VARROC IT POLICY MANUAL

Version 9

December 30, 2022

Note

The information contained in this document is confidential and proprietary to Varroc Group. If it has been received electronically, it is write protected to prohibit changes without authorization from Varroc Information Systems Security Council.

Table of Contents

Amendments Annexure

Clause	Description	Change	Date
13.1	Module access to support team	Definition amended	3-Apr-22
13.2	Authorizations:	Definition amended	3-Apr-22
13.8	SAP Backup:	Definition amended	3-Apr-22
9	Electronic mails and retrieval	Definition/Heading amended	20-Sep-22
13.1	Physical Security	Definition amended	20-Sep-22
4.8	Data Storage	Definition amended	17-Oct-22
6.1	Operating System	Definition amended	17-Oct-22
6.2	Office Suite Software	Definition amended	17-Oct-22
7.5	Backup of the data stored on server (and not of local PC)	Definition amended	17-Oct-22
7.6	Application / Software installation	New Definition	17-Oct-22
10	Security Audit	Definition amended	17-Oct-22
4.6	New User	Definition amended	3-Dec-22
4.7	User Separation	Definition amended	3-Dec-22
11	New Project/Upgrades	Definition amended	14-Mar-23

Gaikwad

Jitendra Gaikwad

Head IT Infrastructure and Security

Vinod Khode

Group-CIO

Amendments Annexure

Clause	Description	Change	Date
13.1	Module access to support team	Definition amended	3-Apr-18
13.2	Authorizations:	Definition amended	3-Apr-18
13.8	SAP Backup:	Definition amended	3-Apr-18
9	Electronic mails and retrieval	Definition/Heading amended	20-Sep-18
13.1	Physical Security	Definition amended	20-Sep-18
4.8	Data Storage	Definition amended	17-Oct-18
6.1	Operating System	Definition amended	17-Oct-18
6.2	Office Suite Software	Definition amended	17-Oct-18
7.5	Backup of the data stored on server (and not of local PC)	Definition amended	17-Oct-18
7.6	Application / Software installation	New Definition	17-Oct-18
10	Security Audit	Definition amended	17-Oct-18
4.6	New User	Definition amended	3-Dec-18
4.7	User Separation	Definition amended	3-Dec-18
11	New Project/Upgrades	Definition amended	14-Mar-19

Ravindra Ghan	Vivek Verma
Head IT Infrastructure and Security	Group-CIO

Amendment Team:

1. Ravindra Ghan - Lead Infrastructure
2. Jitendra Gaikwad - Head -IT
3. Santosh Kulkarni - Sr. Associate - Infra
4. Sanjay Kulkarni - Sr. Associate - Network
5. Aditya Devadhe - Lead - ITFE
6. Sumit Sharma - Associate - IT
7. Rahul Verma - Sr. Associate - Digital
8. Vinod Giri - Lead - Digital

1. Purpose

Purpose of this policy is to establish guidelines for the employees and/or end users using the Varroc IT facilities, including computer hardware, printers, License software's including Operating System, Office Suite, SAP, e-mail, Internet and intranet access, collectively called "Information Technology".

Varroc's all of IT facilities and information resources remain the property of the Varroc Group and not of any individuals. Following this policy will help to ensure IT facilities are used:

- legally
- securely
- without undermining Varroc
- effectively
- in a spirit of co-operation, trust and consideration for others
- so, they remain available

The policy relates to all Information Technology facilities and services provided by Varroc. All staff and volunteers are expected to adhere to it.

2. Disciplinary Measures

Any action that may expose the Company to the risks of unauthorized access to data, disclosure of information, legal liability, or potential system failure is prohibited and may result in disciplinary action which may include the offender being denied access to computing facilities. Deliberate and serious breach of the policy statements may lead to disciplinary measures up to and including termination of employment and/or criminal prosecution.

3. Scope

The policy applies to all Varroc Group, India (except VLS) employees employed at all plants/locations of all companies in the Varroc Group. It is the responsibility of BU Head and Plant Head of all operating plants/locations to ensure that these policies are clearly communicated, understood and followed in spirit.

The IT policy also applies to software contractors, and vendors/suppliers providing services to Varroc Group that bring them into contact with Varroc Group Information Technology infrastructure. The Varroc Group employee who contracts for these services is responsible to provide the contractor/vendor/supplier with a copy of these policies before any access is given.

The policy covers the usage of all the Varroc Group Information Technology and communication resources, including, but not limited to:

- All computer-related equipment, including desktop personal computers (PCs), portable PCs, wireless computing devices, networks, databases, printers, servers and shared computers, and all networks and hardware to which this equipment is connected.

- All electronic communication equipment's wired or wireless communications devices and services, Internet and intranet and other on-line services.

- All software including purchased or licensed business software applications, Company-written applications, employee or vendor/supplier-written applications, computer operating systems, and any other software residing on Varroc Group-owned equipment.

- All intellectual property and other data stored on Varroc Group equipment.

- All the above is included whether they are owned or leased by the Varroc Group or are under the Varroc Group possession, custody, or control.

- These policies also apply to all users, whether on Company property, connected from remote via any networked connection, or using Varroc Group equipment.

4. IT Asset and lifecycle management

Computer hardware broadly includes all the IT devices including networking / storage / PCs/ Laptops etc. Updated list of all hardware devices must be available with Local/regional IT.

4.1 Personal Computers / Laptops:

Considering the Fast Technology changes, Life cycle of hardware would be defined as under:

PC: 5 Years, Laptop: 4 Years, Dot-matrix Printer: 3 Years,

Laser Printers: 3 Years, Desk Jet Printers: 3 Years.

Replacing of hardware will solely depend on functional/physical condition of said Hardware. Decision regarding this will be taken by IT infrastructure team.

Configuration of the PCs/Laptops to be purchased or leased are predefined and updated time to time which is available with IT. New procurement must be in line with the same, any deviation in this requires approval and authorisation from IT infrastructure team.

The issuance of Laptop/Desktop will be on approved note/mail by Department Head/Functional Head submitted to IT Function. The Laptop/Desktop will be issued with all the available standard and legal software installations as required by the business. The employee must submit the signed undertaking form to IT Function for the record.

Using personal laptops / pen drives and other IT devices in Varroc Group company premises are strictly prohibited and any violation of this will liable for disciplinary action.

4.2 Other IT Items:

The requirement of items such as switches, routers, firewall, wireless access point, etc. will be validated and approved by IT Function and PR can be raised for/from respective plant. The inventory will be maintained by IT Function and such items can be shifted and reused at other location based on the demand and availability with proper business justification.

4.3 Disposal of Old IT Hardware:

Old hardware must be declared by related IT Function and certified by Plant Head / Region Head / Function Head for scrapping/ buy back. Such list should also be approved by Apex committee. The Hardware equipment / parts will be stored in secured area defined by stores department for the disposal as per the e-waste rules and regulations circulated time to time by Government.

4.4 Loss or Damage of Laptop:

User must file FIR at concerned police station & simultaneously inform HOD, IT Function and concern HR personnel.

- Change/reset the Domain password immediately after the loss of Laptop/PC/Mobile and inform the concern IT Functional member for the data protection/deletion from such lost devices.
- Obtain a copy of FIR.
- Submit copy of FIR to HR for onward claim from insurance company.
- HR would submit the Insurance Claim based on the FIR filed.
- Post- claim settlement by insurance company; the difference amount between claim received and WDV or balance lease/rent amount will be borne/recovered from the employee who has lost the laptop.
- In case of physical damage due to negligence of employee and non-claimable through insurance, employee will bear the cost of damage.
- For on duty accidental damage, Company will review the incident and decide case to case basis to recover the repair cost from employee, based on approval of Business Head.
- Company will issue the Laptop which is available in stock at that time to the employees who lost the Laptop due to accidental damage, theft, and dead due to physical damage, based on the approval of Business Head.

4.5 Hardware AMC:

Comprehensive AMC of the hardware (excluding devices under warranty) may be given to an authorized vendor. Authorized Vendor will be selected by purchase department in consultation with IT Function. Devices to be covered under AMC will be declared by IT infrastructure team.

4.6 New User:

The basic IT facilities will be provided by IT function which includes but not limited to

- Email - as per email policy
- Access to general purpose applications

- ➢ Electronic access to SharePoint
- BI access with user ID
- SAP access with user ID

The approved request form should be submitted by requestor for granting above IT facilities. The separate approved user request should be submitted for other required special Licensed software, application, tool, subscriptions.

The budget for the same should be available in the plant/corporate of that financial year. The undertaking form for IT equipment's should be duly filled and signed by the end user. The copy of undertaking form should be submitted to IT function and obtain the received copy for the record.

4.7 User Separation:

User must hand over all IT assets and that includes hardware and software to IT infrastructure team.

On receipt of written confirmation/Notification from HR dept. the electronics access for the separated employee will be terminated in next 2 business working days. The electronic access includes but not limited to

- ➢ Email ID
- ➢ SAP ID
- ➢ BI ID
- ➢ Windows domain ID

On receipt of written confirmation request from HR dept for email forward to other employee in case of separated employee will be actioned for email forwarder to the designated person's email box for the max. period up to 1 month only. After the completion of month period the email forwarder will be terminated, and email id of separated employee will be permanently deleted.

4.8 Data Storage:

User's Data must be stored on respective plant server where such facility is provided by IT Function or can be stored on SharePoint (each of the users must be in a domain server). User may save the data on their respective PCs where the central data storage facility is not available as of now; however, laptop users can keep their data on laptop also. For better security, laptop users must save their data on the SharePoint server.

4.9 Software – Purchase and Issuance:

The employees must fill and get approval from Business Head / Functional Head for special software's, utilities and tools with proper business case and /or project details. User must raise the ticket into service desk to check the availability into existing software inventory by IT Function. In case such required software is not available then the concern user will get the budget approved and submit the copy to IT department to raise the PR. IT department will maintain the common and central repository of all type of Software's in the available tool. The software includes the all types of engineering software, tools and utilities. The all such software's will be acquired on company name in the form of perpetual license or subscription base.

The such software's will be upgraded, patched time to time for proper execution and security as per the availability from software providers and demand from business users. The proper AMC should be in effect and approved budget should be provided by respective Department / Business unit.

5 Networking

5.1 Within Plant

Network Diagram will be decided by IT Function as per the prescribed guidelines and certified by IT Team.

All computers within the plant including servers will have CAT – 6 cable connectivity. Where the distance between two switches is more than 80 meters OFC is recommended.

The switches which are needed must be branded manageable switches and the make / model will be decided by IT Team.

Wireless switches approved by IT Team can be installed wherever necessary with proper security arrangements. For guests, restricted network access can be given as per requirement with proper approval from Plant Head / Business Head / Function Head.

5.2 Inter Plant

All Varroc group plants are connected over the SD WAN as spoke location to data center located at TCL IDC, Dighi, Pune as hub location. We will get the stable and assured connectivity as per the agreed SLA. IT Function recommends to all plant to have the High-speed dongle having the strong and assured bandwidth with then as a contingency plan in case of rare outages of SDWAN links. Plants can decide the count of dongles with the help of IT Function for this contingency.

6 Software

Varroc Group strongly believes in using license software only, however, relevant meaningful freeware software may be used after consulting with IT Function.

6.1 Operating System

It is compulsory for every PC / Laptop to have license operating system, for end user's pc/ laptop Varroc Group will have latest Windows X as an operating system.
Any change in this will be communicated to Plant –IT time to time.

For plant level servers and for high end servers, Latest Licensed OS will be as per requirement and will be decided by IT Team.

6.2 Office Suits Software

On limited / Selected PCs other than E3 plan, MS Office License version will be installed and on rest of the pc's where there is minimal use of Spread sheets and documents, Open office may be installed.

6.3 CAD-CAM Software's

Drawing / Design department in Varroc Group will have all licenses designing software as per requirement. The said requirement will be managed, maintained and processed through concern Local/Regional IT / IT Team in consultation with respective Engineering department.

6.4 ERP (SAP)

Varroc has implemented SAP to enable information technology on our business systems. It is recommended to use its default features only. Any change/ modification or new development of any sort of report needs to be routed through concern plant SAP coordinator and approved by concern plant head, so that IT Team will study its feasibility and will develop the same in line with the requirement.

Any Technical / Functional problems will be sorted out by concern super user and he will be supported by concern person from IT Team.

Members of IT Team of different modules will plan their visit to each of the Varroc Group plants to solve plant related problems if any or to have look at plant level activities related to SAP.

There will be 2 days meet of entire Varroc group's SAP coordinator and IT persons once in a year to have better co-ordination / functions / latest updates related to SAP / IT / New technology deployment etc.

6.5 Software Development

Varroc Group is well equipped with strong ERP - SAP, IT will not encourage any software development until and unless it is genuinely required and does not exist in SAP. If it must be developed, the end user must submit/ discuss exact requirement to Local/regional IT. Decision regarding in house development or out sourcing will be taken by IT Team based on feasibility study of the exact requirement.

Entire track of such requirement/ development will be recorded and will be available with Local/Regional IT.

7 Data Security

Data security is one of the prime responsibilities of individual users and for IT Function and should be strictly adhered in accordance with the policy.

7.1 Antivirus

Virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable internet files, diskettes, and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to Pc's/laptops' in terms of loss of data, loss of staff productivity, and/or loss of reputation.

IT Function will install only the Licensed Antivirus decided by IT Team and no employee will Purchase/download/copy any other Antivirus on Company provided PC/Laptop.

IT Function will ensure existence of latest updated Antivirus on each of the PCs/ Laptops/ Servers in respective plants.

7.2 Data Access and Distribution

Unless expressly authorized to do so, employees are prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to Company. Unauthorized dissemination of such material may also result in severe disciplinary action. Segregation of duties must be maintained.

7.3 PC Lockdown

Users are prohibited to download or use any storage devices and install any software tools by himself and to restrict the user, the PC's are lockdown by disabling the USB ports. Users should raise the demand by raising the ticket to IT via service desk. IT will check the software usage policy and licensing details and then push/install from central repository to end user PC's.

7.4 Data Loss and Prevention

DLP is installed by default on all work station and mobile workstations used for design and development under the technical center and design department. DLP will restrict the design users to share, print, attachment to emails and generate the logs on attempts of such activities.

basic objective and advantages of DLP

- Email Protect: Email going out through Microsoft outlook will be scanned.

- ➢ Application File Access - Data accessed by any application will be monitored
- ➢ Printing Protection Rule - Whenever any file or content base file is send for printing then it will be monitored or block
- ➢ Screen capture Protection - Monitor or block screen capturing of confidential data
- ➢ Web post Protection Rule - Monitor or block confidential data going out of endpoint through Web post
- ➢ Plug and Play Device Definition - Bluetooth Devices, CD/DVD Drives, Infrared (IrDA) Devices, Wireless Communication Devices.
- ➢ Removable Storage Protection - Monitor & Block or Encrypt copied files to Removable storage.

7.5 Backup of the data stored on server (and not of local PC)

It is the responsibility of Local/regional IT to back-up the user data kept on the server on hard drive/ tape drives or any other backup devices available at the Plant. User data stored on the SharePoint online is backed up regularly at other cloud location.

7.6 Application / Software installation

All the application, tool, software's used for the business will be stored in the central repository and the installation will be done by pushing them from SCCM server. By default, all the users will be restricted and will not have any access rights to download/install any software by its own. User need to get the approval from dept head for the desired software/application/tool and mail to IT Function for the installation.

8 Internet usage

Internet use facility is provided to employee considering the security measures by restricting the URL category. Employee must be used for company business only. Internet use brings the possibility of breaches to the security of confidential company information. Internet use also creates the possibility of contamination to our system via viruses or spyware. Spyware allows unauthorized people, outside the company, potential access to company passwords and other confidential information.

All employees have a responsibility to use the Company's computer resources and the Internet in a professional, lawful and ethical manner. Abuse of the computer network or the Internet may result in disciplinary action.

8.1 Internet Downloads

Files which are downloaded from the Internet must be authorized and checked for copy-rights, and necessary permissions should be obtained. They should also be scanned for virus contaminations prior to their use. All appropriate precautions should be taken to detect any virus and, if necessary, to prevent its spread.

8.2 Monitoring of computer and Internet usage

IT Function have rights to monitor and log all aspects of its Computer system including, but not limited to, monitoring Internet sites visited by Employees, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by employees.

8.3 Blocking Sites with Inappropriate Content

IT Function has the right to identify and block access to Internet sites containing material deemed inappropriate in the workplace.

8.4 Internet Provision for VIP guest, Auditor, on-site service partners.

Internet will be provided to only to VIP guest and external Auditors on approval of CIO. IT will use the provisioned VLAN and maintain the Access Control List (ACL) to have a managed control on data security and secured network connection.

9 Electronic mails and retrieval

As a productivity enhancement tool, Varroc Group encourages the official use of electronic communications. Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are the property of Varroc Group.

Written permission/email from HR is required to allocate official email id to new joiner.

The official email ID for new employees will be strictly in the form of **first_name. last_name@varroc.com** only. However, if the employee name and/or surname are too long, or of complex in nature than any other sensible format may be accepted. If the names of two or more employees are identical and one is already registered in the system then alternate email id will be provided by IT Function. In such cases the alternate email id will be first_name.last_name1@varroc.com

For retrieving key user emails from server backup which are in litigation hold for any reason like mail lost, deleted, or providing old data to new employee or to that Dept. HOD, IT Function would require approval from HOD/plant head/business head in case of plant employee and approval from concern HOD/Functional Head for corporate users.

Retention (investigation / Litigation Hold) of Emails which are on server would be maintained for 6 months only. In case of retrieval of email or email box, the BU head/functional Head approval is required to raise the ticket to Microsoft.

10 Password policy – SAP / Domain ID / Email ID / BI User

10.1 Overview

All Varroc employees and personnel that have access to organizational computer systems must adhere to the password policies defined below to protect the security of the network, protect data integrity, and protect computer systems.

Sharing of ID and Password is strictly prohibited. Disciplinary action will be taken if violations are found.

10.2 Purpose

This policy is designed to protect the organizational resources on the network by requiring strong passwords along with protection of these passwords and establishing a minimum time between changes to passwords.

10.3 Scope

This policy applies to all personnel who have any form of computer account requiring a password on the organizational network including but not limited to a domain account and e-mail account.

10.4 Password Protection

- Never write passwords down.
- Never send a password through email.
- Never include a password in a non-encrypted stored document.
- Never tell anyone your password.
- Never reveal your password over the telephone.
- Never hint at the format of your password.
- Never reveal or hint at your password on a form on the internet.
- Never use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other program.
- Never use your corporate or network password on an account over the internet which does not have a secure login where the web browser address starts with https:// rather than http://
- Report any suspicion of your password being broken to your IT computer security office.
- If anyone asks for your password, refer them to your IT computer security office.
- Don't use common acronyms as part of your password.
- Don't use common words or reverse spelling of words in part of your password.
- Don't use names of people or places as part of your password.
- Don't use part of your login name in your password.
- Don't use parts of numbers easily remembered such as phone numbers, social security numbers, or street addresses.
- Be careful about letting someone see you type your password.

10.5 Password Requirements (subject to change)

The following password requirements are set by the IT security department:

- Minimum Length - 8 characters
- Maximum Length - 14 characters
- Minimum complexity - Passwords should use three of four of the following four types of characters:
- Lowercase
- Uppercase

- Numbers
- Special characters such as !@#$%^&*(){}[]
- Passwords are case sensitive and the user name or login ID is not case sensitive.
- Password history - Require the number of unique passwords before an old password may be reused. This number should be no less than 4 old passwords.
- Maximum password age - 120 days
- Minimum password age – 1 days
- Account lockout threshold - 4 failed login attempts
- Reset account lockout after - If there are three bad attempts in 20 minutes, the account would be locked.
- Account lockout duration - The account lockout will be 2 hours.

10.6 Regular Message Monitoring

The content of electronic communications may be monitored, and the usage of electronic communications systems will be monitored by Plant/IT Team to support operational, maintenance, auditing, security, and investigative activities. Users should structure their electronic communications in recognition of the fact that Varroc Group will from time to time examine the content of electronic communications.

11 New Project/Upgrades

Following is the structured and informed approach to request, undertake and initiate the IT Projects

- Every IT project needs the duly filled IT Project Request Form.
- All Project Request forms needs to be approved by respective ECM Member.
- Any project estimated beyond Rs. 5 Lakhs needs to have a payback calculation.
- Every project undertaken by IT will have a detailed Project Charter signed off jointly by IT and Business Owner.
- A project closure will have following mandatory steps:
  - Stakeholder's sign off for each logical milestone.
  - Feedback from respective stakeholders.
  - Documentation of Learnings and knowledge gained during the project execution.

BU / Function wise monthly Project status report will be published by IT to BU / Functional heads and Project owners

Considering the technical skill/competency required for the new projects\upgrades, ~~IT Function~~ IT function will technically discuss and will suggest minimum two vendors to the Corporate Materials for finalizing commercial terms & conditions among any one of the vendors suggested by IT Function.

12 Security Audit

IT team can periodically audit any system and other usage and authorization history as necessary to protect its computing facilities.

The IT reserves the right to audit any PC/laptop used for company business to ensure that it continues to conform to this IT policy. The IT Function may also deny network access to any PC/laptop, which has not been properly configured and certified.

IT functions disclaims any responsibility for loss of data or interference with files resulting from its efforts to maintain the privacy and security of those computing facilities or from system malfunction or any other cause.

12.1 Data Center Activities & Applications SAP / BI / Collaboration tool and Domain Control:

- Password - Oracle
- Password – Sun Solaris
- Password – End User
- Transport Requests
- SAP Security
- Backup
- Business continuity plan for Data Center
- Physical security
- Audit Logging and monitoring
- Incident / Helpdesk

12.2 Passwords (Oracle)

Default Passwords of oracle default ids will be changed only once and will be kept with management and data center Administrator

The new Password of oracle default ids will be changed only if there is change in Data Centre Administrator.

Password life time and reuse would be as per the best practices.

12.3 Passwords (Sun Solaris)

Following parameter settings would be maintained for Solaris OS on all the relevant servers wherever applicable.

Parameters set

- MAXWEEKS=25
- MINWEEKS= 3
- HISTORY= 5
- MINDIFF= 3
- MINALPHA=2

- MINNONALPHA= 1
- MINUPPER= 1
- MINLOWER= 1
- MAXREPEATS= 4
- MINSPECIAL= 1
- MINDIGIT= 2
- RETRIES = Not Set

12.4 Passwords (SAP End User)

- Password history would be up to 5 old passwords. At least 5 old passwords will not be assigned back to the user id.
- Password would be case sensitive and minimum of 8 characters in length.
- User id would be locked on more than 3 attempts made to login with wrong password.
- Life of password would be of 180 days from the date of password set by the SAP user.

12.5 User ID creation and mark for deletion.

User ID will be created on receipt of request by end user by raising the ticket in solution manager/email with duly approved by Plant Head/HOD/Business Head/Function Head/IT Management. Varroc technical team will evaluate the requirement and intimation mail would be sent to functional team for user creation intimation. Entire track of such ticket and emails will be maintained by SAP Security team.

User ID will be locked, maintain the validity period and marked for deletion

- If it is not in use and in dormant state for at least three months i.e. 90 days based on periodic review for effective usage and license compliance for SAP ID.
- On request from concern Varroc Functional Team Member.
- On receipt of request by HR dept. in case of employee separation.

Entire track of such ticket/emails will be kept by SAP technical team.

No R/3 user ID will be shared with any vendor for direct access to Production server. Access, if required will be given by using the Remote Desktop/TeamViewer. If it must be shared, written approval should be obtained from the Group CIO.

12.6 SAP Change Management (Transport Requests)

In case of resolving the error reported by SAP end user via email or in case of requirement of any changes in existing business function or in case of introduction of new functionality, business process the solution delivery team shall raise the ticket in solution manager.

Related Varroc functional Team will assign the ticket to himself if no Change Request Management (CHARM) process is required to resolve the SAP issue and ticket would be closed by same end user after the user acceptance and testing (UAT). Varroc core team member will study such cases and record the ticket in CHARM process in solution manager and follow the CHARM process to resolve the issue. The complete process is documented separately and would be followed as the IT policy. SOP for CHARM is attached herewith.

The email record of change request shall be maintained by respective Core team member in case of non-functioning of CHARM. All the transport requests moving into Production system shall be approved by CIO/SAP Head.

13 SAP Security (SAP Authorization & Access Management):

13.1 Module access to support team:

Varroc Core team will use the individual module access for the business support. By default, the SAP ids of Core team member will have the display only access for cross modules and full access for individual module for the support function.

The user access review would be performed once in a year. The dump of existing Tcode list of every business and corporate support function user would be provided to business for the review.

13.2 Authorizations:

Authorization of new t-code will be given to the user by SAP security member once the ticket is raised in solution manager/email by end user and validated by respective module Core Team member. Standard role will be identified and assigned to user as per department's requirement and demanded t-code will be part of this role which will help in further maintenance of authorization.

Record of t-code maintenance will be maintained in email response which will show the profile maintenance activity by recording the below details

T-code assigned/removed, name of role.

13.3 Changes to SAP Production client settings:

Cross Client will be opened only on Chief Information Officer (CIO)/SAP Head approval over mail. The purpose and relevant action log will be maintained.

13.4 Changes to SAP system settings:

The system settings would be changed/maintained as per the recommendations given by the SAP and record will be maintained.

13.5 Change to tables from SAP

The proper mail and justification to change the Table will be approved by CIO/SAP Head over mail and record will be maintained.

13.6 Changes to system profile parameters:

The system Profile Parameters will only be changed on approval from CIO/SAP Head. The record will be maintained.

13.7 Emergency changes/change requests:

In case of business urgency/non-availability of Approval authorities the approval for above mentioned points and T-code assignment and change requests would be obtained by requester in next 3 business days.

13.8 SAP Backup:

Daily Production Online backup will be taken as per the schedule by using Oracle BR-Archive and Symantec NetBackup.

Regular log of the Production backup of DB, Fill mode, Archival will be maintained.

Once in a year, Restoration of production offline/online backup will be checked on additional server.

Above backup procedure will be strictly adhered to the backup policy decided in consultation with business partner.

13.9 Business continuity plan for Data Center

Varroc is having the Disaster recovery site at TCL, IDC Bangalore. The Oracle Data Guard is used for data synchronization between Data center and DR Site for SAP Landscape.

- ➢ Recovery time objective (RTO) – Varroc has decided to have 4 Hrs. of recovery time to sync the DR site completely and user can be alternatively use as primary site on approval of Group CIO

- ➢ Recovery point objective (RPO) - Varroc is using synchronous storage replication then RPO will be the last transaction that was committed and written to disk which should be measured in minutes. Varroc will lose any transactions that were in-flight at the point when a complete or partial outage occurs at the primary site.

Varroc will perform the mock drill and record the activities once in a year to ensure the DR site is ready and can be used as Primary site.

13.10 Physical Security

Varroc Data Centre is co-located in 3-tier Data center at TCL, IDC Pune which is well equipped with:

Primary electrical power, generator, Centralised cooling system, Bio Metric access control, Smoke detector, fire alarm, rodent repellent i.e. entire BM system.

13.11 Audit logging and monitoring

End user's access will be monitored time to time and user access review would be done once in a year and entire log will be maintained.

14 Incident/ Helpdesk

For resolving day today's issues that end users may face in accessing IT resources, Service delivery process is implemented. In service delivery, the user should raise ticket over call to help desk or email the issue. Help desk team will connect to user and raise the issue in system for proper assignment and resolution. The stage-wise status will be auto emailed to users and supporting resolution member. In case of SAP related issue where the external help or configuration changes required then the CHARM will take issue tracking and recording as described in section 12.6