DISASTER RECOVERY POLICY

1. Purpose

The purpose of this Disaster Recovery Policy is to establish a comprehensive framework for preparing, responding to, and recovering from any disruptive event (whether natural or man-made) that may impact the operations of the company. This policy ensures the continued safety and integrity of products while meeting regulatory requirements under ISO 13485.

2. Scope

This policy applies to all areas of CliniSciences Group business, including:

- Importation, storage, and distribution of products.
- Equipment, facilities, and IT infrastructure used to support the QMS
- Personnel involved in the management, oversight, and distribution of products

3. Objectives

This policy aims to ensure the continuous availability of critical resources during and after a disaster while maintaining compliance with ISO 13485 requirements to guarantee that products meet safety, performance, and regulatory standards. By outlining recovery steps that will restore operations in a timely manner, the policy seeks to minimize the impact on patient safety, product quality, and customer satisfaction.

4. Disaster Recovery Team (DRT)

The company shall designate a Disaster Recovery Team (DRT) responsible for overseeing disaster recovery efforts, ensuring effective communication with employees, stakeholders, suppliers, and customers throughout the recovery process. Additionally, the DRT will ensure compliance with regulatory bodies, including making appropriate notifications of significant disruptions.

The Disaster Recovery Team should include representatives from key functions, such as:

- Management: to ensure strategic decisions and oversight.

- Quality Assurance (QA): to evaluate the impact on product quality and regulatory compliance.
- Operations/Logistics: to ensure the continuity of distribution and product supply.
- IT and Infrastructure: to restore data integrity, systems, and electronic records.

5. Disaster Recovery Plan (DRP)

The company must establish a Disaster Recovery Plan (DRP) with clear procedures for the following stages:

5.1 Prevention and Mitigation

The company will identify potential risks, such as natural disasters, cyberattacks, and transportation disruptions, and conduct annual risk assessments to implement preventative measures that minimize the likelihood of a disaster. Additionally, supplier reviews will be performed to ensure compliance with ISO 13485 requirements for product sourcing. To safeguard critical information, the company will also implement cybersecurity measures to protect essential data, including research data and medical device records.

5.2 Detection and Assessment

The company will develop mechanisms to quickly detect a disaster or major disruption through system alerts, environmental monitoring systems, and employee warnings. Upon detection, an assessment will be conducted to determine the scope and impact on the supply chain, facilities or infrastructures, and customer deliveries. Additionally, an immediate evaluation of compliance with ISO 13485 will be performed to assess any potential impact on the quality of products.

5.3 Response and Mitigation

Upon detecting a disaster or major disruption, the Disaster Recovery Team will be activated immediately to initiate the response plan. Clear and timely communication will be established with key stakeholders, including employees, customers, suppliers, and regulatory authorities, to provide updates and reassurance. The team will assess and contain any immediate risks to product quality, such as maintaining temperature control in storage facilities or addressing shipping delays for products. Additionally, appropriate

containment procedures will be implemented for any recalled or affected products to ensure compliance and minimize impact.

5.4 Recovery

Following a disaster or major disruption, operations will be prioritized based on criticality and impact on product availability, with a focus on restoring high-priority activities. Key efforts will include the importation and distribution of critical products and maintaining compliance with regulatory authorities to ensure products' safety. Systems and infrastructure, such as warehouse operations, inventory systems, and electronic document controls, will be restored as quickly as possible. Any recovered or modified products will undergo thorough assessment to ensure compliance with ISO 13485 and regulatory requirements before resuming normal processes with necessary quality controls in place. Additionally, employees will receive training or briefings on lessons learned and process improvements to enhance future preparedness.

5.5 Post-Recovery Review

After recovery, a post-recovery review will be conducted to identify the root causes of the disaster and evaluate the effectiveness of the response efforts. Corrective actions will be implemented as needed, including updates to risk management and contingency procedures within the QMS. If necessary, Regulatory authorities, customers, and stakeholders will be notified of the resolution of the incident and any changes to operational procedures. Additionally, the Disaster Recovery Plan will be updated with findings from the review to strengthen future response efforts.

6. Critical Infrastructure and Resource Management

To support the recovery of operations, critical infrastructure will be identified and protected across key areas. Supply chain continuity will be ensured by advising suppliers to have contingency plans in place.

Data integrity and availability will be safeguarded through regular backups of essential information, such as product registration and quality control records, along with alternative access to systems in case of IT failures.

Additionally, physical infrastructure, including warehouses and laboratories, will be secured against environmental risks, with spare parts and backup equipment readily available to maintain operational stability.

7. Communication Plan

A robust communication strategy is essential for managing internal and external stakeholders:

- Establish predefined communication templates for notifying employees, customers, and suppliers (refer to Annex I of this document).
- Maintain an up-to-date list of emergency contacts, including regulatory bodies, suppliers, and customers in the ERP System.

8. Training and Awareness

Conduct regular training sessions on disaster recovery protocols for employees involved in critical processes. Test recovery procedures through periodic drills to ensure team readiness and identify areas of improvement.

Ensure that employees are familiar with the ISO 13485 requirements for disaster recovery and that the quality management system is continuously maintained.

9. Review and Revision

This policy shall be reviewed annually and revised as needed to ensure its continued effectiveness and relevance to the company's operations. All revisions will be documented, and employees will be notified of any changes.

Tushendan RASIAH (CEO of CliniSciences Group)

ANNEX I - Predefined communication templates for notifying employees, customers, and suppliers

****Subject:** Important Update on Business Operations**

Dear [Supplier/Customer's Name],

We hope this message finds you well. We want to inform you that our company recently experienced an unforeseen disaster affecting our operations. While this has caused some disruptions, we want to assure you that we have activated our Disaster Recovery Plan and are working diligently to restore full functionality as quickly as possible.

Our team is prioritizing the continuity of product supply, quality, and compliance with all regulatory requirements. If there are any anticipated delays or impacts on our service to you, we will keep you informed and work closely with you to minimize any inconvenience.

Your trust and satisfaction are our top priorities, and we appreciate your patience and understanding during this time. If you have any immediate concerns or questions, please do not hesitate to contact us at [contact details].

Thank you for your continued support.

Best regards,

[Your Name]
[Your Position]
[Company Name]
[Contact Information]

ANNEX II - Disaster Recovery team and its defined tasks

Short-term actions

Management

- Ensure Personnel Safety: confirm that all staff are safe and accounted for. QA should support HR in this task.

- Manage personnel of the company to eliminate/resolve the cause of the disaster as quickly as possible.

Operations manager

- Make sure that critical controlled environments (labs, storage areas) are sealed or protected.
- Make sure that equipment is not affected, and if it is, activate the adequate backup plan.

Quality Assurance (QA)

- Evaluate whether products have been compromised (temperature excursions, contamination, etc.).

IT manager

- Secure and back up electronic systems (LIMS, QMS, ERP) and paper records to prevent loss of traceability.

Long-Term Actions

Management

- Perform CAPA Investigations: root cause analysis of all disaster-related issues and define Corrective and Preventive Actions.

Quality Assurance (QA)

- Update Quality Risk Management Files: reflect the disaster scenario in your QRM documentation and adjust mitigation plans accordingly.
- Revise SOPs and Emergency Protocols: Learn from the event and improve your response procedures (e.g., include more robust backup systems or secondary suppliers).
- Open a NC: keep thorough records of what happened, how it was handled, and what was improved.

- Train Personnel on Changes: conduct training for any new procedures or emergency protocols introduced after the event.

Operations manager

- Support Requalification/Validation Activities: revalidate impacted processes, equipment, and systems (IQ/OQ/PQ if needed).
- Train Personnel on Changes: conduct training for any new procedures or emergency protocols introduced after the event.

IT manager

- Restore all affected electronic systems and ensure the website/ERP is functioning properly.