2024

FACT

प्रगति के पथप्रदर्शक

PIONEERS IN PROGRESS

I T Department

I T POLICY DOCUMENT

CONTENTS

1. INTRODUCTION

IT Policy document of the Fertilisers and Chemicals Travancore Limited (FACT) is intended to serve as a management approved reference for policies, procedures, best practices as well as rules & regulations relating to the access, usage, maintenance and administration of Information Technology (IT) resources and services in the organisation.

The IT policy document provides a roadmap for the best practices in the use of Information Technology for carrying out business activities in the organisation.

Divisions and departments of FACT that make use of information technology for discharging their functions are expected to adhere to the approved IT Policy.

The IT Policy document shall be reviewed on a regular basis and modified to reflect changes in Company policy and technological/ business environment.

1.1. IT department

The IT department of FACT is responsible for implementation of the approved IT Policy. Besides providing IT support for FACT, the IT department manages its SAP based Enterprise Resource Planning (ERP) system, its Data Communication Network, Servers, Desktop/ Laptop PCs, Printers, Networking equipment, e-mail facility, corporate intranet and the official web-site (www.fact.co.in).

1.2. ERP System

1.2.1. The present ERP system of FACT was implemented during the period April - November 2009 on SAP platform, the global market leader in ERP segment.

1.2.2. The SAP ERP system in FACT, also known as FACT>>FORWARD system (F>>F) integrates business processes on an enterprise-wide basis and covers functional areas such as Finance, Marketing, HR, Production, Materials, Maintenance, etc.

1.2.3. SAP ERP system facilitates day-to-day business transactions and also provides information support for corporate management. FACT Centre of Excellence also known as CoE group is constituted with members from each functional area and are responsible for functional support for SAP ERP system as well as making periodical configuration modifications so as to reflect changes in business rules/ practices.

1.3. Information Security

1.3.1. Information security is essential for protecting information assets from threats originating from different sources, including computer-assisted fraud, industrial espionage, sabotage, vandalism, natural disasters, computer viruses, hacking, denial of service attacks and so on.

1.3.2. Officers/ staff of FACT having access to ERP system Internet, e-mail, other IT resources/ facilities are to maintain information security, confidentiality and also mitigate any potential threats by adhering to the approved IT policy.

1.4. Policy structure

1.4.1. The IT policy document is laid out broadly in accordance with IT Act 2000 / IT (Amendment) Act 2008 and covers the two main sections mentioned below:

1.4.1.1. ***Corporate IT Plan*** which spells out the management's vision and direction as regards the present and future scope of IT in the organisation.

1.4.1.2. ***IT Security Policy*** which aims to provide guidelines for achieving information security objectives of confidentiality, integrity and availability of information.

1.5. Policy implementation

1.5.1. Following factors are critical for successful implementation of IT policy:

- Support from FACT management
- Effective communication of IT security policy to all stakeholders of FACT
- Periodic review and assessment of the effectiveness of the policy
- Regular updates to the policy document by continuous improvement and addressing changes in FACT's business objectives/ environment

2. CORPORATE IT PLAN

2.1. IT Mission statement

2.1.1. The following IT mission statement is promulgated considering criticality of the IT function in achieving FACT's business goals/ growth/ strategic plan and also considering the impact/ consequences of any potential lapses in IT security.

2.1.1.1. ***To provide timely, cost-effective, reliable and sustainable technology services for meeting information needs of decision-makers, managers and staff of FACT by equipping the organisation with information technology resources while maintaining confidentiality, integrity and availability of data.***

2.1.1.2. ***Developing and maintaining superior communications and computing infrastructure.***

2.1.1.3. ***Identifying and responding to changing needs of the company through fiscally responsible collaboration and innovation***

2.2. Operational Plan

2.2.1. Role of IT department

2.2.1.1. Provide IT support to all the functional areas in the organisation by leveraging in-house efforts / outsourcing and collaborative efforts with other organizations / expert groups / institutions of higher learning, etc.

2.2.1.2. Procure, Install, maintain and upgrade suitable cost-effective IT hardware, software and other IT infrastructure and ensure high levels of data and information security.

2.2.1.3. Strive to spread IT-culture amongst employees based on organizational need, roles & responsibilities of personnel and facilitate the objective of becoming a world-class business organization.

2.2.1.4. Impart IT training to all related personnel at regular intervals.

2.2.1.5. Perform the following functions :

- Maintain, control and manage IT systems in the enterprise
- Plan, procure, configure, maintain, augment and upgrade IT resources
- Monitor IT developments and plan for technological changes/ adoption
- Submit technical surveys, study reports, clarifications to top management and advise/ assist management decision-making on IT investments
- Provide SAP-BASIS support for F>>F system including service pack upgrades, patch level updates, management of access control, end-user roles & privileges
- Perform system administration and troubleshooting of servers, desktop PCs, laptops, networking equipment and enterprise-wide e-mail services
- Organise manpower support for facility management (including hardware, networking) and technical/ functional support for F>>F modules
- Manage round-the-clock operation of F>>F system, help-desk support and periodic archival of data and system files
- Maintain enterprise-wide inventory of IT assets & computer consumables
- Procure and distribute computer consumables to end-users
- Co-ordinate maintenance support for IT infrastructure

- Manage AMC of computers and peripherals
- Keep corporate website/ intranet updated with latest facts & figures
- Technical support for website maintenance
- Training/ guidance for internship students and apprentices
- Administration of Internet facilities, leased lines, broadband and modems
- Maintenance support for legacy servers/ applications
- Technical support for attendance recording systems, fertiliser monitoring system of Govt. of India, public procurement portal, etc.
- Co-ordinate with Centre of Excellence (CoE) group (constituted by the management for providing functional support for F>>F system) and ensure :
- Decision support for senior level management
- Information support to staff on salaries/wages, settlement of claims etc.
- Productivity by reducing breakdowns of plant machinery through production/ maintenance/ materials modules and office automation
- Financial discipline through checks and balances in accounting system
- Enhancements/ process improvements through configuration changes
- Preparation, revision and update of system/ user level documentation
- Management of custom developments on SAP-ABAP platform
- Organise training programmes for end-users at various levels
- Periodic disposal of e-waste

2.2.2. Functioning

2.2.2.1. IT department monitors system capacity and plans for future capacity needs sufficiently in advance and procure/ upgrade system resources to ensure availability of adequate resources and reduce possibility of overload.

2.2.2.2. Administrative approval shall be obtained from IT department in case procurement/ upgrade of hardware, software, network or services is needed.

2.2.2.3. IT department functions independently of user departments and is not assigned initiation/ authorization of transactions or changes to data files.

2.2.3. Segregation of duties within IT department is along the following lines:

- Operations
- IT Security administration
- Application programming and system configuration
- AMC/ maintenance support/ facility management
- Ensuring availability of computer consumables/ media

IT staff are assigned to tasks based upon their individual skill levels and

capability for performing assigned responsibilities. Training programs (both in-house and external) are instituted to ensure that IT personnel possess the knowledge necessary to adequately perform their assigned responsibilities.

2.2.4. Duties & responsibilities of each staff are identified as Primary and Secondary. Rotation of responsibilities is periodically carried out at Secondary level to the extent possible subject to manpower constraints. Manpower availability is periodically reviewed vis-à-vis requirement and requests for posting internal candidates from other departments and/ or new recruitment are put up.

2.2.5. Project management

2.2.5.1. Project planning is done to assess/ define the nature, requirement specification and scope of the project.

2.2.5.2. Necessary tasks to complete project are identified, defined and assigned.

2.2.5.3. Wherever appropriate, user departments are involved in specifying the general nature and scope of a project. Project teams consisting of appropriate IT and user personnel are established for each major project.

2.2.5.4. Project planning includes an analysis of alternative courses of action that will satisfy the requirements established for the project. Critical milestones in each project's life cycle are identified along with estimated timelines.

2.2.6. Processing of IT Contracts

2.2.6.1. Role of IT department consists of:

- Defining the Pre-Qualification criteria
- Defining technical specification and technical scope of work
- Technical evaluation of bids
- Preparation of technical recommendations

2.2.7. Documentation policy

2.2.7.1. The objective of system documentation maintained by IT department, is to describe the way systems function, their contents, and controls. Policy in respect of the different documentation types is as follows:

- *User manuals* covering facilities, access control and operating instructions
- *Program manuals* covering technical information about structure and design of ABAP/ web programs that are required for software maintenance

- *Database schema* and *Logical schema* to be maintained.
- *A list of codes and codification logic* used to codify data items such as materials, vendors, unit of measure, plants and so on, to be maintained by CoE.
- Functional specification document, Technical specification document, Business blueprint and Solution document to be maintained.

2.3. Disaster and contingency planning

2.3.1. Disaster recovery site for SAP server landscape is outsourced to external agencies experienced in this field.

2.3.2. Disaster recovery (DR) plan is available in Annexure 1.

2.3.3. DR plan is kept in a continued state of readiness and periodically tested to ensure that critical application data, files, programs, etc., work correctly.

2.4. FACT Website

2.4.1. FACT corporate website www.fact.co.in is hosted by National Informatics Centre (NIC) broadly in accordance with the Guidelines for Indian Government Websites (GIGW). The website is designed to be accessible to PwD (Persons-with-Disabilities), facilitate regular content update and be protected against unauthorised use.

2.4.2. Website security audits by CERT-In empanelled 3rd party audit agencies are carried out.

2.5. Adherence to Cyber Security

2.5.1. Cyber crisis management plan is prepared along the following lines to identify cyber security incidents and prepare for appropriate response/ remediation.

2.5.1.1. Cyber security framework includes the following safeguards/ best practices :

- Restricting administrative privileges for software, operating systems, devices and network along with mechanism to track and log privileged actions
- Ensuring patching and updates of firmware and software
- Installing security devices such as Firewalls, Intrusion Prevention and anti-virus system capable of detecting events such as network scanning, probing and countering Cyber-attack
- Implementing application security controls for web and mobile applications
- Segmentation of network, with separate VLANs for different functional requirements so as to control communication between different VLANs

- Use of firewalls to create a buffer zone between Internet and networks used by the business
- Secure protocols are used. All non-IP-based protocols are not to be used
- Deploy external firewalls in High availability (HA) mode as a perimeter security device
- Ensure that IP addresses allocated to each network appliance/system/server is not user modifiable
- Deploy web/ email filters to block known bad domains/ addresses, malicious IPs
- Ensure that mobile apps address vulnerabilities such as man-in-the-middle, DDoS etc.
- Build organisation's network diagram and keep it confidential
- Enable encryption for Wi-Fi access between user & Wireless Access Point
- Implementing advisories of CERT-In
- Periodical IT security audits through CERT-In empanelled auditors and deployment of appropriate security controls.
- Conducting Cyber Security Awareness Program regularly for sensitising end users about cyber threats and observing cyber hygiene.

2.5.1.2. Social media security

- Official Social media platform to be operated by designated officials only and on trusted devices only.
- Always use a dedicated/ separate email for official social media accounts
- Always use a different set of credentials for official email account and official social media platform account.
- Multi factor authentication should be enabled wherever possible.
- Content updates to be approved by appropriate authority.
- Ensure to log out from official social media platform after usage.
- Do not use official social media platform accounts on public devices
- Disable Geolocation (GPS) access feature for official social media platforms.
- Ensure that social media platform updated to the latest version
- Enable alerts for unrecognized login attempts under login & security settings
- Regularly monitor email associated with official social media for any alerts

2.5.1.3. Incident management

- An updated list of point of contact (i.e. key persons and authorities/entities) to be contacted at the time of incident response is to be maintained

- Apart from addressing an incident, FACT shall mandatorily report cyber incidents to CERT-In within 6 hours of noticing such incidents or being brought

to notice about such incidents. Also, the information about its occurrence shall be shared with relevant stakeholders.

2.6. Master Plan

2.6.1. Master Plan aims to lay down a road map for realising IT Mission statement by setting short/ medium term goals consistent with business goals of enterprise.

2.6.2. Budgeting is done as per corporate guidelines and includes a hardware acquisition plan that reflects the requirements for short/ medium term needs.

2.6.3. Plan targets

2.6.3.1. Upgrade SAP to higher version if necessary, a cloud based ERP system

2.6.3.2. B2B facility to integrate with SAP installations in Fertiliser ministry and PSUs

2.6.3.3. Reverse auctioning system for automating global tendering for procurement of raw materials such as rock phosphate, sulphur etc.

2.6.3.4. Paperless office system to automate office records/ correspondence/ approvals

2.6.3.5. Automation of railhead operations using laptop computer & portable printer-based system for on-line generation of goods receipt, issue of delivery challan for secondary movement/ sales and sales/ stock accounting

2.6.3.6. E-payment/ E-collection systems for Bills payment and Collection receipt

2.6.3.7. Reduce the use of ad-hoc reports and design a robust MIS platform with decision support/ dashboard interfaces for use at the corporate level

2.6.3.8. Web enabled Quarters Application system, Recruitment portal

2.6.3.9. Implementation of Medical Claims system, Travel Claims system

2.6.3.10. Whatsapp integration of Fertiliser Sales system, Chatbot for Product/ MRP

2.6.3.11. Automation of Material pass system

2.6.3.12. Mobile app to be developed for enabling employees to access information such as Leave, TA claims, Medical claims, Payslip, Perks etc. via common facility.

2.6.3.13. Mobile App to be developed for Marketing personnel

2.6.3.14. QR code based Electricity Charges remittance system for township shops

2.6.3.15. Arrangement for providing hands-on training in association with Training Centre to cover regular CoE support for HCM and other modules. Possibility of arranging training on SAP configuration for all modules is to be explored.

2.6.3.16. Possibility to be explored for engaging on regular basis, a cross-functional team of expert SAP consultants for providing functional/ configuration support as done currently for HCM module, to strengthen/ supplement existing CoE team .

2.6.3.17. Web Learning platform is to be implemented so as to enable all employees with web access to avail on-line training content on relevant subjects including plant

operation, safety besides technical and management topics.

2.6.3.18. Hands-on training on MS-Excel for power users covering advanced topics such as Macros is to be organised in association with Training School.

2.6.3.19. Possibility of introducing RFID tagging wherever feasible and a GPS based real-time fleet monitoring system for road transport are to be explored.

2.6.3.20. Bringing all Logistics in the company under one Logistics system such as Vehicle Entry Token System.

2.6.3.21. Providing fibre optic cabling wherever it is not available and switching cabling network from copper to Fibre.

2.6.3.22. Automating document flow within the organisation by a Document Management System/ E-Office.

2.6.3.23. Integrating SAP with GeM.

2.6.3.24. An early detection/ warning system is to be developed to provide alerts as and when any news item pertaining to our organisation is reported or published in social media including Facebook, Twitter/ X, YouTube, Websites, Whatsapp.

2.6.3.25. Key statistics are to be incorporated in our Corporate website including Visitor Counts, Page hits, Pages with high/ low hit counts and so on.

3. IT SECURITY POLICY

3.1. Data ownership, classification and control

3.1.1. Department, section or office responsible for maintaining any master data or for creating/ generating transaction data is considered as owner of that data.

3.1.2. Data owners may delegate responsibilities, but will remain ultimately responsible for the data owned by them.

3.1.3. In case any security incident is detected, data owners shall intimate the IT department for initiating appropriate action.

3.1.4. Before any confidential information is extracted from IT systems and passed to any outside agency authorization shall be received from data owner concerned. Appropriate non-disclosure agreements must be in place with any outside agency before information is shared with that agency.

3.1.5. Information must be consistently protected throughout its life cycle, from its origination to its destruction. Information must be protected in a manner commensurate with its sensitivity, regardless of where it resides, what form it takes, what technology was used to handle it, or what purpose it serves.

3.1.6. Retention policy: Business data in ERP shall be retained for up to ten (10) years.

3.1.7. FACT's data classification system, applicable to electronic data maintained in ERP system, legacy systems and end-user PCs is as follows :

3.1.7.1. Confidential: Sensitive information for which access shall be tightly restricted on need-to-know basis. Disclosure requires the information custodian's approval and, in the case of 3rd parties, a signed confidentiality agreement required to be executed.

3.1.7.2. Internal: Information related to FACT but not available to public, shall only be disclosed to 3rd parties if a confidentiality agreement has been signed.

3.1.7.3. Public: Information such as press releases, company website, marketing brochures, etc.

3.1.8. All computer-resident confidential information shall be protected via access controls/ administrative controls to ensure that it is not improperly disclosed, modified, or deleted.

3.1.9. Without consent of appropriate authority, employees/ contract personnel are prohibited from recording confidential information with recording devices such as mobile phone, digital camera, webcam, etc., copying to media such as CD/DVD/USB-devices, computers residing outside FACT premises, Internet based file shares, transmission by e-mail/social media/fax/post to non-official addresses.

3.1.10. Unless specifically been designated as "Public", or "Internal", all FACT internal information shall be assumed to be confidential.

3.1.11. Access to departmental PCs containing confidential information shall be restricted and the data shall be protected by the employees concerned.

3.2. Asset ownership, classification and control

3.2.1. IT assets including software & physical assets shall have an approved custodian.

3.2.2. In order to maintain accountability for assets, IT department, who are the owner, has compiled a list of all its information assets which includes among other details, i/d no:, category, custodian, location, etc., with software to manage asset records.

3.2.3. Data centre is equipped with fire detection, prevention extinguishing systems

accessible to operations personnel. Operating staff are sensitised to the importance of keeping the centre clean and free from combustible materials.

3.3. Third Party Access

3.3.1. Access of 3rd parties to information processing facilities of FACT will be clearly spelled out in contract covering physical, logical and network assets with specific reference to FACT's IT security policy.

3.3.2. Risk assessment will be carried out by owner/ custodian before granting any 3rd party access.

3.4. Security incidents

3.4.1. All suspected policy violations, system intrusions, virus attacks and other security incidents shall be immediately reported to IT department.

3.4.2. Incidents and malfunctions will be reviewed by IT department during the security review process so as to prevent future incidents.

3.5. Malicious software

3.5.1. IT department shall implement procedures, user awareness and change controls to detect and prevent the introduction of malicious software into the organization's computing environment.

3.5.2. To prevent interruption of service caused by computer viruses for computers and networks, all end-users must keep current versions of approved virus-screening software enabled on their PCs at all times.

3.5.3. End-users must avoid downloading files from untrusted sources in the Internet and media such as CD/DVD/USB devices so as to minimise risk exposure. Shared folders in end-user PCs if any must be set to read-only mode.

3.5.4. All user departments shall comply with the requirements of software licenses. No unauthorized or illegal software shall be used.

3.5.5. All e-mail attachments shall be automatically scanned when entering the network or mail server and scanned prior to use.

3.5.6. IT department shall whenever necessary, disseminate information on real threats, hoaxes and the procedures for handling each type of attack.

3.5.7. All devices accessing FACT Network must run anti-virus software with current updates/definitions.

3.6. Housekeeping

3.6.1. IT department will regularly back-up software, documentation and business information.

3.6.2. Restoration procedures will be documented.

3.6.3. To protect IT resources from loss or damage, desktop/ laptop PC custodian concerned shall be responsible for regularly backing-up data.

3.7. Exchange of Information

3.7.1. Reasonable measures shall be taken to prevent loss, modification, or misuse of data that is electronically transmitted (i.e. email and file transfer).

3.7.2. IT facilities in divisions/ departments shall take care not to produce unsolicited commercial e-mail (otherwise known as SPAM) to be sent out into the Internet.

3.7.3. If approved mass e-mailings are to be made, IT department shall be consulted to check for adverse effects on systems/ network and appropriate mitigation measures will be enforced.

3.8. Vulnerability Management

3.8.1. Vulnerability management shall be done to reduce risk to IT installations by verifying that systems or network devices are using latest patch levels, are not running unnecessary services and do not have default passwords.

3.9. ERP Access Control

3.9.1. User Access Management

3.9.1.1. Creation of user in ERP system shall be duly authorized by division/ functional head.

3.9.1.2. Each person accessing ERP system shall use a unique FACT-assigned User ID and a private password.

3.9.1.3. Access control rights for each user/ groups shall be provided after due authorization from functional heads in consultation with respective CoE.

3.9.1.4. Administrator access to production systems will be limited to only those with a genuine business requirement. Developers and other application personnel shall not have OS level access on production systems, except in emergencies and in such cases, access shall be granted only for the necessary duration.

3.9.1.5. Access rights shall immediately be removed or modified when a user leaves the organization or there is a change in his/her job profile due to transfer/promotion/deputation or special reasons such as vigilance enquiry.

3.9.1.6. Users' access rights will be reviewed at regular intervals. Functional Heads in consultation with respective CoE will review their employee's rights to ensure they are consistent with their present job function. IT department will review user rights to ensure that elevated privileges have not been granted without authorization and accounts that have not been used recently or belong to terminated employees are deactivated.

3.9.2. Password policy

3.9.2.1. Users will be responsible for safe keep of their passwords.

3.9.2.2. Users will be granted initial temporary passwords and will be forced to change them immediately.

3.9.2.3. Passwords are an important aspect of computer security and poorly chosen passwords may result in the compromise of the entire IT function. As such, all employees shall take following steps, to select and secure their passwords :

- All passwords are to be treated as confidential FACT information. They should not be shared with anyone, including administrative assistants.
- If an account or password is suspected to have been compromised, IT department shall be contacted immediately.
- Privileged passwords (i.e. for "root", "administrator", etc.) should be changed every 90 days or whenever someone with administrator-level access leaves the services of the company or is transferred internally.
- Old passwords shall not be re-used for a minimum of 12 months.
- Temporary passwords shall be changed at first log-on.
- Systems shall be configured to lock user accounts in event of 8 consecutive unsuccessful login attempts and for reset by System Administrators.
- Use of "Remember Password" feature of applications is not recommended.
- Passwords shall not be disclosed in e-mail or other communications.
- Passwords shall not be written down or stored unencrypted on ANY computer (including mobile phones and portable media)

- System accounts shall use passwords that meet or exceed requirements.
- System-level passwords must be changed at least once every 90 days.
- All user-level and system-level passwords must conform to the following requirement: (i) Passwords shall be at least 8 characters long; (ii) Passwords shall be composed of alpha-numeric characters.

3.9.3. Information Access Restriction

3.9.3.1. Access to menus and menu items shall be controlled so the users only view data or menus that they are authorized to view.

3.9.3.2. Users' rights shall be based on a Least-Privileged basis, so that they limited to only those functions to which they are authorized (i.e. read, write, delete, and execute). User's rights shall be reviewed on a periodic basis to ensure that no user or group has excessive privileges.

3.9.3.3. Outputs available to users shall be limited to those authorized specifically.

3.9.4. Monitoring System Access and Use

3.9.4.1. ERP should be configured to log all security-relevant events or exceptions. Event logs will be retained for at least one year and at least 3 months on-line. Administrator group will monitor event logs at periodic intervals.

3.9.4.2. Administrator group will regularly review the results of the monitoring of information processing facilities to detect deviations from the organizations' access policy and to improve and discipline those who deviate.

3.9.4.3. Event and security logs must be protected in order to assure their accuracy and to protect them against tampering or misuse. All original logs must be kept unaltered. Extracted log events shall be kept separately from the original logs.

3.9.4.4. System administrator will ensure that all system clocks in ERP servers are synchronized.

3.10. E-Mail and Internet Access Monitoring

3.10.1. E-mail/ Internet access are primarily for FACT's business requirements. FACT reserves the right to access e-mail systems at any time with or without advance notice or consent of the employee. Such access may occur before, during or after working hours by any manager or security personnel designated by FACT for the said purpose.

3.10.2. FACT also reserves the right to monitor all Internet access. While FACT recognizes that accidental access to undesirable sites is unavoidable, prolonged or repeated access to undesirable sites will be construed as intentional violation of IT department's policy and may result in disciplinary action.

3.10.3. Employees should always ensure that the business information contained in Internet communication is accurate, appropriate, ethical, and lawful.

3.11. Mobile Computing

3.11.1. Users must reasonably ensure mobile devices are physically secure at all times if they contain FACT sensitive data, by taking precautions such as:

- Mobile devices should never be left visible in a car and should never be left in the trunk or other storage location overnight.
- Mobile devices should be carried onboard aircraft and not checked-in.
- Mobile devices should not be left at tables in public places (i.e. restaurants) if they will be out of sight.

3.11.2. Users are strongly encouraged to back up their FACT data stored on mobile devices. Backup may be done when connected to FACT network (file shares and other backup facilities), or may be backed up to removable media. If backed up to removable media, it must be physically protected or the data encrypted.

3.12. General Use and Ownership

3.12.1. While IT department's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of FACT. Because of the need to protect IT department's network, management cannot guarantee the confidentiality of information stored on any network device belonging to FACT.

3.12.2. Employees are responsible for exercising good judgment regarding the reasonableness of internet use.

3.12.3. Employee shall exercise due diligence to protect sensitive or confidential data.

3.12.4. For security and network maintenance purposes, administrators of systems and networks may monitor equipment, systems and network traffic at any time.

3.13. Unacceptable Use

3.13.1. Under no circumstances, an employee of FACT is authorized to engage in any

activity that is illegal under local, state, national or international law while utilizing FACT's IT resources.

3.13.2. The following indicative list of activities are generally prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if it is disrupting production services).

3.13.2.1. System, Network, and Internet Activities

- Private use of Internet may be permitted within reasonable limits, provided that the websites accessed are not unlawful or inappropriate.
- Internet must not be used to violate intellectual property rights of any party such as copyrights, trademarks, patents, trade secrets, publicity and privacy rights. Employees are prohibited from interfering with or attempting to disable anti-piracy mechanisms or other measures used by copyright owners.
- Attacking in any way, scanning, probing or penetrating, computer systems or networks on the Internet is strictly prohibited. All employees shall be aware that Internet access may be screened/ logged/ monitored, in permissible ways.
- FACT reserves its right to block access to websites which are considered as inappropriate. Deliberate attempts to access such sites will result in disciplinary action.
- Download of untrusted files from Internet by employees is not recommended.
- Unauthorized copying of copyrighted material including, but not limited to, digitization & distribution of photographs from magazines, books or other copyrighted sources/ music and installation of any copyrighted software for which FACT/ end user does not have active license is strictly prohibited.
- Willful release of malicious programs into system is prohibited.
- Employees shall not disclose official passwords to others or allow use of their accounts by others.
- Employees may not use any FACT computing asset for sexual harassment, fraudulent offers of products, items, or services or unlawful activity.

3.13.2.2. Email and Communications Activities.

- Employees shall not send unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals (email spam).
- It is prohibited to participate in any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Employees shall not use FACT email or computing resources to participate in creation of/ forwarding of chain letters, "Ponzi", or other schemes of any type.

3.14. Systems Development

3.14.1. Security Requirements Analysis and Specification

3.14.1.1. The purpose of this policy is to ensure that all new systems comply with the organization's security requirements.

3.14.1.2. Risk assessment shall be done to evaluate security of new major system/ upgrade

3.14.2. Security in Application Systems

3.14.2.1. All applications developed using any programming language/ platform shall perform validation of input data before storing or processing so as to ensure that input is correct and appropriate and thus the system integrity is protected.

3.14.3. Digital Signatures

3.14.3.1. FACT will consider appropriateness of the use of digital signatures to protect and authenticate the integrity of electronic documents.

3.14.3.2. Officers who are involved with electronic commerce will conduct risk assessment to assess message authentication and integrity of transaction.

3.14.4. Development and Support Processes

3.14.4.1. For effective utilization of ERP System, a full time CoE member possessing requisite domain experience from each MM, FIN, SD, HR, Production/Maintenance shall be posted to IT Department.

3.14.4.2. As any new development/ changes in ERP have cross-functional implications, close interaction among the CoE members is essential. Hence all the CoE members have to be located in IT Department.

3.14.4.3. Each CoE member of respective module shall be responsible for overseeing security and control procedures of all changes to functional configurations of ERP system and custom developments therein. Any software change in the respective ERP module requires formal approval by the Functional Head. All changes to software shall be documented by respective CoE.

3.14.4.4. IT department shall ensure that programmers are only given access to areas of application that are necessary for the approved work.

3.14.4.5. CoE shall oversee entire application change process prior to change including:

- Ensuring changes are submitted by authorized users.
- Obtaining formal proposals and specifications before work commences.
- Obtaining formal approval prior to work commencement.

3.14.5. Functional Heads along with respective CoE shall oversee entire application change process including:

- Ensuring change minimized business interruption.
- Documentation is updated and old documentation is archived..
- Version control is maintained
- Maintaining an audit log of all change requests.
- Updating all user procedures.
- Ensuring that users accept all changes prior to implementation.

3.14.6. Respective CoEs of individual modules shall oversee entire application change process after the change including:

- Ensuring that testing is done securely (in a test environment that is segregated from development and operational systems).
- Ensuring that implementation does not disrupt business processes.

3.14.7. IT department will institute a Patch Management process for operating systems and SAP ERP system, that will include the following elements:

- Identification of new patch availability.
- Assessment of applicability and criticality of patches.
- Patching effort timing and methods.
- Effects of patches on existing applications.
- Testing of patches before deployment.
- Documentation of patch levels for various systems and applications.

3.15. Compliance

3.15.1. Intellectual Property Rights

3.15.1.1. Officers and staff of FACT shall comply with legal aspects of intellectual property protection rights and limitations of license agreements for software products.

3.15.1.2. Users shall not download/ install 3rd party pirated software on FACT systems

3.15.1.3. Users shall not download/ install any non-approved software from the Internet without due clearance from IT department and only if there is a genuine

business need for the same.

3.15.2. Security Policy

3.15.2.1. There shall be a full time cyber security officer posted to oversee the overall IT security of the company.

3.15.2.2. FACT will continually monitor the organization's compliance with its security policies to maintain the security, integrity and availability of IT assets.

3.15.2.3. IT department shall periodically conduct security audit of all external/ internal routers, firewalls, access points, hosts and DR facilities/ media storage.

3.15.2.4. Department Heads shall monitor their end-user's compliance with organization's IT security policies, procedures, standards and requirements.

3.16. Logical access controls

The following logical access controls provide means of controlling accessibility of information to users of software systems including ERP system.

3.16.1. Identification and authentication

3.16.1.1. Users duly nominated by concerned department heads vide request letter are assigned a unique login identity by IT department as per user preferences. A default password is assigned by IT department to new logins and communicated to users concerned with specific instructions to change the password during their very first login session. Users are also instructed to ensure that login passwords assigned to them shall be kept strictly confidential.

3.16.1.2. The system provides facility for enabling users to change their password at any time. System has built-in provisions for automatic ageing of passwords, making periodic password changes mandatory and precluding choice of obvious/ vulnerable passwords.

3.16.2. Role based access control

3.16.2.1. Users of each application module such as Finance, Materials, Sales, Production, etc. are categorised depending on the role assigned to them.

3.16.2.2. Facilities, features and operations in any application module are grouped into different roles. Required role or roles are assigned to each user by IT department as per instructions from concerned CoE/ Department head vide

request letter/ e-mail.

3.16.2.3. The system enables user access only to those facilities, functionalities and operations in any given form/ screen that are specifically assigned to the particular role/ roles allotted to the logged in user.

3.16.3. Operating system level interfaces

3.16.3.1. Operating system level access is restricted exclusively to systems administrator.

3.16.4. Secure gateway (Firewall)

3.16.4.1. Firewall is used to filter access to FACT's internal network from the Internet and all external access so as to keep out/ prevent malicious hackers, scan incoming traffic for viruses and at the same time allows privileged users at divisions/ departments to use the Internet.

3.17. Physical access controls

3.17.1. Physical access controls shall be used to protect sensitive IT resources. These controls shall be designed by the custodian concerned to prevent unauthorized access, damage or interference to business processes that take place therein.

3.17.2. Access to sensitive information and information processing facilities will be restricted to authorized persons. Authentication controls will be used to authorize and validate entry. A visitor log of all visitors shall be maintained by the site manager. Physical barriers (i.e., doors) must be of sufficient strength and construction to deter entry, based on the results of the risk assessment.

3.17.3. Access rights shall be given on a least-privilege basis, and shall be as granular as necessary to protect all categories of information or facilities. Access rights to secure areas shall be reviewed by site manager periodically and updated.

3.17.4. All visitors to secured areas shall be supervised and only allowed in for authorized purposes. A visitors' log shall be in place at all secure areas to record date and time of entry and exit. Visitors shall be given security instructions.

3.17.5. IT contractors, service vendors, suppliers, technicians etc., shall be advised of site rules and regulations concerning their proper conduct within FACT's property.

3.17.6. Access to Data centre/ Disaster recovery site must be controlled by biometric systems, door lock keys, or any other physical access control systems. Master badges or keys must be restricted to very few individuals per site or system. Wherever possible, control of these systems will be retained by IT department.

3.17.7. Sensitive media will be locked in file cabinets or other protective furniture such as fireproof vault that takes into account the results of the risk analysis.

3.17.8. Where possible, systems shall monitor the physical security of facilities such as Data centre (DC) or Disaster recovery (DR) sites. Monitoring could include any or all of the following technologies, based on the outcome of the physical security risk assessment:

- Closed circuit TV or video cameras.
- Fire/smoke sensors for sensitive working areas.
- Security patrols by CISF.

3.17.9. Hazardous items like batteries or combustible materials such as printing stationery shall be stored at a safe distance from secure facilities.

3.17.10. Back-up media shall be stored off-site and at a safe distance from facilities so that it would not be damaged if the facility is damaged.

3.17.11. External access controls.

3.17.11.1. Servers are located centrally in Data Centre at IT department/ HO and admittance to the server room and facilities is restricted to staff on duty. Backup media is kept securely in fireproof enclosures under lock and key.

3.17.12. Application version control and change monitoring

3.17.12.1. All configuration changes to ERP system and customisations/ enhancements are authorised by Centre of Excellence (CoE). Such changes are reviewed, tested and documented by CoE before release in Production system.

3.17.12.2. Privilege for update of production system rests exclusively with IT department administrator group which carries out updates after due confirmation from CoE.

3.17.13. System software maintenance

3.17.13.1. Standard procedures are used for system software installation, maintenance and configuration management which ensure that all modifications are

properly authorized, tested, implemented, and documented. Only system software packages and associated procedures from ERP are used.

3.17.14. New system software/ updates are tested on a system devoted to testing functions in ERP landscape.

3.17.15. Proposals for modifications or enhancements to existing system software are reviewed to determine if they satisfy business/ operational requirements, affect system integrity and abide by vendor specifications, mandates, recommendations or scheduled maintenance announcements.

3.17.16. ERP administration.

3.17.16.1. The position of database administrator is fixed at a sufficiently senior level within the department to ensure independence in judgment/ and decisions.

3.17.16.2. Procedures are in place for recovering database environment to the point just prior to failure, and minimizing time required for recovery. The above procedures are tested periodically.

3.18. Network access control

3.18.1. Network devices, such as switches, routers, DNS servers, gateways, bridges, etc. shall not be deployed on the FACTNET except by IT department. If other departments require these services, they must consult with IT department and these services must be configured to not interfere with FACTNET.

3.18.2. If partners or vendors need to connect devices to FACTNET, the vendor should consult with FACT Network and Administration Team for doing so.

3.18.3. All 3rd party devices that require connection to FACTNET must be approved by IT department and the Network Manager before the device may be connected.

3.18.4. IT department shall implement strict controls on the organization's networks to ensure safeguarding of information and protection of organization's infrastructure. Controls shall guarantee security of data in networks and protect connected services from unauthorized access.

3.18.5. A record of trouble incidents is with details of each problem and history of incidents is maintained.

3.18.6. Performance management

3.18.6.1. Network monitoring addresses traffic levels for capacity planning purposes and used to study processing load, nature of traffic, usage growth, and trends in order to plan for increased network facilities.

3.18.7. Change management

3.18.7.1. All changes to network hardware/ configurations are implemented only after due testing and authorisation. Changes are adequately tested using a test and acceptance plan to validate functionality of changes before they are implemented. All changes to network system are documented and tracked.

3.19. Operating system level security.

3.19.1.1. End-user level access to server operating system is not granted.

3.19.1.2. Use of functional IDs (those set up to perform a specific function such as backup or shutdown) is kept to a minimum. A user ID is disabled after a specified time interval when ID has not been used (e.g. 120 consecutive days).

3.19.1.3. Standard user IDs and passwords supplied by the software vendor is changed prior to placing the software into production.

3.20. Computer operations control

Purpose of computer operations controls is to ensure that server and support systems are properly started/ shutdown, file backups are taken at appropriate intervals, recovery procedures for processing failures are established and actions of computer operators and system administrators are reviewed.

3.20.1. Backup and recovery procedures.

3.20.1.1. Recovery procedures are formally documented, reviewed and approved by Operations Team Head.

3.20.2. Helpdesk & Facility Management

3.20.2.1. IT Helpdesk is the central point for reporting and resolving all user queries, incidents and service calls for IT support and handles :

- Recording & addressing of queries and complaints of users.
- Receiving information on viruses and other threats to FACT information systems.

- Escalating all unresolved queries to specialists and vendors
- Reporting query resolution back to users.

3.21. Process automation controls

3.21.1. Manufacturing divisions concerned are responsible for implementation of best practices in Process Automation that covers Distributed Control Systems (DCS), SCADA (Supervisory Control and Data Acquisition), PLC (Programmable Logical Control) equipment, laboratory systems such as Gas Chromatograph (GC) and proprietary systems.

3.21.2. IT department shall perform an advisory role in this regard, if necessary.

Annexure 1

Policy Statement

This policy is designed to support disaster recovery planning, preparedness, management, and mitigation of risks to the continuity of information technologies (IT) systems and services used for FACT Production purposes.

Reason for Policy

The disaster recovery standards in this policy provide a systematic approach for safeguarding the vital technology, services, and data managed by both the Information Technology (IT) Department and individual departments. This policy also provides a framework for the management, development, implementation, and maintenance of a disaster recovery (DR) program for the systems and services managed by IT Dept. that uses FACT's data.

Entities Affected by this Policy

All Divisions/Offices of FACT Ltd, including Marketing offices of all states.

Who Should Read this Policy

All employees of FACT, those who are utilizing the Company's information technology resources.

All Users and custodians of FACT's data.

Contacts

Direct any questions about this policy or IT Disaster Recovery, to General Manager (IT), Head Office, Udyogamandal, Kochi, Kerala using one of the methods below:

- Office: 0484 – 256 7314
- Email: csc@factltd.com

Overview

Adoption of Disaster recovery setup is important for all Departments to maintain availability of Company Operations and resiliency of data/applications.

What is Disaster Recovery?

Disaster Recovery (DR) aims at protecting the Department from the effects of significant catastrophic events. It allows the Departments to quickly resume mission-critical functions after a disaster.

Types of Disasters

A disaster can be related to any incident (both intentional and/or non-intentional) that causes severe damage to the operations and data of any Organization.
There are three major type of disasters:

- **Natural Disasters**
  (Earthquakes, floods, Hurricane etc.)

- **Man-Made**
  (Cybercrime, human error, terror attacks, etc.)

- **Technological**
  (Chemical releases, power outages, Fire etc.)

Implementation

After the failure of connection to the applications/data hosted in FACT's Data Centre, the IT team will co-ordinate and execute the Disaster Recovery plan to continue the essential IT services to run the Company operations.

The officer in charge of DR system will contact the support team of Disaster Recovery Site after getting instructions from the Head of Information Technology Department. The support team will soon start the procedure for switching over the ERP operations to the Disaster Recovery Site and establishing the connection to the DR system. Connections to the Disaster Recovery site will be secured by using VPN technology. Critical users will be able to access ERP thru VPN using the pre-configured limited number of User IDs / passwords.

Testing

After establishing connections to the DR system, a User level Testing will be carried out to ensure the data integrity in the DR system. Testing will be carried out by all the User Departments and the process will be headed by the respective COEs. If any issues/loss of latest data are found during the testing then the same will be resolved by co-ordinating COEs, IT and Support Team.

After the successful testing, the system will be used in Production to continue the IT services for running Company operations.

Post Disaster Recovery Plan

After the restoration of Servers/Systems in FACT's Data Centre, the ERP transactions done in Disaster Recovery site will be synced to FACT's Data Centre and operations will be switched back to FACT's Data Centre. Subsequently, other systems will also be switched in a time-bound manner.