be copied into, from, or by any user or group, except pursuant to a valid license or as otherwise permitted by copyright law.

7.20.2 Copyrights

1. All copyrighted information (text, images, icons, programs, video, audio, etc.) retrieved from computer or network resources shall be used in conformance with applicable copyright and other law. Copied material shall be properly attributed. Plagiarism of digital information is subject to the same sanctions as apply to plagiarism in any other media.

7.20.3 Ownership

1. Wockhardt has the right to own all electronic documents, reports, worksheets and email messages that are generated on Wockhardt' s network

7.21 Broad Summary "Do's and Don'ts" for Information Security

7.21.1 DO's:

a) **DO** Understand that Information Security and Confidentiality is Everyone's responsibility.

b) **DO** Ensure that new and existing staff members, who are your responsibility, read and understand this policy.

c) **DO** Report immediately any threat to, or breach of information security to CIO.

d) **DO** Feel free to contact local IT personal for further guidance or advice on information security.

e) **DO** Ensure that the equipment on your desk, in your office or work area and which you use as part of your job is kept as secure as possible.

f) **DO** Ensure that all visitors are supervised and do not gain access to restricted areas (e.g. Data Communications Room, Server Room) without the prior approval of the CIO.

g) **DO** Ensure that any equipment taken off-site is booked in and out through a document which is authorized by Department Head and IT location senior persons or designee.

h) **DO** Ensure that 'condemned' electronic equipment which having memory is returned to the local IT before disposal.

i) **DO** Ensure that data saved on local disks of PC's, laptops or notebook computers are backed up regularly on official media which should not be taken out of official premises without permission from Departmental Head. Preferably, store any official data on Network File server.

j) **DO** Store Pen drives, CD/DVD and other storage media in a secure environment.

k) **DO** Keep your password(s) secure and change them regularly (as per Wockhardt Password Policy). Password and Login information should be Confidential.

l) **DO** 'Lock' or Log out of your PC or terminal when leaving your desk or workstation ensure that your PC screensaver is password protected.

m) **DO** Log out and turn off your Desktop and Laptop before leaving the premises.

n) **DO** Dispose of printouts containing personally identifiable data securely (via confidential waste or shred them).

o) **DO** Desktop and/or Laptop Usage should be only for official business purpose.

p) **DO** User is responsible for protection of Information stored on his Desktop and/ or Laptop.

q) **DO** Data backup and archiving only on official media.

7.21.2 DON'Ts:

a) **DON'T** piggyback (enter any access controlled area by following another authorized person) through access control doors. Kindly flash your access control card to the card reader for identification, even if the door is opened by other Authorized personnel.

b) **DON'T** Assume that the responsibility for information security rests with someone else.

c) **DON'T** Position or leave computer equipment where it may be easily damaged or stolen.

d) **DON'T** Leave visitors unattended in areas where computer equipment is kept or used.

e) **DON'T** Allow visitors to enter secure areas (e.g. Server Room) without the prior approval of a member of the local IT person or CIO or respective Admin Department.

f) **DON'T** Utilize the Auto Forward facility in the Out of Office Assistant to forward e-mails to a Home Internet E-Mail Account.

g) **DON'T** Take computer equipment off-site without obtaining authorization.

h) **DON'T** Leave computer equipment taken off-site unattended in public places, in your car or any other location where theft or damage may occur.

i) **DON'T** Ignore any potential or actual breaches of security or confidentiality.

j) **DON'T** Install USB modems onto computers or connect your PC to any external data communications network without obtaining authorization and the necessary security software (secure login).

k) **DON'T** Forget to make backup copies of data held on internal disks (e.g. Systems Hard Drive) by copying it to network drive.

l) **DON'T** Leave Pen drives, CD/DVD or print outs on your desk unattended.

m) **DON'T** Throw Pen drives, CD/DVD away unless they have been reformatted. If in doubt ask the IT Department for assistance.

n) **DON'T** Exchange data via Pen drives, CD/DVD, FTP or any other media with any external organization without first consulting/approval of the Departmental Head/MIP/CIO.

o) **DON'T** Reveal your password to anyone else.

p) **DON'T** Provide access to applications to other users.

q) **DON'T** Leave your PC or terminal logged-on when not in use or when you leave your desk/workstation.

r) **DON'T** Leave your Laptop PC in 'suspended' mode while transporting from one location to another. The system must be turned off whilst being transported.

s) **DON'T** Share identifiable patient information with those unauthorized to see it.

t) **DON'T** Give out any information about individuals over the phone unless you are absolutely sure they are authorized to receive it.

u) **DON'T** Copy application software unless specifically advised to do so by the IT Department.

v) **DON'T** Use and/ or load unofficial software on Desktop/Laptop/Tabs.

w) **DON'T** Share Laptop issued for official purpose with friends or with other family members.

x) **DON'T** Transfer and/ or archive business information on personal storage media and/ or devices.

y) **DON'T** Misuse and/ or mishandle officially issued Laptop and/or Desktop.

7.22 Compliance

7.22.1 Information Technology Act, 2000

1. Under Sections 65, 66 and 67, the following offences are punishable with imprisonment ranging from 3 years to 5 years and also with fines ranging from Rs. 50,000/- to Rs.2,00,000/-.
    a. Tampering with computer sourced documents (Section 65): This includes concealing, destroying or altering any computer source code / program / system / network.

b. Hacking with computer systems (Section 66): This includes destroying or deleting or altering any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means.

c. Publishing information which is obscene in electronic form (Section 67): This includes publishing or transmitting any material which is lascivious* or appeals to the prurient** interest

2. All employees shall carefully note that the foregoing acts are punishable offences under law. If any such acts are committed by any employee of Wockhardt, Wockhardt shall have no alternative but to report the incident with full details to the law enforcing agencies including the police.
3. In addition to reporting the incident to the law enforcing agencies, Wockhardt reserves the right to take necessary disciplinary action against an erring employee, which may include summary dismissal without notice depending upon the gravity of the offence.

Dictionary meaning : * feeling or showing an open or offensive sexual desire

: ** having too much interest in sexual matters

7.23 Disciplinary action by Wockhardt

1. This policy shall be strictly followed by all employees of Wockhardt. Any breach, whether intentional or unintentional, shall be viewed seriously by Wockhardt. Wockhardt reserves the right to take necessary disciplinary action against the employee in breach of this policy. Depending upon the seriousness of the breach, Wockhardt may in its sole discretion, decide upon the type of disciplinary action which may include summary dismissal without notice.

Make security a habit!!!