CHEMVEDA

INFORMATION TECHNOLOGY POLICY

Document Governance		
MM/ YY	September 2025	
Entities covered	Chemveda Life Sciences India Pvt. Ltd.	
Owner	Information Technology Department	
Revision History	Earlier Version: 00 Date of Revision: NA Revision Effective Date: NA	Policy Approved By: CEO Dr. Bheema Rao Paraselli P. Bheema Rao September 11, 2025

1.0 PURPOSE:

This IT policy states that information security protects critical business information to ensure continuity, minimize damage, and maximize returns. The company commits to securing organizational information assets using appropriate technology and processes to protect against threats to confidentiality, integrity, and availability. This policy will be communicated to all employees through induction and classroom training.

2.0 SCOPE:

This policy is applicable to all employees of Chemveda group. Contractors and third-party entities engaged with Chemveda are required to adhere to the provisions of this policy.

3.0 RESPONSIBILITY:

S. No	Department	Responsibility
➢	IT Department	• Responsibile for the effective implementation and administration of the IT policy. • Ensuring security and integrity of company data and systems. • Managing access controls and user permissions.
➢	Employees	• Are required to understand and adhere to the process outlined in the IT policy. • Report any IT-related issues or security concerns to the department.
➢	Division Head/CEO	• Reserves the right to amend any clause of the IT policy from time to time as required. • Responsible for ensuring overall compliance with the IT policy across the organization.

4.0 DEFINITIONS:

Not applicable

5.0 PROCEDURES/RULES/PROCESS:

- **Computing Usage:** Employees ensure security of computing resources/data.
  - **User Access to Information & Applications:**
    - Access granted to authorized users via unique credentials.
    - Access/revoke by app admin with supervisor/HOD approval
    - Request must specify purpose/nature of access.
    - Re-authentication after 5-15 minutes of Inactivity.
- **Password Management:**

  Access to a majority of the computing resources shall be controlled using User ID and password for identification and authentication. Hence, it is necessary that all users adhere to the following guidelines relating to password:

  - The minimum length of password shall be set as 6 - 8 characters. It can be a combination of alphabet, numerical and special character.
  - Passwords shall not be created from personnel information like family names or pet names or birthdays or dictionary words.
  - A password expiration period of 60-90 days shall be set, so that users shall be forced to change their passwords at regular intervals.
  - Users shall change the password at the time of the initial logon.
  - System shall maintain a password history of last 5 passwords.
  - System shall lock the account after 3 unsuccessful attempts during logon.
  - No user shall disclose passwords even to a system administrator or helpdesk.
  - If passwords have been compromised, the user shall inform the system administrator immediately and change the password.
  - Passwords must never be displayed in clear text or stored in readable form.
  - Exceptions to the password management policies for certain applications shall be documented in respective operational procedures.
- **Ensuring Logical Security on Desktops & Laptops:**

  All desktops and laptops shall have a login password. The folders or disk drives in individual desktops or laptops must not be shared unless appropriate access controls have been enabled on

the folder or the disk drive. Sharing of confidential information is not permitted. By default, usage of external devices like Pen Drive, External HDDs, CD, DVD, SD Card, etc. should be blocked to all users. Based on proper approval from his/her supervisor/HOD it shall be released only after enabling.

Laptop users shall take necessary precautions to ensure privacy and confidentiality of company's data stored in laptop hard disk.

- **Reporting of Information Security Incident:**

A formal reporting procedure shall be established to enable the users to report the security incidents. It is incumbent upon employees, contractors and third parties of Chemveda to adhere to the procedures. Users shall report an incident which is a potential threat to information security as per the defined procedure. Users shall report the nature of the incident to his/her supervisor/HOD. As a part of the reporting, users shall be required to mention observations, error messages, or failures if any. The user shall not attempt to perform any investigation, which could unintentionally compromise the evidence. A key aspect of incident investigation is preservation of evidence. The respective departments or units must notify the IT Manager if the security incident is suspected or indicative of security vulnerability.

- **Reporting Software Malfunction:**

Users shall notify any software malfunctions, i.e. software not functioning correctly as per the procedure (suspected malicious software, such as virus infection) to the IT department. As part of the notification, users shall be required to note symptoms such as error messages, failures, etc. The respective departments shall notify the IT service desk if the software malfunction is suspected or indicative of security vulnerability. In case of software malfunction, users are expected to follow the below procedure:

- Note the problem / messages appearing on the screen if any.
- If a security breach is suspected (e.g. suspicious mail client behavior), the user should
- inform the system administrator immediately for appropriate remedial action.
- The computer should not be used until a clearance is obtained from the system
- administrator for usage of the same. Also, the data/diskettes shall not be transferred to other computers.
- In case the system administrators suspect a security breach after the preliminary

assessment of the incident, they should report the same immediately to the IT Manager.

- The users are advised not to remove malfunctioning software, without the support of IT department.

➢ **Classification & Retention of Information / Data:**

All the information and data must be classified depending on its Confidentiality, Integrity and Availability.

Classifying the Information:

All the information assets shall be classified into one of the following categories:

- **Sensitive:**

  This classification applies to strategic business information, which is most critical and intended strictly for use within a closed group of Chemveda. Its unauthorized disclosure could seriously and adversely impact on Chemveda stakeholders, business partners and customers leading to legal and financial repercussions and adverse public opinion (Example: business plans, trade secrets, customer data, information security data, pricing strategy, strategy document, etc.).

- **Confidential**:

  This classification applies to less sensitive business information, which is intended for use within Chemveda. Its unauthorized disclosure could adversely impact on Chemveda employees, customers, stakeholders and business partners (Example: employee performance evaluation, CTC details, internal audit report, short-term marketing plans, analysis of competitive products / services, experience, knowledge, skill, information of people, etc.).

- **Internal Use**:

  This classification applies to all other information, which is supposed to be shared only within Chemveda which does not clearly fit into above categories. It's unauthorized disclosure against the policy, is not expected to have serious or adverse impact on Chemveda employees, customers, stakeholders and business partners (Example: information posted related to employee usage, HR policies, administrative circulars, training materials, manuals, etc.).

- **Public**:

  This classification applies to information, which has been explicitly approved by Chemveda management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm (Example: information posted on internet portals, product brochures, advertisements, job opening announcements, published press releases, etc.).

- **Ownership of the Information:**

  All the critical applications, information shall have designated owners. The files created by individuals shall be owned and classified by them. The data owners shall also define access rules and retention period. IT department takes the responsibility of the security of the information / data based on the definition provided by the owner.

- **Legal Compliance:**

  The objective for ensuring compliance is to avoid breaches of any criminal, civil law, statutory, regulatory, or contractual requirements. The data owners of respective business functions should be aware about legal aspects of using information systems and their responsibilities for ensuring compliance to the same. The organization shall identify all the relevant acts and regulations applicable to its environment and make all the data owners aware about the same.

- **Software Licensing:**

  IT department must maintain an inventory of existing software, applications, operating systems and databases that Chemveda is authorized to use and the number of licenses available for the same. Purchase and use of third-party software must be in accordance with third party license agreement and following restrictions shall be considered for such software:

  - Specific user restrictions such as the number of copies allowed, the number of machines the software can be installed on, or the number of concurrent users of the software allowed at any one time.
  - It is strictly prohibited to use or copy the software on another computer instead of intended computer for which it is licensed.
  - The IT department must perform periodic reviews of software usage on

Chemveda desktops, laptops and servers to ensure that it follows software licensing agreements.

- All software that is being used shall be procured only from approved / certified vendors.

- **Software Copyrights:**

  All users of software on Chemveda information systems must strictly abide by "Copyright Laws" and restrictions detailed by the software manufacturer.

- **Software Ownership:**

  The software / application developed by or for Chemveda is the property of Chemveda. This clause must be added in the contract for all third parties, who develop software or application for Chemveda. This prevents any dispute about ownership of the software, including the source code, once the project is completed. Any software/application developed by Chemveda employee, while on job, becomes the property of Chemveda.

- **Computer Virus Control:**

  All Desktops, Laptops, Workstations, Servers and other IT equipment must be adequately protected from virus. The computer virus may affect the stability of a system and may cause damage or loss of valuable business information. Adequate protection from virus would ensure that information, data, and software are protected.

- **Antivirus Software on End Point:**

  IT department shall ensure to prevent software and information processing facilities reasonably free from malicious software.

  - Users should not disable antivirus and not stop auto scan.
  - The antivirus software shall be updated by obtaining the latest updates from the antivirus vendor and distributed promptly across the organization.
  - Bypassing the in-built scanning process is strictly prohibited.
  - Users shall not be allowed to download freeware or shareware from internet without proper authorization from IT. All open source software shall be thoroughly tested and evaluated before being used to prevent Information leakage.
  - Any electronic information being brought into Chemveda's environment (e.g.

CD, USB drive, etc.) shall be subject to scan under supervision of IT department personnel prior to use.

- If a virus attack is suspected, user shall immediately intimate to IT department and discontinue the use of the system till further instructions from IT.

- **Antivirus Software on Server:**
  - Antivirus software installation is applicable not only at end point devices, but also at sever level which shall protect from malicious Virus, Trojans and Malwares from the network or from the internet. Antivirus software shall be installed on all Windows servers and activated. Administrator should duly update the antivirus software and their latest virus definitions as and when released. Administrator should also ensure for the timely distribution of the patches to all other locations and maintain an updated list of locations with patch update status.
  - Antivirus software should be invoked at start-up and keep enabled all the time while system is up and running and it should also be invoked whenever any new software or drivers are installed. The pen drives, CD, DVD, etc. should be scanned prior to use. Test & development servers should be protected in the same manner as production servers.

- **E-mail Security:**

  The use of official e-mail should be for the business purpose and advancement of business of Chemveda. Chemveda has an e-mail system for employees to facilitate better communication. The purpose of e-mail Security is to define necessary standards with respect to approved use of Chemveda e-mail system.

- **Authorized & Acceptable Use:**

  The e-mail system is intended for use in the conduct of Chemveda's business. Though limited personal usage has been allowed, but it should not compromise its official usage. The employees shall use the e-mail facility with responsibility and prudence. All e-mail messages shall be considered as Chemveda records, and retains all rights to read the contents of any message sent from Chemveda network.

- **Unauthorized Use includes, but is not limited to:**
  - Transmitting or storing offensive material like pornography.

- Soliciting for political, personal, religious or charitable causes or other commercial ventures outside the scope of the user's employment and responsibilities at Chemveda.
- "Spamming" - sending unsolicited messages, promotions, sending or forwarding chain letters.
- "Letter bombing" (re-sending the same e-mail repeatedly to one or more recipients).
- Creating, sending, receiving or storing materials that infringe the copyright or other intellectual property right of any third parties.
- Sending, transmitting or distributing proprietary information, data or other confidential Chemveda information to unauthorized recipients.

- **Awareness and Undertaking:**

  It is the responsibility of the user, who have been provided with the e-mail facility, to make themselves aware of the usage norms.

- **Access to External Public E-mail Systems:**

  Corporate Emailing facility would be provided to all authorized and approved users for official and business usage on a need basis. All employees are encouraged to send mails using the official e-mail facility provided. Chemveda does not provide access for external webmail portals like Hotmail, Rediff Mail, Yahoo Mail, Gmail, etc. and prohibited to use for any official communication. In case of any exigencies, where use of corporate e-mail is not possible due to down time or any other reason, management may permit the usage of public e-mailing on a case to case basis.

- **Access to E-mail Contents:**

  All the contents of mailboxes on corporate e-mail would be property of Chemveda. In the event of misuse, the management shall formulate a committee who reserves the right to inspect and review any data maintained in its e-mail system without prior consent of, or notification to, the employee.

- **E-mail Management:**
  - E-mail facility shall be granted to users only after receiving approval from the supervisor/HOD. The access may be granted on need and case to case basis.

- Users shall not allow others to operate their e-mail account under any circumstance.
- User should not open e-mail attachments unless they are sure about its contents and know their senders.
- Size of the e-mail should be kept as small as possible. For sharing large files within the office, shared folders on the network resource should be preferred over sending e-mail.
- Every individual should be assigned a limit on the size of Mailbox. This shall vary as per the job requirement of the user.
- Maximum size of e-mail with attachment permissible is 10 MB. In case of absolute necessity, sending of the mails with bigger attachment sizes can be facilitated by the IT-Department under approval of supervisor/HOD.
- An automatic warning should be given by e-mail administrator to user once the mailbox size reaches 80% of limit.
- Considering the e-mail storage space / bandwidth utilization, IT shall retain one - month e-mails in live mailbox.
- Users should send the attachments in a compressed mode / zipped format.
- All incoming e-mail messages should be scanned for virus / malware to prevent virus infection to the Chemveda's network or systems. This is an automated process at e-mail gateway level, and any such incidents where users receive file extensions such as .vbs, .exe, .com .bat, should immediately inform to IT person.

- **Creation of E-mail ID for Third Party:**

  Creation of temporary e-mail IDs for third party or contract staff is against the policy. Any exception to this would permit by management for business need only in following cases:

  - Request is approved by concerned HOD.
  - A start & end date for the account is specified.
  - Only one user shall have access to the e-mail account and name of the user need be specified in the form.
  - Non-Disclosure Agreement (NDA) should exist between Chemveda & third party.
  - The third party should agree to take the responsibility of actions of the individual operating the e-mail ID provide by Chemveda.

- **E-mail Etiquettes:**
  - User Responsibility - Each employee is responsible for the content of his / her e-mail.
  - Using Another Individual's E-mail - Individuals accessing the e-mail services of the Chemveda must not use or access an e-mail account assigned to another individual to either send or receive messages. If there is a need to read another person's e-mail (while he / she is on a vacation) due to exigency, the HOD shall authorize an identified user with access such as message forwarding, delegate permission etc.
  - Treatment of e-mail - Company employees must treat e-mail messages and files as Company information. E-Mail must be handled as private and direct communication between a sender and recipient.
  - Transmission of chain messages - Transmission / re-transmission of chain messages is prohibited.
  - Profane, Obscene or Derogatory remarks in e-mail messages - Users must not create their own, or forward externally provided e-mail messages which may be considered to be harassment, or which may contribute to a hostile work environment. Hence, users must not use profanity, obscenities, or derogatory remarks in e- mail messages discussing employees, customers, competitors or with any others.
  - Use appropriate mail addressee either in To or Cc. It is a good practice to avoid the Bcc.
  - The text in upper case is significantly more difficult to read than lower and mixed case text, so avoid writing in capital letters. When you write in all capital letters, it may look like as if you are shouting at recipient. The e-mail message should have proper header and footer, like header should contain greetings (Dear Sir/Madam, Hi, hello etc.), footer should contain thanks giving message (Thanks, regards etc.), and no short keys are allowed to use in the body of the e-mail (e.g. u, thx, etc.)
- **Internet Usage & Security:**
  - The use of official internet should be for the business purposes and advancement of business of Chemveda. The objective of this policy is for disciplined usage of internet and to protect information systems from attacks through the internet.
  - The Internet is a global public computer network providing a variety of information and communication facilities. It provides access to several services including e-mail

data transfer, login from remote systems, and data storage among many others. However, the use of the Internet also poses significant and widespread cyber security threats that make organizations' IT infrastructure and computer systems vulnerable.

- **Access to Internet:**

  Employees shall be provided with internet access on needed basis subject to approvals from their HOD.

- **Authorized & Unauthorized Use of Internet:**

  Internet usage must be restricted to serve business requirements. Though Internet facility has been provided to employees for official purposes only, they may use it for limited personal usage. They shall use Internet facility with responsibility and prudence. Unauthorized use of Internet shall include, but is not limited to:

  - Using for personal entertainment, personal business or profit, and publishing personal opinions.
  - Attempting to gain or gaining unauthorized access to any computer system of Chemveda or any other organization.
  - Sending/receiving/viewing racial, sexually threatening, defamatory or harassing messages.
  - Sending, transmitting or distributing proprietary information, data or other confidential information of Chemveda.
  - Using Internet for non-business purposes and wasting computer resources like uploading and downloading large files not related to business, accessing audio and/or video files, playing games on the Internet and engaging in online chat groups, not related to business. For any such usage administrative / legal action shall be taken.
  - Introducing computer viruses, worms, or Trojan horses.
  - Downloading obscene written material or pornography.

- **Downloading or Uploading of Software:**

  The users are not allowed to download or upload any software from/to internet without prior approval from the IT Department as well as their HOD. Any software download or upload should be based on business requirement, if business require to download the software, the downloaded software must be tested by IT representative on a standalone non-production

machine that has been recently backed-up. There shall be periodic review of all desktops by system administrator to ensure that no unauthorized software is installed.

- **Wi-Fi Access:**

  A wide range of devices use wireless technologies, with handheld devices being the most prevalent form today. This Policy discusses the most commonly used wireless handheld devices such as text messaging devices, Laptops and smart phones etc. As per policy, no Wi-Fi access is provided to any of the devices / users by default, it would be provided on needed basis based on approvals from the respective department HOD and will be subject to the following routine security measures.

  - Ensure that users on the network are fully aware of the risks involved / associated in computer security and wireless technology.
  - Place APs in secured areas to prevent unauthorized physical access and user manipulation.
  - Ensure that all APs have strong administrative passwords & all passwords are being changed regularly.
  - For guest user password shall be generated on the fly for internet access only based on the need and shall be disabled automatically.

- **Physical Security at Workplace:**

  Work environment must be secure from unauthorized access, damage or interference. The physical & environmental security measures must be in place to ensure security and the integrity of information processing facilities and information assets located within. The environmental controls at work place that shall be followed to maintain a minimum level of protection to information systems. Users shall also need to follow certain guidelines to ensure physical security of information and information processing systems in their work environments.

- **Securing the premises from visitors & third parties:**

  The date & time of entry and departure of visitors and third parties and the purpose of visit must be recorded in a visitor's log. He/she should keep their entry restricted to the discussion rooms or reception area. The employees are not authorized to take any visitor near user workstations. However, visitors and third parties may be allowed escorted entry to work place

for authorized and specific purpose only. They should not be permitted unsupervised access to computers/laptops or any other information or documents.

- **Workstation:**

  Computer terminals must not be left logged on, when unattended. Key locks, power-on and screensaver passwords, or other controls shall be used to protect them when not in use. Computer media like CD, Pen Drive, Memory Cards, external hard-disks etc. containing confidential information shall not be kept at unsafe area. They shall be stored in suitable locked cabinets when not in use, especially after working hours. Computer terminals should be switched off when not in use and should be protected by key locks, passwords, screensavers or equivalent controls to ensure sensitive information is not easily available to an unauthorized user. Files and other papers (non-electronic format) that contain sensitive or confidential information must be protected from unauthorized access. Users shall not leave such papers unattended on printer trays, photocopiers, are on their desks. Incoming and outgoing mail points must be protected from unauthorized use after working hours. 'Sensitive' and 'Confidential' information and storage media must be stored at secured area (ideally in a fire resistant safe or cabinet), when not in use.

- **Hardware:**

  All hardware devices acquired/developed by the Chemveda Group shall remain a company property. All such hardware devices must be used in compliance with applicable licenses, contracts, and agreements.

- **Purchasing:**

  The purchasing of company hardware devices shall be centralized within the IT department to ensure that all equipment conforms to industry standards. All requests for computing hardware devices must be a part of the annual IT budget and shall have the department HOD approval.

  - The request must then be sent to the IT department, who shall review the need of hardware, and then determine standard hardware that best accommodates the desired request.

- **Hardware Standards:**

  Hardware configuration is reviewed in order to determine what equipment shall be the best to meet the need of end user. The IT department makes every effort to provide the most suitable desktop or laptop while maintaining company cost effectiveness. Employees shall be given access to appropriate network printers. In certain cases, employees may be given local printer if deemed necessary by their respective department HOD in consultation with the IT department. If employees needing computer hardware beyond that which is typically provided must request such hardware from the IT department.

- **Outside Equipment:**

  Outside equipment not allowed to connect to the company's network without the IT department's permission.

- **Backup, Restore & Retention:**

  The purpose of this policy is to backup electronic data for all computerized systems. It is an essential task to ensure against the loss of valuable information. These backups are used to restore a system to a current state (from most recent backup) in case of system failure, or to restore individual files which are inadvertently deleted or lost. Each unit (corporate/site) in the Chemveda Group shall be equipped with automated backup software to back up the electronic data using authorized procedure. These backup logs (hard copies or electronic form) are maintained for proper tracking of the electronic data. The electronic data retrieval and retention shall be governed through authorized procedure.

- **Laptop:**

  An employee using company provided laptop shall be responsible for the security of that laptop, regardless of whether the laptop is used in the office, at one's place of residence, or in any other location such as a hotel, conference room or while travelling.

- **Eligibility:**

  Laptops shall be provided to employees purely at the discretion of the supervisor/HOD. The decision of the Supervisor/HOD to provide an employee with a laptop or a desktop shall be based on the following factors:

- The nature of the employee's job (e.g. need to operate system simultaneously along with other official interactions).
- Their working environments/conditions (whether or not they have permanent/individual office space)
- The necessity of an employee's availability after office working hours.

- **Intended Use of Laptop:**

  Every laptop user must ensure that the laptop is being used only for official purpose and in the course of the rightful discharge of their duties and not for generating, transmitting, corresponding any content that is contrary to company policies. This may lead to the user being subject to disciplinary or any other appropriate action as per company policies.

- **Physical Security & Theft Prevention:**

  To ensure physical security of laptops and data therein, all laptop users are required to undertake the following actions:

  - The physical security of company provided laptops is the user's personal responsibility. He/she is therefore required to take all reasonable precautions, be sensible and stay alert to the risks.
  - Keep your laptop in your possession and within sight whenever possible.
  - Never leave the laptop unattended when using it outside the office.
  - Never leave a laptop visibly unattended in a vehicle. If absolutely necessary, lock it out of sight in the trunk or glove box but it is generally much safer to take it with you.
  - Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage.
  - Keep a note of the make, model, serial number and the Chemveda asset label of your laptop but do not keep this information with the laptop.

- **Virus Protection:**

  Viruses are a major threat to valuable organizational data and laptops are particularly vulnerable if their antivirus software is not kept up-to-date. In this regard all laptop users are to ensure the antivirus patches are updated in order to safeguard their systems from potentially

harmful viruses. Report any security incidents (such as virus infections) promptly to the IT Helpdesk in order to minimize the damage.

- **Unauthorized Software / Content:**

  The user shall not install any unauthorized accessories/software like messengers, chatting software or any malicious software, which may cause problems to the functioning of the Laptop and strictly adhere to Company's software use age policy.

- **Handover of Laptop:**

  When an employee resigns, it is their responsibility to handover the laptop to IT department along with the proper password. In case the same laptop is issued to other departments or the same department, then IT shall keep a track of the laptop.

- **Networking Management:**

  This policy shall define the design, management, operation and use of the Chemveda Group Local Area Network (LAN), and it includes appropriate technical and procedural controls to reduce risk. IT Head of the respective unit shall oversee the management, operation and use of the Chemveda Group's data and voice networks.

- **Network Monitoring:**

  All LAN cabling can only be carried out by authorized, accredited personnel / third party. Access from the Chemveda wireless network to the wired network shall be provided to end users based on the respective departments HODs approval. Chemveda's entire network is protected by firewall/UTM policies. The backup of configuration of routers, switches and network architecture diagram (high level) documentation shall be maintained by IT.

- **Physical & Logical Access:**

  The network room/rack should be always locked, and network room/rack access shall be provided to authorized IT persons.

- **Remote Access Management:**

  The remote access of server/system shall be provided to vendors & service providers to troubleshoot the problem. The access account should revoked/disabled immediately once the problem is resolved. When remote access is provided to vendor/service provider, ensure that it

is restricted to particular server / system / IP address. The remote access credentials should be used only by the individual to whom they were assigned and may not to be shared with others.

- **Secure Software Development & Acquisition:**

  The purpose of this policy is to establish adequate security controls for the acquisition and deployment of Chemveda information systems.

  Policy and Guidelines:

  - During the requirement finalization, security features shall also be invariably included in addition to performance and other requirements.
  - The application should support authentication of individual users, not groups.
  - The databases should not store passwords in clear text or in any easily reversible form, rather encryption tools and techniques may be considered.
  - The workflow should be provided for role management, such that one user can take over the functions of another without having to know the other's password.
  - User identification and authentication requirement based on statutory and regulatory requirement, criticality of transactions etc. to be incorporated.
  - The system architecture shall be reviewed in the context of good design engineering principles for technology, databases, interfaces and accessibility.
  - The criteria and test cases for acceptance of the developed or acquired systems need to include security test cases in additional to functional test cases.
  - The development network and production network shall be separated to avoid any information security risks.
  - The outsourced development parties shall also be required to adhere to the secure development practices by including such requirements in development agreement, source code ownership, privileged access to database, test data provision etc.
  - In the maintenance phase, the information technology team shall download and maintain all latest patches to one central location.
  - The applicable patches shall be installed and tested on test system. The connectivity, compatibility and features shall be reviewed before formalize the application patches for all relevant users/network.
  - Information Technology team shall also obtain feedback from respective team Leader or Manager after testing the system. If any problem or abnormal behavior found, then

the installed patches shall be rolled back and system shall be restored to previous working condition.

- **Whistle-blower Procedure:**
  - This procedure provides an organized, confidential, and secure means for employees, contractors, and stakeholders to report unethical behaviors, IT policy violations, or suspected misbehavior linked to IT systems and information security.
  - **Areas covered include:**
    - Misuse of company IT assets.
    - Unauthorized access, data theft, or breach of confidentiality.
    - Cybersecurity incidents deliberately concealed.
    - Violation of IT security policies.
    - Use of IT systems for fraudulent or illegal activities
  - **Reporting Mechanism:**
    - Whistle blowers may report concerns through the following secure and confidential channel:
    - Dedicated Email ID**:** Whistleblowers@chemvedals.com
  - **Confidentiality and Anonymity:**
    - All reports will be handled with strict confidentiality.
    - Whistleblowers may choose to remain anonymous.
    - Retaliation or victimization of whistleblowers is strictly prohibited and will result in disciplinary action
  - **Investigation Process:**
    - Acknowledgement – The complaint is acknowledged within 3 working days of receipt.
    - Preliminary Review – The IT Security/Compliance team performs an initial assessment.
    - Formal Investigation – Evidence is gathered, and relevant stakeholders are interviewed.

- Corrective Action – Disciplinary, technical, or legal actions are taken, if required.
- Closure & Documentation – The case is closed, and records are securely maintained.

- **Protection for Whistle-blowers:**
  - Whistle-blowers reporting in good faith will be protected against retaliation.
  - Any act of retaliation will result in strict disciplinary action against the offender.
  - Whistle-blowers will not be penalized for mistaken reports made in good faith Roles.

- **Responsibilities:**
  - Employees/Stakeholders: Report any suspicious IT-related activity or violation.
  - IT & Security Team: Ensure confidentiality, secure evidence, and conduct impartial investigations.
  - Management/HR/Compliance: Enforce non-retaliation, implement corrective measures, and provide oversight.