PUNJAB CHEMICALS & CROP PROTECTION LIMITED

User accounts and passwords

- All users must have one access account created by Syaters administrator to access the network.
- Computer must be password protected and only System administrator/HOD other than the user should know this account and password.
- ERP users must have separate users account and password for each user for protection of software and data.
- Users are responsible for the security of their password which they not divulge, even to colleagues.

Email & Internet

- The email & Internet facilities provided to staff should not be used for political, business or commercial purpose not related to the organization. Never use this facility to send illegal or inappropriate material.
- Staff should minimize the number of messages in their inbox to ensure maximum efficiency of the delivery system. Access to the Internet is provided for business purpose related to the company only.
- Staff should not make inappropriate use of their access to the Internet. They must not use the system to access pornographic, illegal or other improper material Staff should not subscribe to chat rooms, dating agency, messaging services or other online subscription Internet sites unless they pertain to work duties. Programs, including screen savers, must not be downloaded from the Internet.
- Abuse of Internet access will be dealt with severely relative to seriousness.
- Company retains the right to access and View all emails sent and received by the email system and Internet usage. This right is exercised solely through IT department and they shall report to the Management on the matter on regular basis.

Monitoring use: The Company reserves the right to monitor any and all of its IT facilities to determine if a user is acting unlawfully or violating this policy or any other company policy or rule. Such monitoring may include, Individual login sessions, the Internet sites visited by users and the content of electronic communications. Monitoring may be done with or without prior notice to the user.

Compliance with legal requirements: To avoid breaches of any statutory, criminal or civil obligations and of any security requirements. The design, operation and use of IT systems may be subject to statutory and contractual security requirements.

- Control of proprietary software copying
- Safeguarding of organizational data and records
- Data protection
- Prevention of misuse of IT facilities
- Compliance with security policy

Compliance on user's part: Users of companies IT facilities are responsible for adhering to the provisions of this policy. The company may take remedial action and suspend user access with or without prior notice in response to suspected breaches of this policy. Breaches by users or staff that constitute misconduct will he considered seriously by the company.

Implementation and Review: All Heads of departments will be responsible for the implementation of this policy in their respective areas of responsibility.

- The IT department shall be responsible for regular reviewing of policy.
- The IT department shall have the authority to issue from time to time the guidelines due to changes in the law or changes in the practices of the company
- The IT department shall have the authority to amend any guidelines issued

PUNJAB CHEMICALS & CROP PROTECTION LIMITED

Anti-Virus Policy

In order to protect the organizations resources against Intrusion by viruses and other malware, it is mandatory to install anti-virus software on every computer. It is the responsibility of IT department to Implement effective Anti-Virus software and to ensure and draft the strategy that how often a virus scan is to be done, how often updates are to be done, what programs will be used to detect, prevent, and remove malware programs.

The organization will use a single anti-virus product for anti-virus protection. The

Following minimum requirements shall remain in force.

1. The anti-virus product shall be operated in real time on all servers and client computers. The product shall be configured for real time protection.

2. The anti-virus library definitions shall be updated at least once per day.

3. Anti-virus scans shall be done a minimum of once per week on all user controlled workstations and servers.

4. The installation of anti-virus software on all machines is the responsibility of IT department.

5. Remote users and users of portable machines will assist, the upgrade of anti-virus software in accordance with specified mechanisms agreed with the IT department, eg. Internet update.

6. Staff should virus-scan all media (including floppy disk, zip disk, CDs, etc.) before use.

7. On detection of a virus staff should notify the IT department who will provide assistance.

8. No one should be able to stop anti-virus definition updates and anti-virus scans except for System Administrators.

User accounts and passwords

- All users must have one access account created by System administrator to access the network.

Computer must be password protected and only System administrator/HOD other than the user should know this account and password. ERP users must have separate users account and password for each user for

PUNJAB CHEMICALS & CROP PROTECTION LIMITED

Network Policy

Network management, administration and maintenance within PCCPL are the responsibility of IT Department Access to and usage of the Servers and administrative passwords are restricted to authorised staff only.

Remote Access: The remote access policy defines standards for connecting to the PCCPL network and security standards for computers that are allowed to connect to the PCCPL network.

This remote access policy specifies how remote users can connect to the main PCCPL network and the requirements for each of their systems before they are allowed to connect. This will specify:

1. The anti-virus program remote users must use and how often it must be updated.

2. What personal firewalls they are required to run.

3. Other protection against Spyware or other Malware.

The remote access policy defines the methods users can use to connect remotely such as dial up or VPN. This is to prevent damage to the organizational at work or computer systems and to prevent compromise or loss of data.

Approval: Any remote access using either dial-in, VPN, or any other remote access to the PCCPL network must be reviewed and approved by the appropriate supervisor. All employees by default will have account settings to deny remote access. Only upon approval will the account settings be changed to allow remote access.

1. The anti-virus product as approved by IT department is required to be operating

On the computer at all times in real time protection mode.

a. The anti-virus product shall be operated in real time on the computer. The product shall be configured for real time protection.

b. The anti-virus library definitions shall be updated at least once per week.

c. Anti-virus scans shall be done a minimum of once per week.

d. No one should be able to stop anti-virus definition updates and anti-virus scans except for System Administrators.

2. The computer must be protected by a firewall at all times when it is connected to the Internet.

Network Risk Evaluation: The IT department must list all network security risks and help the reader determine where the greatest threats on their network. The reader should list their opinion of the severity of each throat and how common they believe it to be on their network. Then the number of times per month that this threat has materialized should be listed. There are several main items to consider when listing throats and their ability to threaten the network. These include:

1. The threat such as virus, spyware, worms, computer hack and others.

2. How common or often the threat is realized on the network.

3. Hostile software through email borne viruses into user computers & server.

4. Unauthorized user installed programs - Users bringing their own programs into the network on disks or memory sticks

5. Hostile software through user web browser due to wrong configuration and/or software vulnerability.
6. Throats to server from user computers.

7. Attacks to the server through vulnerable applications.

8. Attacks through vulnerabilities in services such as web server and mail services.

9. Attacks through operating system vulnerabilities,

10. Attacks due to wrong configuration of services or system such as allowing relaying on mail server allowing spam to be sent, not including down internet Information Server (IIS) leaving it vulnerable, or leaving default administrator accounts with default passwords set.

Documentation: The network structure and configuration shall be documented and provide the following information:

1. IP addresses of all devices on the network with static IP & Dynamic IP addresses.

2. Server documentation on all servers as outlined in the Server Documentation "documents.

3. Network drawings showing:

a. The locations and IP addresses of all hubs, switches, modems, routers, and

b. The various security zones on the network and devices that control access firewalls on the network.

c. The locations of every network drop and the associated switch and port on the switch supplying that connection.

d. The interrelationship between all network devices showing lines running between the network devices.

e. All subnets on the network and their relationships including the range of IP addresses on all subnets and net mask information.

f. All wide area network (WAN) information including network devices connecting them and IP addresses of connecting devices.

3. Configuration information on all network devices including:

a. Switches

b. Routers

c. Firewalls

d. WI-FI, AP, RF.

4. Configuration shall include but not be limited to:

a. IP Address

b. Netmask

c. Default gateway

d. DNS server IP addresses for primary and secondary DNS servers.

5. Network connection information including:

a. Type of connection to the internet or other WAN Including T1, T2, frame relay.

b. Provider of Internet/WAN connection and contact Information for service and support.

c. Configuration information including netmask, network ID, and gateway.

d. Physical location of where the cabling enters the building and circuit number.

e. Lease duration time.

The IT head or any person authorized by IT head shall have full access to all network documentation. The IT networking staff shall have the ability to read and modify network documentation. The authorized persons shall have access to read and change network documentation but those not designated with change access cannot change it.

Change Notification: The help desk staff, server administration staff, application developer staff, and IT management shall be notified when network changes are made including.

1. Reboot of a network device including switches, routers, and firewalls.

2. Changes of rules or configuration of a network device including switches, routers, and firewalls.

3. Upgrades to any software on any network device.

4. Additions of any software on any network device. 1. Changes to any servers which perform significant network functions whether

Configuration or upgrade changes are made Notification shall be through email to designated groups of people.

Documentation Review: The Network System Administrator shall ensure that Network documentation is kept current by performing a monthly review of documentation. The Fresh service Help desk requests within the last month should be reviewed to help determine whether any network changes were made. Also any current or completed projects affecting network settings should be reviewed to determine whether there were any network changes made to support the project.

Storage Locations: Network documentation shall be kept either in written form or electronic form in a minimum of two places. It should be kept at different locations preferably Company's own premises. Information in both facilities should be updated monthly at the time of the documentation review.