Human Wellness

Information Technology

RESPECT each other's differences

FREEDOM in your work and personal lives

TRUST you as an adult

TRUTH in what we do every day

MEGA COMMITMENT

is to provide

Quality Products and Services to Our Customers

Through constant Improvement and Innovation

1 Introduction

We are all privileged to work for one of the finest companies. It is our utmost responsibility and duty to preserve and strengthen our Company's worldwide reputation built by people over many years. We have built our successes on the strong foundation of sustainable, transparent & Ethical business practices and quality products. Our quest for growth and excellence goes hand in hand with unflinching commitment to integrity in all our relationships with employees, customers, suppliers, government, local communities and our collaborators and shareholders.

The Information technology is aimed at conducting effective business through good corporate governance and to build a secure information technology environment in the Company. This Code applies to all Directors, Executives, Management and Employees of Mega Lifesciences Public Company Limited and its subsidiaries, associates and assigns (“Mega”). Mega strongly encourages implementation of this code for the benefit of the Company.

2 Foundation and Governance

This policy aims to ensure that Mega conducts business by efficiently leveraging the strengths and advantages of IT and also manage IT related risks aligned with corporate wide risks. The IT resources and data can be linked and harnessed to ensure Mega is able to meet its objectives including strategies and actions inclyuding policies and decisions to implement such strategies. IT requires appropriate risk management, reporting and monitoring, to ensure that applied technology can facilitate strategies and lead the enterprise towards business achievements as well as competitiveness and added value. The IT policy lays down the matters under its scope to help achieve the above stated objectives. Mega has prepared this policy in writing and communicate this Policy to those whosoever it is applies for meeting the stated objectives herein. This policy shall be applicable from December 01, 2021 and Mega or its Board of Directors/ Board of Management has the right to amend this policy from time to time.

3 Risk management

IT Risk Management shall be aligned with the Corporate Risk Management Policy and cover the following aspects:

1. Define roles and responsibilities in IT risk management

Manager – Head of Information Technology team shall be the risk owner and will be responsible for managing including mitigating risks.

2. Identify IT-related risks

- Physical and environmental risks concerning Data Room where servers, network and other equipment are located. Entry to the room must be regulated. Others include the room's temperature control system and fire alarm system.

- Risks concerning the use of software on the Company's computers, to prevent the installation of unsafe or malicious software which, for example, may bring in Malware or computer virus or let in attacks from outside networks on the machine or other machines working on the same network.

- Risks concerning the use of the Company's network system: the internal network and the Internet system shall be checked and watched, through the procedures that block outsiders' access to servers and clients which require the monitoring on Internet usage, the installation of antivirus software, the filtering of incoming and outgoing emails, etc.

- Personal risks that require control on access to the computer network, equipment and data in line with their roles, to prevent editing or changing of data.

3. Risk assessment shall cover probability and possible impacts, to prioritize risk management. Risks are classified into 4 categories as follows:

- Technical risks that may arise from an attack on computers and peripheral equipment.

- User-related risks that may arise from inappropriate identification of users' rights, that allows access beyond responsibility and may cause damage to information.

- Risks from disasters and emergencies caused by man-made or natural disasters other situations such as power outages and protests.

- Management-related risks arising from inconsistency of existing guidelines with possible risks.

4. Identify methods or tools to keep risks within the Company's appetite

Prepare the Description of Risk containing subjects, risk names, types of risks, description, risk factors, impacts, etc.; assign probability; and predict the severity of impacts and prepare Risk Map.

5. Determine IT Risk Indicators, and the system to monitor those indicators and report the results to responsible persons, so that risks can tackled in an appropriate and timely manner.

4 Security

1. Additional guidelines on IT Security Policy and security measures

- Objective

To guard against violations of IT Security Policy

- Guidelines

- Do not use computer resources and network for illegal or immoral actions such as creating a website to sell or promote anything that is contrary to the prevalent legal and moral norms.

- Do not use computer network or computer with others' user account, whether with or without the permission of the account owner.

- Do not access the computer system or encrypted data of other person to edit, delete, add or copy the data.

- Do not share other persons' data or the organization's information without permission from the information owner.

- Do not obstruct, damage or destroy the Company's computer resources and network, by spreading computer virus or enter the program that leads network computers or equipment to Denial of Service (DOS), etc.

- Do not smuggle data from the Company's network or others' machines connected with the network for data transmission.

- Always activate antivirus software before opening portable drives, email attachments and files downloaded from the Internet.

- Users must not share their accounts and passwords with others who share a computer.

2. Organization of Information Security

- Objective

To establish the management framework for information technology security within the organization.

- Guidelines

- Top executives shall oversee the compliance with the Company's IT Security Policy and guidelines.

- Manager – Head of Information Technology Department shall give assignments to IT operators, to ensure security and control the operations as prescribed in the IT Security Policy and guideline.

- Manager – Head of Information Technology Department is responsible for the management, supervision, monitoring and review of the overall IT Security Policy.

- IT operators, assigned as administrators, must inspect and ensure system security. In the event of undesirable or unexpected security incidents, they must fix the problems and report to supervisors.

- Users as well as internal and external offices must follow the Company's IT Security Policy and guidelines and must not commit any act that violates the Cyber Crime laws including but not limited to Personal Data Protection Act and Computer Crime Act.

3. Human Resource Security

- Objective

To ensure all users understand their roles and responsibilities when accessing the Company's IT system

- Guidelines

1. Establish written rules and responsibilities for employees or contractors, which must be aligned with the IT Security Policy.

2. Have employees and departments sign non-disclosure agreement (NDA). Considered part of the employment, NDAs bind employees to secrecy while they are working for the Company and at least 1 year after the termination of employment.

3. Demand Human Resources Division or relevant offices to immediately notify IT Manager in case of the following events, to ensure the most accurate and updated user account management:

- Employment
- Change in employment condition
- Resignation or termination of directorship or employment
- Transfer

4. Employees and contractors must acknowledge the policies related to information technology security management.

5. Newly-recruited employees must be given orientation on IT Security Policy, which should be part of the orientation.

6. Following a change or termination of employment or at the end of project, access to information must be immediately terminated.

5 IT Physical Asset Management

The objective of this clause is to inform users of their roles and responsibilities in using the Company's computer and peripheral equipment as well as the need to strictly comply with rules so that the Company's resources and data remains secured, accurate and available.

- Users of the Company's computers and peripheral equipment are responsible for the machines.

- Do not use the Company's computer and network for personal business purposes or inappropriate services.

- Users are barred from installing new software or changing programs installed in the Company's computer, unless seeking consultation or advice from system administrators or receiving authorization from the management.

- Do not modify computers and peripheral equipment unless authorized by system administrators or responsible units. Users must maintain the condition of computer and peripheral equipment.

- Users must not store or use computer in hot, damp and dusty environment and avoid dropping the device.

- Do not use or place the equipment near liquids, magnetic fields, high-voltage electricity, vibrating surfaces and the environment with temperature above 35 Degree Celsius.

- Move computers with great care. Do not put heavy items on top or throw the computers.

- Do not move while the hard disk is still in use or while turning on.

- Keep computer screens away from hard objects to avoid causing scratches or damage. Gently clean the screens and wipe the cleaning cloth in one direction. Moving the cloth in a circle can cause scratches.

- Users must return computers and peripheral equipment in their possession to the responsible units when their employment is terminated or contract project is over. The device and equipment must in good condition.

- Follow the Company's rules on the use of the Company's assets out of premises when needing to move computers out of the premises.

- Users are responsible for losses. They should not leave computers in a public place or place computers in the spots where risk of loss is high.

6 Software Licenses

The Objective of this clause is to raise users' awareness in their roles and responsibilities to computer software; and ensure their understanding in the use of copyrighted software, strict compliance with guidelines and maintenance of security in line with the Computer Crime Act and relevant laws.

System administrators' roles and responsibilities

- Take responsibility for controlling the application of software and allocating software accordingly to users' rights
- Take responsibility for software installation and upgrade for users in accordance with pre-arranged schedules.
- Remove and cancel access to software immediately after receiving notifications from the Company and/or departments.

Users' roles and responsibilities

- Use computer as if it is their own property, without committing illegal acts which may harm the Company.
- Programs that are installed on company computers are programs that have purchased with legitimate licenses. Therefore, users are prohibited from copying programs and installing them on other computers or modifying them.
- Do not copy, sell, publish pirated programs and sets of orders without permission, specifically as a tool for legal offences.
- Installation of unlawful programs on computer computers is strictly prohibited. If any user uses other programs other than the installed ones, whether they are licensed or freeware, the user shall be solely responsible for any possible damage or violation.
- Users shall submit separate requests for the installation, cancellation, transfer and return of computers and programs to the authorized persons and system administrators are responsible for executing the approved requests on a case-by-case basis.

7 Computer and Server Access Control

The Objective of this clause is to provide guidelines when unused, information assets – documents, recording media, computers and information –shall be kept out of reach of the unauthorized. Users are required to log out of the IT system when not using it, under the following guidelines;

1. Log out immediately when finishing work.

2. Apply proper authentication before using, to protect computers.

3. Save and store significant information of respective departments. Storage can be done in the following formats:

- in the database of the application system which is covered by the Company's Data Center, which will prevent the export of information;

- in shared file (central drive) in folders accessible in accordance with users' rights.

4. Shut down computers when it has been unused for more than an hour or when daily work is finished, except computer servers which must be operational around the clock.

5. Set the Screen Saver to automatic lock after more than 10 minutes of inactivity.

6. Seek approval from division chiefs or those with higher authority whenever wanting to move information assets – document, recording media and computer equipment – out of the Company. Such process must follow the Company's Asset Transfer-in/Transfer-out rules.

7. Be careful and take care of the Company's assets, treating them as their own assets. In case of loss due to negligence, they shall be responsible or pay for the damage.

7 Electronic Mails (Emails)

The objective of this clause is to ensure proper, convenient, fast, timely, efficient and safe electronic mail (email) messaging in support of operations, as guided by law, regulations, rules and the Company's IT security measures; and to ensure users' understanding and awareness of the problems caused by electronic mail services on the Internet. Users shall understand the rules set by system administrators and do not breach the rules or attempt any action that will cause troubles or is against the rules. They must strictly follow the administrators' instructions.

1. Email users must not violate the Computer Crime Act, the Electronic Transactions Act, related laws and the Company's IT policy and rules.

2. Business units or employees that use the Company's email messaging service must use emails for the Company's interests.

3. Employees have the right to use email. System administrators will complete the registration based on the list of employees from Human Resources Division.

4. Do not use others' email address to send or receive emails without the address owner' consent. In that case, the address owner is responsible for the usage.

5. In using email, the user must refrain from spoofing.

6. In sending emails on the Company's assignments, the senders must solely use the Company's email address, except when the Company's email system malfunctions and supervisors approve the use of other email addresses.

7. Using email requires polite language. It must not go against good morals. Do not provoke, satire or violate the laws. Users must not send personal opinions, claiming they are the Company's opinions which may cause damage to the Company.

8. Do not use the Company's email to publish information, texts, images and others that are against good morals, national security and lèse majesté, harm the Company's operations, or disturb others including the Company's service recipients.

9. Users are prohibited from using email addresses for personal activities, like private business and social media sign-up. If such action is detected, the email owner or users shall be responsible for it.

10. Do not perform any actions that will cause problems to the system's resources like creating chain mails, sending spam mail, sending letter bomb or sending emails to spread computer virus.

11. Do not send the Company's confidential information to other persons or departments not involved with the Company's mission.

12. Confidential information, if to be sent, shall be encrypted and the importance of such information shall not be specified in email headers.

13. Always log out after finish using email.

14. The Company reserves the right to cancel or suspend email service to employees when receiving complaints and requests or when finding unlawful acts. An investigation will be launched.

15. Witnessing any inappropriate or offensive activity, users shall file reports to the Company's whistleblowing channel.

16. Users shall be responsible for any action relating to the distribution, both in the form of email and the user's homepage. System administrators and the Company shall have no involvement whatsoever.

7 Data and Information Access

The Objective of this clause is to outline measures on Internet usage via the Company's network for efficiency and security and to raise users' awareness in accessing websites through the Company's network.

1. Information Technology Department shall outline Internet connection routes via security systems like Firewall or Proxy server.

2. Antivirus program must be installed and vulnerabilities must be addressed, before connecting the Company's computers with the network.

3. After using the Internet, users shall close web browsers to prevent access by other people.

4. Users shall access the information deemed suitable for their roles and responsibilities, for the network's efficiency and the Company's safety.

5. Users are prohibited from disclosing the Company's confidential information, unless it complies with the Company's official disclosure guidelines.

6. Users shall be careful when downloading programs through the Internet, including downloads for program updates, bearing in mind that such downloads must not violate others' copyrights or intellectual property.

7. Users are bound to verify the accuracy and reliability of data on the Internet before using it.

8. Users must not use the Company's Internet network for personal business benefits or to access inappropriate websites like those against good morals or those with information harmful to national security, religions, the Monarchy and society, as well as pornography websites.

9. Users' Internet usage must not infringe others or cause harm to the Company. Users must not act in violations to the Computer Crime Act or relevant laws. In using the Internet to support their job assignments, users must strictly follow the procedures prescribed by the Company.

8 Cryptographic and related Controls

A. Data management

1. Confidential information must be classified and categorized accordingly to mission and importance. The management of each category must be defined along with the practices to treat confidential or important data prior to cancellation or reuse.

2. Important data transmitted through public networks must be encrypted with international encryption standards like Secure Socket Layer (SSL) and Virtual Private Network (VPN).

3. Measures to control the accuracy and conformity of data input and output must be put in place, in case that the data is stored at more than one place (distributed database) or is related to other data sets.

4. Data security measures should be outlined in case computers are moved out of the Company's premises for repair or other purposes. For example, some data may need to be deleted.

B. User Privilege Control

1. Control access to data and processing equipment with usability and security of the IT system in mind. Define rules regarding access permission and privilege, to be acknowledged by employees at all levels for their strict compliance. Employees should realize the importance of IT system security safeguarding.

2. Define employees' access to data and IT system; for instance, access to the Application System and access to the Internet in accordance with their roles and responsibilities. Grant employees the access only to accomplish necessary work, with written approval from responsible persons. Review the access on a regular basis.

3. If any user requires a privilege access, it must be under tight control. The following factors are considered to determine whether control measures are tight enough:

- Approval from authorized persons
- Strict access; for example, only when necessary
- Time limits setting and immediate termination of access at the end of the time limits.
- Periodic password change; for example, after completion of task or every 6 months if such access is required for a long period of time.

4. Set measures to prevent access by unauthorized persons to computers, when authorized users are away. For example, demand authorized users to log out before leaving their computers.

5. Where it is necessary for users who own sensitive information to grant other users access to modify their information, like through shared files, such access shall be limited to an individual or a group of individuals and it must be revoked when such access is no longer necessary. The data owners must produce a proof of authorization, set time limits and revoke the access immediately after the time limits.

6. Where it is necessary to grant emergency or temporary access to IT system or network, the protocol must be followed and permission from the authorized persons must be obtained at all times. Record reasons and necessities of such permission, set the duration of use and cancel it immediately after the end of the period.

C. User Account and Password Control

1. Establish concise identification and authentication protocol, like a requirement for a password difficult to guess. Each user must have his/her own user account. In determining whether passwords are difficult to guess and password control is tough, the Company will use the following factors for overall consideration:

- Passwords should have a fair length. Most international standards suggest a minimum length of 8 characters (alphabet and numeric).

- Contain special characters such as <, >, $, @ and #.

- General users should change passwords at least once every 6 months. Privilege users like system administrators and default users should change passwords at least every 2 months.

- The new password should not repeat the 3 most recent ones.

- Passwords should not set conventionally or predictably like “abcdef”, “aaaaaa”, “123456”, “password” or “P@ssw0rd”.

- Passwords should not contain users’ information like first name, last name, date of birth and address.

- Passwords must not be a word that appears in a dictionary.

- Set the number of times a user is allowed to enter the wrong password (Logon Attempt-Retires). Generally, it is limited at 5 times. Entering the wrong password more than the limits, the system or program will be blocked.

- Adopt a prudent and secure means to pass users their passwords, for instance, through a sealed envelope.

- Upon receiving a default password or a new password, users should immediately change the password.

- Users shall keep their passwords confidential. Do not write it on a paper and post it on the screen. If the passwords are known to others, the users shall immediately change the passwords.

- In case of sharing shared users licenses such as SAP system, system administrators will send an email notification to the person in charge to change the password when there is a change of affiliated users.

2. Encryption is required for password-storing file, to keep it safe from leakage or modification.

3. Check the list of users of critical systems on a regular basis. Check the list of users whose rights are terminated, including those who have resigned and default users. Suspend the users immediately upon detection, by disabling their access, removing them, changing passwords, etc.

9 Physical Security

The objective of Data Center Room Access Control is intended to prevent unauthorized persons from accessing, knowing, altering or damaging data and the computer network. Damage prevention is intended to protect data and the network from disasters or other factors. This section covers access control measures for Data Center Room and prevention systems the Company should provide in Data Center Room.

A. Data Center/ Server Room Control

1. Important computer equipment such as servers and network devices must be located in Data Center Room or a restricted area. Access to Data Center Room should be limited to only responsible persons such as system administrators.

2. Measures shall be in place if individuals without regular function need to access Data Center Room from time to time; for example, by requiring administrators and/or related operators to supervise such function thoroughly.

3. There should be Data Center Room's access log that contains details of involved persons and the time of their entry and exit. The log should be reviewed on a regular basis.

4. Data Center Room should be divided into separate sections, for Network Zone, Server Zone, UPS Zone and Batter UPS Zone and etc., for ease of operation and more efficient control over access to important computer equipment.

B. Damage Prevention systems

1. Fire Protection System

- Fire alarm system shall be installed, concerning smoke and heat detectors, to promptly prevent or extinguish fires.

- Main Data Center Room shall be equipped with automatic fire extinguisher. At secondary centers, there shall be at least fire extinguisher to first tackle fire incidents.

2. Power Failure Prevention System

- Install a system to protect computers from possible damage caused by power failure.

- Install power backup system for key computers and network, to ensure uninterrupted operation.

3. Temperature and Humidity Control System

- Maintain appropriate temperature and humidity level by setting air-conditioner's temperature and humidity control level in accordance with the computer system's specification or the computer system may not operate smoothly under unsuitable temperature and humidity.

4. Water Leakage Warning System

- In case Data Center Room floor is elevated for the installation of air-conditioners, electrical wires and network wires underneath the floor, the water leakage warning system should be installed to prevent or promptly tackle leakages. If Data Center/ Server Room is in a location vulnerable for water leaks, regular checks for possible leaks are advised.

10 IT Operational Security

The Objective of this clause is to ensure proper and secure operations of the Company's IT system, which will prevent information loss and protect the system from Malware.

1. Prepare manual or procedures concerning the Company's key IT systems, to prevent operational errors.

2. Put control on information modification; for example, a requirement for supervisors' approval before proceeding.

3. Back up information, before modifying it.

4. Install a monitoring system to check the sufficiency of IT system's resources such as CPU, Memory and Hard Disk and use the results in future planning to determine whether to increase or decrease resources.

5. Separate the development of critical systems from daily-operational systems, to prevent unauthorized data modification.

6. Survey and classify data levels; and define data that requires backup as well as backup frequency.

7. Critical data should be frequently backed up. The Company should have a data backup facility in an off-site location.

8. Examine IT data backup system's availability at least once a year.

9. Establish anti-malware measures including

- Install anti-virus program and address vulnerabilities of operating systems and web browsers prior to connecting personal computers or notebooks with the Company's network.

- Regularly update operating systems and programs following issued patches and/or HotFix to fix bugs in programs. Users can download updates from software companies' websites.

- Scan virus with an anti-virus program before sending or receiving email.

- Users must install the program prepared for by the Company. If users wish to install other software, they must notify Information Technology Department for safety check.

11 Communication Security

The objective of this clause is to protect data from individuals, virus and malicious codes which may access or cause damage to IT system's data or operations.

1. Network Security Management
2. Control access to ensure network's security.
3. Provide separate networks for internal users and external users.
4. Information Transfer integrity through encryption and agreements.

12 Outsourcing

The Objective of this clause is to protect the Company's accessible assets from IT outsourcing-related risks, while maintaining levels of security and service quality as agreed in service agreements.

1. Outline the Company's data security rules, when needing to grant the outsourced party an access to the Company's data or property. Such rules shall be aligned with the clauses in non-disclosure agreements.

2. Communicate and enforce data security rules when needing to grant the outsourced party an access to the Company's data or property, before approving the access.

3. Specify regular service monitoring, review and assessment schedules in service agreements.

4. In case of changes in the agreements for critical systems, security risk assessment is required.

13 Information security incident management

The Objective of this clause is to achieve streamlined and effective approaches in managing information security incidents and display the security situation and weaknesses of IT system.

1. Define the roles and procedures in tackling security incidents.

2. Establish a clear communication channel by which users can file reports on incidents related to IT system security.

3. If users find any incident that may interfere with IT system security to Information Technology Department.

4. Require reporting on the security situation of the IT system accordingly to the severity of incidents. An incident that will affect a large number of users must be announced quickly.

5. Record security breach incidents, at least the type of incidents, frequency and cost of damage, so that the Company can learn from the lessons and prepare preventive measures.

6. Gather and collect evidence in accordance with rules or guidelines, for reference in court proceedings.

14 Continuity Management

The Objective of this clause is to prevent business disruption, caused by crises or disasters, and ensure the availability of IT system equipment.

1. Demand Information Technology Department to prepare mitigation plans for uncertainties and disasters that IT system may encounter, in line with the Company's Crisis Management Plan.

2. Assess and evaluate information-related risks at least once a year.

3. Review continuity plan at least once a year.

4. Examine the availability of backup system at least once a year.

15 Development and Maintenance

The Objective of this clause is to control the development or modification of IT system for accurate and complete operational results in line with users' specifications, which will reduce integrity risks. This part covers the overall development or modification process, from requests to develop or modify work systems until the tasks are completed and implemented.

1. Create written processes or procedures for development or modification of work systems. At least, it should cover request; development or modification; testing; and work transfer processes.

2. Create procedures or guidelines on emergency changes in work systems. The necessity of such changes, which must be approved by authorized persons at all times, must be specified.

3. Communicate the details of those procedures thoroughly with users and related persons and monitor compliance.

- Development or Modification Control

a. Request

- Requests for the development and modification of work systems must be in writing, including in electronic forms like email. The requests shall be approved by authorized persons such as supervisors of the departments that submit the requests or system administrators.

- The written assessment of impacts on operation, security and functionality of relevant work systems from such changes shall be prepared.

- Relevant official rules should be crosschecked as several changes may interfere with compliance with official rules.

b. Work System Development

- Separate the computers for development purposes (Develop Environment) from operational computers (Production Environment) and limit access to each part only to relevant persons. The separation can be done by using two computers or by sharing space in a single computer.

- Requesters of the development or modification and relevant users should engage in the process to achieve desirable work systems.

- Throughout the process, from the first stage, give priority to security and availability of work systems.

c. Testing

- Involve requesters and Information Technology Department as well as other relevant users in the testing, to ensure the efficiency of the developed or modified work systems as well as accurate and complete processing prior to work transfer and implementation.

d. Work Transfer

- Regularly verify the work transfer.

e. Prepare document and details of the development process for safekeeping.

- Store details of the currently-used programs, concerning previous development and modification.

- Regularly update all related documents following each development or modification, including the details of data structure, work system manual, registration of eligible users, work process of the programs and program specification. The documents must be kept at a safe and convenient place.

- Keep the previous version of modified programs for emergency use, in case that the current version shows errors or fails.

f. Post-Implementation Test

- Schedule a test on a developed or modified program after implementation for a certain period, to ensure the work system's efficiency, accurate and complete processing, and ability to meet users' needs.

g. Change Communications

- To inform relevant users of changes for successful implementation.

16 Enforcement of this Code

All Directors, Executives, employees and associates including suppliers, joint ventures partners, consultants and service providers shall comply with this code in addition to any specific requirements as per the Agreements signed with Mega. IN the event of discrepancy between this Code and the Agreements/ documents, the Agreements/ documents shall prevail.

17 Non-retaliation

We do not tolerate retaliation against an employee or stakeholder who files a non-compliance incident report. Each report is and will be diligently investigated and appropriate remediation measures taken to prevent further wrongdoing and penalize aberrations in the past, to the extent such acts are determined in the inquiry to be in the nature of misconduct.