Contents

Prepared By	Verified By	Approved By
Head-IT	Jt. Managing Director	CMD

1 Introduction

The Information Technology Policy Manual is prepared as a policy guideline for ensuring safe and securemanagement of information and information assets across all facilities of the company.

Information security is defined as the protection of information and systems from unauthorized access, use,disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

The policy guideline covers management of security of compute, storage, database and network infrastructure. This also includes management of application-specific software like SAP, tools and platforms.

It also outlines the roles and responsibilities of users, IT managers, Head of the departments and themanagement.

This policy guideline shall be implemented in conjunctions with the relevant procedures and work instructions asrequired.

Prepared By:-	Reviewed By:-	Approved By:-

1.1 Scope

The careful implementation of information security controls is vital to protecting an organization's information assets as well as its reputation, legal position, personnel, and other tangible or intangible assets.

This policy is applicable to all the IT infrastructure including but not limited to computer systems, servers and network equipment that are used for acquiring, processing and storing data at CRRPL

This policy covers all aspects of IT Infrastructure Management

- **Infrastructure Security – Physical and Logical Security**
- **Data/Information Security**

This policy includes any computing devices brought into the organization or connected to the organizational network using any connection method. This includes but not limited to following items:

- **Desktop Computer System Servers**
- **Printers & Scanners**
- **Laptops**
- **Switches, Modem, Routers, Firewall**
- **UPS systems**
- **CD's, Blue tooth, Pen Drives, Detachable hard disk, CD writers etc.**

1.2 Glossary

1. Information security is defined as the protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality,integrity, and availability.

2. **Confidentiality** - "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" A loss of confidentiality is theunauthorized disclosure of information.

3. **Integrity** - "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" A loss of integrity is the unauthorizedmodification or destruction of information.

4. **Availability** - "Ensuring timely and reliable access to and use of information…"A loss of availabilityis the disruption of access to or use of information or an information system.

5. **Application Servers** - An application server is a type of server designed to install, operate and hostapplications and associated services for end users, IT services and organizations

6. **Database Servers** - A database server is a server which uses a database application like SQL Server that provides database services to other computer programs or to computers, as defined by the client–server model.

7. **Network Servers** – A network server is a computer, a device or a program that is dedicated tomanaging network resources

8. **Storage Servers** - A server is a computer, a device or a program that is dedicated to managingnetwork resources

9. **Desktops** - A desktop computer (or desktop PC) is a computer that is designed to stay in a singlelocation. It may be a tower (also known as a system unit) or an all-in-one machine,

10. **Laptops** - Portable and compact personal computer with the same capabilities as a desktop computer.

11. **Network Routers** - A router is a networking device that forwards data packets between computernetworks and perform the traffic directing functions on the Internet.

12. **Network Switches** - A network switch (also called switching hub, bridging hub, officially MACbridge) is networking hardware that connects devices on a computer network by using packet switching to receive, and forward data to the destination device.
13. **LAN** - A local area network is a computer network that interconnects computers within a limited area,within the premises of CRRPL Limited.

14. **PBXs** - A PBX (private branch exchange) is a telephone system within an enterprise that switches voice, data and video calls between enterprise users on local lines while allowing all users to share acertain number of external phone lines.

15. **Firewalls** - A firewall is software used to maintain the security of a private network. There are three basic types of firewalls that are used by companies to protect their data & devices to keep destructiveelements out of network, viz. Packet Filters, Stateful Inspection and Proxy Server Firewalls

16. **Encryption / Decryption** - Encryption is the conversion of data into a form, called a cipher, that cannot be understood by unauthorized people. Decryption is the process of converting encrypted databack into its original form, so it can be understood.

17. **Authentication, Authorization and Accounting Servers** - Authentication, authorization, andaccounting (AAA) is a term for a framework for intelligently controlling access to computer resources, enforcing policies and auditing usage.

18. **Application Software** - Application software is a term which is used for software created for a specific purpose. It is generally a program or collection of programs used by end users.

19. **Tools** - A program that is employed in the development, repair, or enhancement of other programs orof hardware.

20. **Platforms** - A computing platform or digital platform is the environment in which a piece of softwareis executed. It may be the hardware or the operating system, even a web browser and associated application programming interfaces, or other underlying software, as long as the program code is executed with it.

2 Desktop and Laptop Security Policy

1. Each employee shall be assigned desktops or laptops based on the individual roles and responsibilities

2. Employees shall be assigned roles as per business needs.

3. Access to the application software, tools, platforms, internet and email servers shall be provided based on
assigned roles.

4. All laptops and desktops shall have the privacy protection disabled on the allotted computer systems as allthe systems are monitored for security purposes.

5. All laptops and desktops shall have standard and approved configurations, application software, tools andplatforms installed on them.

   5.1. Standard Wall-Paper activation shall be disabled
   5.2. CD-ROM Drive shall be disabled

6. Employees shall not install software from external sources.

7. For any specific software, tool or platform needed for business purposes the employees shall get the necessary approvals from the designated approving authorities. The IT/EDP team shall install and configure thesoftware, tool or platforms as per the approval.
8. Employees shall not install unlicensed software on computers.
9. Employees shall log off and switch off their workstations and printers before leaving for the day.
10. Email and Internet Access activity shall be monitored for security purposes.
11. When an employee exits the company, he/she shall surrender the computer/laptop/storage devices with allthe user credentials.
12. IT department shall take backup of the compute/storage resource of the exited employee in encrypted andsecure Storage Servers.

3 Employee Guidelines

1. Every employee shall undergo the CRRPL. IT Security Training
2. Employees shall not disclose any company data directly or through emails and messages withoutauthorization
3. Employees shall not use computing power for the personal gain or in a manner inconsistent with' theprofessional conduct like downloading inappropriate content from internet, sending chain or mass mailers with no legitimate business purpose. This shall be considered as a severe security and integrity violation.
4. Employees shall not leave their computers and laptops unattended.
5. Employees shall not disclose or share user access and authorization credentials like username andpassword with anyone.
6. Employees shall use strong password as per the password policy/procedure.
7. Employees shall promptly report any security violations to IT team
8. Employees shall not leave printers unattended when printing restricted information.
9. Employees shall secure all printed data and electronic records. In case of any loss, employee shallimmediately inform their managers.
10. Disposal of unused, printed data shall be according to the data security policy.

11. Waste copies of company restricted information that is generated in the course of copying /printingshall be destroyed, preferably by a paper shredder.

12. Employees shall not intentionally develop or use programs which' disrupt other computer users orwhich access private or restricted portions of the system and/or damage the software or hardware components of the system.

13. Computer users shall ensure that they do "not use programs or utilities, which interfere with othercomputer users, or which modify normally protected or restricted portions of the system or user accounts.

14. Computer users shall not use network links for any use other than permitted in this policy.

4 Server Management Policy

4.1 Scope:

This policy is applicable for all types of Servers

- Database Servers

4.2 Physical Security

1. All servers would be installed in designated, physically isolated and secured Server Rooms
2. Physical Access to these Server Rooms shall be for only authorized system administration personnelonly

4.3 Logical Security

1. By default access to applications and data in servers is denied
2. Servers shall be placed in a secure domain through network and server firewalls
3. Access to the applications and data on servers shall be approved and authorized based on the responsibilities.

4.3.1 Database Servers:

1. Data in Database servers shall be protected using SQL grants to applications and designated adminroles assigned to authorized and approved individuals
2. Data shall be stored in Database Servers shall be in encrypted form.

4.3.2 Storage Servers

1. The storage on the Storage Servers shall be partitioned based on
   1.1. Application
   1.2. Departments
   1.3. Record types
2. Access to Data in Storage Servers shall be given to designated roles assigned to authorized and approved individuals.
3. Data shall be stored in Storage Servers, the critical data are kept in encrypted form

4.3.3 Attach, Detach, Movement or Removal of Servers

1. Servers shall be attached to or detached from the company's network or moved or removed from the normal location with the approval and authorization of IT Department.
2. IT department shall follow the requisite process of backup, archive of the data and application images before moving or removing the Servers from the company network
3. Any personal or vendor/supplier equipment shall be denied connection by default.
4. If personal or vendor/supplier need to connected for business purpose then they shall be provided temporary access and authorization based on assignment of approved role.

4.3.4 Server Power Supply

1. All Servers shall have regulated power supply with voltage range 210V to 230V
2. Power supply shall be monitored by the maintenance department.
3. Earthing shall be checked periodically and maintained as per the standards.
4. All the servers shall be connected to UPS with specified battery backup.

4.3.5 Retirement of Servers

1. Servers would be retired when the hardware or software operating platform is declared obsolete or end of life.
2. Servers and the Application Platforms that store and process electronic data and records that are mandatory as per regulatory requirement shall be preserved and maintained in secured storage cabinets.
3. The preserved servers and application platforms shall be periodically verified.

4.3.6 Installation and commissioning

1. In case of new server, IT department shall create and maintain the Server Connectivity Diagram
2. The Power and Data cables shall be labeled and numbered to ease the identification of all connectivity.
3. The power and data cables shall be separated appropriately.

5 Application Specific Security

5.1 Application Access

1. Access to the applications such as SAP, HRMS etc would be provided based on the roles and responsibilities
2. Users shall be assigned different roles based on the authorization and approval process by designated

5.2 Software security

1. The application software, tools and platforms on Servers, Laptops and Desktops shall be installed /uninstalled only by designated persons who are assigned the system administration role.
2. The IT department shall maintain a list of application software, tools and platforms that have been approved by the business. This list shall be reviewed and updated after approvals periodically as perbusiness needs
3. Any additional application software, tools and platforms needed for the business shall be approved bythe designated authorities and shall be installed temporarily by designated persons who are assigned the system administration role.

5.3 Software Service Management

1. All critical application software, tools and platforms would be under AMC and/or need based services from respectiveVendors/Suppliers
2. Any software malfunctioning shall be reported immediately to the IT department.
3. While reporting, user shall provide the System error message displayed on the screen and theapplications used.
4. In case of critical error that could affect other systems, the affected computer shall be immediatelyisolated from the company network.
5. The reported errors shall be rectified along with the vendor/supplier as per service level agreements
6. The IT department shall resolve all the errors within 24 hours

5.4 Maintenance of Original Software

1. The IT department shall create and maintain the inventory of the original and licensed application software, tools and platforms as approved by the business.
2. The media -USB and others for original license software shall be maintained in secured storage and the back up of the images shall be available on Storage Servers.

5.5 Software Change Control

1. Any changes arising out of upgrades/updates, security patches and obsolescence in applicationsoftware, tools and platforms shall follow the Software Change Control procedure.
2. The movement, removal, installation, un-installation, configuration of application software, tools andplatforms shall be done by the IT department with the approval and authorization as per roles and responsibilities
3. IT Department shall maintain the change history. The back-up of the software and data of previousversions shall be retained and archived on the Storage Servers.

6 Network Security Policy

6.1 Secure Network Architecture

1. Network Devices, including Firewall and Boundary Devices shall be configured to monitor andcontrol communication at the external and key internal boundaries.
2. ACLs, Inbound and Outbound routing shall be configured to restrict the flow of information to/fromcritical information systems.
3. Networks connecting critical information assets are physically and logically segregated and placed insecure groups.
4. All the network policies are approved and reviewed by the IT expert and management.
5. Redundancy shall be built in to all the network connections to ensure availability

6.2 Secure Access Points

1. IT department shall place limited number of access points and switches to access the internal andexternal access points.
2. The access points and switches will be placed in security groups segregated based on networkdomains
3. The administration and control of access points and switches would be authorized based roles and responsibilities
4. All communication through access points and switches is through

6.3 Access to external networks

1. Access to external networks – internet and inter-facility networks shall be given through controlled environment.
2. Administration and configuration of controlled environment, switches and firewalls shall be done byusers assign approved roles as per the roles and responsibilities
3. Roles approved for internet access shall be assigned to users as per the roles and responsibilities
4. Firewalls shall be configured to block and alert un-approved access, intrusion and denial of service(DDOS) attacks

7 Data Security Policy

7.1 Data exchange

1. The data and file exchange between company units, consultants, partners and customers shall be donethrough secure and encrypted connections.
2. The data and file exchange in shared folders shall be protected user name and password.
3. The data/files shared folders shall be stored in encrypted form

7.2 Media Security Policy

1. Computer media being sent outside the organization
   - 1.1. The media transit between facilities and to customer locations shall be approved and authorized asper roles and responsibilities
   - 1.2. The data on the media is sent in encrypted form with a shared key security approach
   - 1.3. The gate pass, sender and receiver records shall be maintained by respective departments for audittrail of the media.
   - 1.4. The media shall be sent in locked cases and standard packing with the keys available only to thesender and receiver
   - 1.5. All previous contents on the media shall be backed up and erased if the media is to be disposed offrom the organization.

2. Disposal of corrupt media
   - 2.1. Any media that is corrupt and can no longer be used shall be disposed securely and safely.
   - 2.2. Corrupt CD/USB shall be returned to IT department for destroying.
   - 2.3. All corrupt CD/USB shall be destroyed by breaking them into two parts and Tapes by cutting thetape at various places.

3. Media handling & storage
   - 3.1. Media shall be handled as per the technical specifications given thereon.
   - 3.2. Any media, when inserted in the drive or ejected from the drive shall be done with utmost care.
   - 3.3. All media shall be stored in a safe and secure environment in accordance with manufacturer'sspecifications.

8 Access Control Policy

Access of information and business processes shall be strictly controlled on the basis of business requirements

8.1 Role based Access

The Role based access are provided and the list of approved roles and the authorization – create, read,update, delete, execute privileges for each role.

8.2 Company-wide and Site-specific Approval Matrix

The Company-wide and Site-specific approval details provides the list of employees who requests, reviews and approvesthe assignment of roles to specific users

8.3 Password Policy

1. All employees shall be assigned individual windows login, passwords and access rights fordesktop/Laptop.

2. Naming Conventions
   2.1. Email ID shall be provide as directed by the management like department e.g. marketing shall be marketing@chopraretec.com. For employees at senior level, email id can be given by name.
3. Each employee granted access to the windows shall be assigned a user name and Password.
4. Password Rules
   4.1. Users shall keep the password confidential and shall not share the same with fellow-employees orexternal people.
   4.2. Users shall always keep the password confidential. Disciplinary action shall be taken fordisclosing the password.
   4.3. Password shall be a combination of alphabets and numerals and shall not be user's name, surname,family member's names etc.
   4.4. Password shall be minimum 8 characters long.
   4.5. User shall change password at first log-on and thereafter periodically. Password shall be changedat least once 90 days.
5. All user logins and related access shall be disabled on the last working day of the employee.
6. External users or Third party access.
   6.1. For access of information by third party, proper justification / permission shall be obtained from theapproving authority.
   6.2. Temporary Login ID/internet E-mail account shall be given to them if their stay is for a longerduration. The ID shall be disabled/deleted immediately when they leave.

8.4 Special restrictions for computers/desktops connected to measuring and test equipment

1. CD-ROM Drive shall be disabled
2. CD Burning software shall be uninstalled and disabled

8.5 Virus Protection Policy

1. Installed Anti-virus software
   1.1. IT services shall install approved Anti-Virus software on all PCs, Laptops and Servers.
   1.2. USB pen drives, Mass storage devices, external media, wherever permitted, shall be scannedautomatically as soon as they are inserted in to the computer systems.
   1.3. If there are any threats identified, the files shall be cleaned. If the cleaning fails the user shall informthe IT department immediately.
   1.4. The system shall be configured to either quarantine or delete infected files.
2. IT department shall install the Anti-Virus Software updates as soon as they are received from the vendor.
3. In case of new virus attack, it shall be brought to the notice of IT Department immediately.
   3.1. Affected PC, Laptop, Server etc. shall be immediately isolated from LAN and its usage stopped.
   3.2. IT department shall contact anti-virus company for remediation.
   3.3. Other users shall be alerted for the same.

9 Infrastructure Documentation

1. IT department shall maintain the inventory of all infrastructure including
   1.1. Hardware Configuration for laptops, desktops, servers, network switches and routers
   1.2. Application Software, Tools and Platforms installed on the computer systems with version numberand service pack information
   1.3. Company-wide Licenses and original software media
   1.4. Current status of all controls implemented
   1.5. All documents received for the Application Software, Tools and Platforms
2. IT department shall maintain the
   2.1. Records of access rights
   2.2. Roles assigned to individual users
3. IT department shall maintain record of Laptops/Desktops assigned to employees,
   3.1. Hardware Configurations
   3.2. Application software installed on them
   3.3. User IDs, admin password, email ids
4. IT shall create and maintain Company-wide and Site-specific Network diagrams
5. IT shall maintain
   5.1. the infrastructure system logs
   5.2. Infrastructure and Data breach incidence records,
   5.3. corrective and preventive maintenance

10 Physical and Environmental Security Policy

10.1 Physical Segregation

The following equipment shall be physically segregated with secure server room.

1. The Application, Database and Storage Servers
2. Network Switches connected to internet
3. Internet Firewalls
4. Telecommunication Systems

10.2 Fire Safety

All the areas that have critical information assets – Servers, UPS, shall have adequate fire fighting arrangements

10.3 Climate & Temperature

All the areas that have critical information assets – Servers, UPS, shall have

1. Climate control and ACs to ensure operating temperature and humidity is maintained at a desirable level
2. Display alerts monitored by trained personnel

10.4 Power Supply

All the critical information assets shall have

1 Fully redundant power supply systems

2. 24/7 UPS

11 Business Continuity Management Policy

11.1 Availability

All critical information assets shall have

1. Redundant fault-tolerant architecture to address fail over
2. Back-up and Recovery Processes in case of fail over based on approved Recovery Time Objective andRecovery Point Objectives
3. Process of periodic back-up of critical data and machine images in different locations

11.2 Incidence Response

All critical information assets shall have

1. Industry standard diagnostics to monitor health and performance
2. Procedures to drive quick resolution and prevention of incidence on impacted systems

11.3 Executive Review

IT department shall periodically review the resilience and performance of critical information assetsand report the findings and action taken to the executive leadership.

12 Abbreviations

AMC	Annual Maintenance Contract
HO	Head Office
IT	Information Technology
ITP	IT Policy
LAN	Local Area Network
PC	Personal Computer
PDA	Personal Digital Assistant
RAM	Random Access Memory
SOP	Standard Operating Procedure
SME	Subject Matter Expert
QA	Quality Assurance
QC	Quality Control
HOD	Head of the Department
DVD	Digital Versatile Disc