NEW STRUCTURE VERSION

CURIUM CODE OF BUSINESS CONDUCT

INTRODUCTION

Dear Colleagues,

Curium's current and future success is based on living our values. At the foundation of these values is total integrity, highest ethical standards and compliance with all applicable laws, regulations and rules.

We operate in a heavily regulated industry. Many behaviours, actions or inactions can damage our Company's name, reputation or credibility. Therefore, all of us who represent Curium in any position or capacity should be personally committed to comply with the Curium Code of Business Conduct ("Code of Conduct") and spread within our organization a culture in which integrity and compliance with this Code is constant and a priority. Unethical or dishonest behavior cannot be tolerated.

You are requested to acknowledge having read this Code of Conduct and performed the short training exercise included herein.

Thank you for all you do for Curium, your colleagues, our customers and their patients.

Who is covered by this policy?

The Code of Conduct applies to everyone working for and on behalf of Curium; employees, consultants, officers, directors, distributors and agents (each a "Curium Stakeholder").

We also expect all of our business partners and suppliers to uphold the same standards and, where considered necessary, to adhere to the Code of Conduct.

What is expected of me?

It is your responsibility:

- to read and understand the Code of Conduct and to keep yourself updated on our Company's policies,
- to follow the standards expressed by the Code of Conduct in your day-to-day work,
- to seek guidance and training when you have questions or doubts about the Code of Conduct,
- to be alert to actions by employees or third parties that do not comply with our Code of Conduct,
- to speak up if you become aware of non-compliances with the Code of Conduct and,
- to cooperate fully and transparently in all compliance related matters
- to complete from time to time, the training exercises and, if and when applicable, the self-certification confirmation forms.

How to report a suspected violation of the Code of Conduct?

As Curium Stakeholder you are requested to report any conduct you believe in good faith does not comply with the Code of Conduct or the law. By reporting compliance concerns you are acting in the spirit of our Code and helping to protect our business and our reputation. If you have compliance concerns, it is generally best to talk to your manager who will further report the concern to the Compliance Office. You can also report your concerns anytime to a manager of higher rank, Human Resources or directly to the Compliance Office depending on the nature of the concern.

No Retaliation

You must feel comfortable raising concerns or non-compliances with the Code of Conduct and you should have no fear of retaliation. Curium will not tolerate any retaliation against persons who report concerns in good faith.

Compliance Office

The Compliance Office is comprised of the Chief Legal Officer, the SPECT US General Counsel and the SPECT International General Counsel. The Compliance Office is fully autonomous in its functions and directly reports to the Board of Directors. The Compliance Office has the power to give advice independently in the decision-making process and always ensures that their work is not tempered with possible conflicts of interests between the Compliance Office and other departments of Curium. In any case, the Compliance Office is protected and shall not be blamed for any action taken in case management decided not to act or not to investigate against the criterion of the Compliance Office.

The Compliance Office will ensure the security and the confidentiality of information collected. Taking into account such information, the Compliance Office will carry out a thorough analysis to decide on the adoption of appropriate measures concerning issues raised about compliance matters. If it deems appropriate, the Compliance Office may contract with an external service provider to carry out an investigation.

Emails sent to the Compliance Office (Compliance.Office@curiumpharma.com) will arrive correctively to the Chief Legal Officer, the SPECT US General Counsel and to the SPECT International General Counsel.

Rules of Construction

In interpreting and construing this Code of Conduct: (a) words in the singular shall be deemed to include the plural and vice versa as the context requires, (b) words of one gender shall be deemed to include the other gender as the context requires, (c) the word "including" and words of similar import means including without limitation, unless otherwise specified, (d) the word "or" shall not be exclusive; and (e) references to "written" or "in writing" include in electronic form.

References to "Curium", "we" and the "Group" in the Code of Conduct refer to the worldwide family of Curium companies.

References to "Company" in the Code of Conduct refer to the global Curium organization (i.e., the Group) or, if the context requires, the specific Curium entity for which you serve in the capacity of employee, consultant, officer, director (sub-)contractor, distributor or agent.

References to "these rules" refer to the requirements and prohibitions set out in the Code of Conduct.

Q&A

Q: I have a concern about the actions of a colleague. How should I report this?

A: The most important thing is to raise your concern – it does not matter which route you choose. If you feel comfortable talking to your manager, do that. Your manager is there to support and help you

choose the correct course of action. You can also simply refer by email to Compliance.Office@curiumpharma.com and one of the three persons listed above will contact you directly.

Q: Can I remain anonymous?

A: If reported to the Compliance Office, the confidentiality of the report may on request be ensured. In any case, please note that Curium complies with applicable laws concerning the protection of the whistle-blower. Indeed, if a whistle-blowing case happens, Curium will not retaliate against the whistle-blower for reporting misconduct and Curium will establish support measures to ensure adequate protection of the whistle-blower.

Chapter 1 – Social and Environmental Matters

A. Protecting Human Rights and Celebrating Diversity

Our people are our most valuable resource. It is our responsibility to ensure we provide a sustainable working environment with fair terms and conditions for everyone working for us.

HUMAN RIGHTS. We respect and work in line with internationally proclaimed human rights and ensure that we do not abuse any part of the human rights principles.

NO DISCRIMINATION.

General provisions

At Curium, each person must be able to work in a comfortable, productive work environment free from offensive, disrespectful or harassing behavior. Working for Curium, you must treat your colleagues and any other person you interact with in the professional context with respect, dignity and common courtesy. Nobody should be discriminated against due to age, race, gender, religion, sexual orientation, marital status, social origin, political opinion or ethnic background.

Definitions

Harassment includes but is not limited to discriminatory, abusive, or offensive verbal, visual, or physical conduct directed at a person because of his or her race, religion, gender, sexual orientation, veteran status, or any characteristic whether or not protected by applicable law or regulation.

Sexual harassment is a type of harassment which encompasses unwelcome sexual advances (either verbal or physical), requests for sexual favors, or any other verbal, visual, written, or physical conduct of a sexual nature. It encompasses but is not limited to submission to such conduct that is made either explicitly or implicitly a term or condition of an individual's employment (e.g., promotion, training, hiring, work assignments, pay, etc.). Such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile or offensive work environment.

Procedures

In case of harassment, a person witnessing or who is a victim of this type of behavior may inform the person engaging in the harassment that his conduct is offensive and that he must immediately put an end

to it. If the victim does not wish to act directly, he may report the offense to his Manager, to HR or to the Compliance Office.

Curium shall promote a harassment-free work environment and be proactive when advised with a harassment claim. When aware of harassing behaviors, Supervisors and Managers shall act promptly to stop the offensive behavior and shall report this incident to HR. HR shall be notified by Supervisors and Managers even if the employee(s) involved seems reluctant to come forward or requests that the information be kept confidential. In that case, the Manager or Supervisor should inform the employee that the information will be handled as confidentially as possible, but it must be disclosed to the extent necessary to conduct an appropriate investigation and resolve the harassing situation.

Complaints
Complaints can be written or verbal, they can be made through the phone, in person, or by other means. The recipient of a complaint shall forward this complaint to HR, unless the complaint involves HR employees.

Curium Stakeholders may be interviewed in the course of the investigation. They shall answer truthfully to the questions they're asked and keep confidential the information they learn about the matter under investigation, except to the extent necessary to support the investigation an any associated disciplinary process.

Sanctions
Any person who, in the opinion of the Company, is found to have engaged in harassment will be subject to disciplinary action up to and including termination of employment or contract. Discipline will be applied in accordance with applicable laws and/or collective bargaining agreements. The person found to have engaged in harassment may be required to participate in appropriate training or counseling or other remedial measures.

DIVERSITY.

General provisions
As an inclusive organization, Curium believes that a diverse workforce and a respectful work environment are essential components of a thriving innovative and sustainable business. Our workplace is built on respect for each other, honesty and integrity and we celebrate the diversity of all employees and partners represented by this global company.

Equal opportunity and fair treatment are expected to be applied to all employees in all employment decisions. Curium prohibits any form of discrimination that violates this Code of Conduct and/or the laws of the countries in which we do business.

Discrimination in our workplace activities is not allowed on the basis of the following characteristics whether or not prohibited by country or local law:

- Age
- Disability
- Gender or Gender Identity
- National Origin
- Religious beliefs

* Culture and language
* Ethnicity
* Marital or family status
* Race or color
* Sex or Sexual Orientation

Curium will comply with all civil rights, human rights, environmental, and labor laws in the countries in which we operate. This means we will act in a socially responsible way, prohibit child labor, and provide clean and safe work environments for all stakeholders globally. Curium employees and contract staff (collectively, "Personnel") are also expected to respect the diversity of our customers and suppliers in the same way we value differences of our own people.

Sanctions
Violation of these provisions about diversity may result in disciplinary action up to and including termination of employment or contract in compliance with applicable local law and/or collective bargaining agreements.

FAIR EMPLOYMENT AND REMUNERATION.

We embrace fair employment practices where all Personnel have the same opportunities for a job based on qualification and merit, taking into account job requirements such as education, prior experience, skills, performance, values, leadership and other relevant criteria. We also aim to ensure that similarly situated employees with the same experience and qualifications receive equal pay for equal work. Everyone who works for Curium should have the right to fair wages according to local conditions and working time that complies with applicable regulations and collective bargaining agreements, including time to rest, overtime and holidays.

FREEDOM OF ASSOCIATION.

We recognize and respect the freedom of our Personnel to be a member of any employee organization of their choosing. Where employees are represented by a legally recognized trade union, we establish a constructive dialogue and engage in negotiations or consultations as required with their representatives.

Q&A

Q: A colleague is recruiting a new team member. I am concerned that they may be discriminating against my female colleague who is pregnant but interested in the job. What can I do?
A: You are right to raise your concern as we will not tolerate any form of discrimination. You should first of all urge your colleague to discuss the selection criteria with the HR manager. If there is no change, then you should raise the issue with your manager, another senior manager or the Compliance Office.

B. Healthy and Safe Work Environment

Curium is committed to creating and maintaining a safe working environment at all sites and preventing workplace accidents and injuries. All necessary precautions for a safe and sound work environment must be met regardless of whether you work at an office or a manufacturing site. Everyone with a job that requires specific safety instructions and protection will receive all necessary training prior to starting the work and the workplace must be equipped with adequate protection materials and tools. We do not tolerate the abuse of drugs or alcohol in the workplace.

Q&A

Q: What should I do if I suspect that a colleague is operating equipment under the influence of alcohol or drugs?

A: You should let your colleague know that this is not appropriate, and you should also report this incident to your line manager or the Human Resources department.

C. Promoting Global Sustainability

SUSTAINABILITY. Curium is committed to act ethically and in a socially and environmentally responsible manner at all times in combination with maintaining sound financial results and good governance. The principles in our Code of Conduct are all cornerstones in building a sustainable company for the future.

HIGH STANDARDS ON SUPPLIER. As described in this Code of Conduct, we have set high standards on the way we do business and we expect the same from our suppliers in their own businesses and their business relationships. In many cases, suppliers have implemented their own codes, and these should be substantially in line with, and comply with, our standards as a prerequisite to doing business. In specific situation, we may ask a supplier to adhere in writing with this Code of Conduct.

REDUCING ENVIRONMENTAL IMPACT. We are committed to reducing the environmental impact of all operations in the Company and of our products and solutions. We strive to effectively utilize all types of resources needed to support this commitment when products and processes are developed and implemented, for example, energy, natural resources and raw materials. We also aim to minimize waste and emissions to air and water, and recover or recycle materials, water and energy wherever feasible and practical. We avoid materials and methods that may cause health or environmental risks and avoid the use of hazardous materials whenever possible.

D. Handling Conflicts of Interest

A conflict of interest arises when a Stakeholder has a personal interest, directly or due to his close association with another person (such as a relative, friend, competitor, supplier, customer, distributor or agent), that could influence his professional activities performed for Curium. Every decision and financial commitment must promote the goals and objectives of Curium. Curium Personnel may engage in legitimate and lawful financial and other activities outside working hours so long as those activities do not create a conflict with or otherwise harm Curium's interests. There are many possible scenarios that can create a conflict of interest – some of which may not be obvious. These are some examples:

- Accepting personal gifts or entertainment from competitors, customers or suppliers
- Working for competitors, suppliers, customers, distributors or agents or holding shares or interest in any such entities
- Engaging in any work in competition with Curium or using directly or indirectly your position in Curium
- Employing close relatives, especially when those relatives report directly or indirectly to the Curium employee
- Using a supplier in which a friend or relative has a financial interest or plays a role.

Q&A

Q: Are there any guidelines to help me avoid potential conflicts of interest in interactions with suppliers with whom I have become close?

A: You can ask yourself these questions to determine whether the relationship with the supplier can expose you to a conflict of interest, or the appearance of a conflict:

- Is it a personal friendship or a friendly professional relationship?
- Do you fear that your personal loyalty may compromise your ability to objectively evaluate the supplier and make decisions in Curium's best interest?

You should discuss with your manager to avoid any potential or appearance of a conflict of interest.

Q: What should I do if I receive a personal gift from a supplier in a country where refusing business gifts can be seen as an insult?
A: In situations where rejecting the gift is culturally impolite and can damage the relationship, you should accept the gift on behalf of Curium and turn it over to your manager for proper disposition by Curium. If unsure, consult the Compliance Office for guidance.

E. Communication with Media and Investors

FINANCIAL INTEGRITY

In order to maintain our investors' trust and fulfil our accountability with them, we must record all transactions promptly, accurately, completely and honestly in accordance with applicable internal and external financial and accounting principles, standards and regulations. We never alter or manipulate source documents, accounting entries or financial statements to achieve a forecasted or desired result.

EXTERNAL COMMUNICATION AND FINANCIAL DISCLOSURE

All our communication, through whatever channel, shall be truthful, reliable, timely and appropriately authorized in accordance with Curium's Delegation of Authority. Everyone working for Curium must be mindful of situations in which they may be perceived to be communicating on Curium's behalf. Only authorized representatives should communicate publicly on Curium's behalf and all questions from third parties should be reported to the Compliance Office prior to being answered.

Curium is a privately held company, and so, except as required by local statutes, public disclosures of financial information is limited and less frequent as compared to publicly traded companies. All financial communication from Curium shall be authorized by senior management within the Finance or Treasury Department, distributed only to the approved recipient(s), and supported with correct and relevant facts and circumstances.

Q&A
Q: I was asked to sign my name on a sales contract using a date from two weeks ago. This does not seem right. What should I do?
A: Falsifying information in Company documents, like contracts, can lead to the improper recording of transactions in violation of accounting rules and financial regulations. No employee should ever prepare or sign a document in a manner that misrepresents the underlying facts. You should contact the Compliance Office for guidance on specific contract-related questions.

Q: I incur business expenses infrequently and, whenever I do, the amounts are not very large. Do I need to worry about coding the expenses properly when I submit my expense report?
A: Yes. Each Curium employee must make sure the Curium books and records they create – including internal expense reports – honestly and accurately reflect the underlying transaction or expenditure. No employee may allow a record to be entered that is inaccurate, incomplete or misleading.

Chapter 2 – Anti-Corruption Matters

A. Introduction

Our business dealings are heavily regulated by laws. Breaking these laws can result not only in significant fines but also in criminal penalties for the Company and us as individuals. These laws prohibit bribery and other corrupt dealings, such as kickbacks, that may improperly influence the decisions or actions of others.

Curium Stakeholders must conduct their activities in full compliance with this Chapter, the laws of the country where located and all applicable anti-corruption laws, including local anti-corruption laws, the UK Bribery Act and the United States Foreign Corrupt Practices Act ("FCPA"). Improper actions are prohibited, whether carried out directly by Curium Personnel or indirectly through a third party such as a distributor, agent or consultant.

Curium Personnel should report any potential violations to the Compliance Office. Curium Personnel should abide by and participate in the Company's regional or local Anti-Corruption training. Curium Personnel must understand that failure to comply with the FCPA, UK Bribery Act and any other applicable anti-corruption laws may result in prosecution, with penalties including fines and/or imprisonment.

This Chapter provides a general guide to anti-corruption compliance. It does not address every potential scenario that may raise issues bearing on compliance with Anti-Corruption Matters. Therefore, any Curium Personnel who have any questions concerning the requirements of this Chapter should consult with the Compliance Office.

B. Curium Personnel Shall not be Permitted to Pay or Receive Bribes

Curium prohibits accepting anything of value from any person or company when it is designed to influence an action or obtain an improper advantage. This applies in every country around the world and to interactions with both governments and the private sector. Everyone working for or on behalf of Curium must also follow all applicable laws and regulations pertaining to interactions with healthcare professionals ("Healthcare Professionals" or "HCPs" further defined hereunder in point E) and officers or employees of a government, political parties, party officials, and candidates for political offices (collectively, "Government Officials"). While some anti-corruption laws are focused on interactions with foreign Government Officials, for purposes of this Code of Conduct the term Government Officials includes also such officials in any country, and the rules set forth in this Chapter ("Anti-Corruption Rules") shall apply accordingly.

Curium Stakeholders are not permitted to give or offer anything of value, directly or indirectly, to any Government Official or any commercial party for the purpose of improperly obtaining or retaining a business advantage or unduly influence others in business dealings. "Anything of value" should be broadly interpreted to include cash, gifts to family members, forgiveness of a debt, loans, personal favors, entertainment, meals and travel, political and charitable contributions, business opportunities and medical care, among other items. Simply put, bribes, kickbacks or similar payments are never permitted, whether made to a HCP, a Government Official or to customers, investors, clients or other private parties. Opportunities that are subject to making improper payments must be turned down.

If confronted with a request or demand for an improper payment or other action that would violate this Chapter, the request or demand must be immediately rejected and reported to Curium's Compliance Office. Similarly, if any person knows or believes that an improper payment has been or will be made, that person must report such payment to the Compliance Office.

Q&A
Q: From time to time I provide meals, gifts, travel and entertainment to customers. Is this appropriate?
A: Providing business courtesies can be an appropriate way of doing business, but only under the right circumstances. There are a variety of laws that govern business courtesies. These laws are complex, differ from country to country and can have serious repercussions for our Company. Before offering or providing a business courtesy, make sure it satisfies all the guidelines and requirements in Curium's Anti-Corruption Rules and consult the Compliance Office in case of doubt.

Q: I have a suspicion that one of Curium's distributor sales representatives has been making improper payments to an end customer. I do not think anyone at Curium was involved. Should I report this?
A: Absolutely. Both Curium and our employees, directors or officers can be held liable for the actions of third parties, even if we were not directly involved. Report this to the Compliance Office immediately.

Q: A Curium distributor has asked for an additional product discount above and beyond our regular discount due to unexpected government fees. Do we need to look into this?
A: Yes, we must clearly understand what additional fees the distributor is being asked to pay. This makes good business sense and helps ensure these are valid charges that cannot be viewed as a bribe.

C. Additional Anti-Corruption Rules

This Chapter sets forth various rules relating to gifts, entertainment, travel, meals, lodging and employment. All such expenditures must be recorded accurately in the books and records of the Company, in accordance with Section F below.

a. Gifts

As a general matter, Curium competes for and earns business through the quality and reliability of its products and services, and the expertise and dedication of Curium Personnel, not through gifts or lavish entertainment. The use of Curium funds or assets for gifts, gratuities, or other favors to Government Officials or any other individual or entity (in the private or public sector) that has the power to decide or influence the Curium's commercial activities is prohibited, unless all of the following circumstances are met.

- the gift does not involve cash or cash equivalent gifts (e.g., gift cards, store cards or gambling chips);
- the gift is permitted under applicable industry codes of ethics as adopted by the Company or the applicable regional business unit (e.g., the Code on Interactions with Healthcare Professionals as issued by the Pharmaceutical Researchers and Manufacturers of America);
- the gift is permitted under both local law and the guidelines of the recipient's employer;
- where required, the gift has been approved or notified to the competent local authorities;
- the gift is presented openly with complete transparency;
- the gift is properly recorded in the Company's books and records;
- the gift is provided as a token of esteem, courtesy or in return for hospitality and should comport with local custom; and the item costs less than EUR 200 or USD 250, and no gift in aggregate should exceed a value of EUR 500 or USD 600 for one single party over a period of six months. If local Curium leaders have established lower limits, the related Curium Personnel must comply with such lower limits.

Gifts that do not fall specifically within the above guidelines require advance consultation and approval by the Compliance Office.

Note that the Rules in this Chapter concerning gift giving and the associated reporting requirements apply even if Curium Personnel are not seeking reimbursement for the expenses (i.e., paying these expenses out of your own pocket does not avoid these requirements).

Curium Personnel must not accept nor permit any immediate family member to accept any gifts, gratuities or other favors from any customer, supplier or other person doing or seeking to do business with Curium, other than items of nominal value. Any gifts that are not of nominal value should be returned immediately and reported to your supervisor. If immediate return is not practical, they should be given to Curium management for charitable disposition.

b. Meals, Entertainment, Travel and Lodging

Common sense and moderation should prevail in business entertainment and the payment of travel and lodging expenses engaged in on behalf of the Company. Curium Stakeholders should provide business entertainment to or receive business entertainment from anyone doing business with Curium only if the entertainment is infrequent, modest and intended to serve legitimate business goals.

Meals, entertainment, travel and lodging should never be offered as a means of influencing another person's business decision. Each should only be offered if it is appropriate, reasonable for promotional purposes, allowed under applicable industry codes of ethics, offered or accepted in the normal course of an existing business relationship, and if the primary subject of discussion or purpose of travel is business. The appropriateness of a particular type of entertainment, travel and lodging of course, depends upon both the reasonableness of the expense and on the type of activity involved. This is determined based on whether or not the expenditure is sensible and proportionate to the nature of the individual and entity involved. Adult entertainment is strictly prohibited.

Expenses for meals, entertainment, travel and lodging for a HCP, Government Official or any other individual or entity (in the private or public sector) that has the power to decide or influence Curium's commercial activities may be incurred without prior approval by the Compliance Office only if all of the following conditions are met.

- The expenses are bona fide and related to a legitimate business purpose and the events involved are attended by appropriate Company representatives;

  The cost of the meal, entertainment, travel or lodging by person is less than:
  * Breakfast: EUR 50/USD 60
  * Lunch or Dinner: EUR 200/USD 240
  * Refreshments unaccompanied by a meal: EUR 50/USD 60 per person
  * Travel: economic class only and limited to a reasonable number
  * Hospitality (Hotel): reasonable in consideration of the date and place

  Note, however, that if local Curium leaders have established lower limits, the related Curium Personnel must comply with such lower limits.

- The meal, entertainment, travel or lodging is permitted by the applicable industry codes of ethics as adopted by the Company or the applicable regional business unit, and by the rules of the recipient's employer (if applicable).

For more detailed information concerning this topic, please refer to the Travel Expenses Policy.

c. Employment/Internships

On occasion, HCP's, Government Officials or Curium's business partners may request that Curium provide internships or employment to certain individuals (or the other way round). Offering internships or employment to HCP's, Government Officials or Curium's business partners may be viewed as providing an item of value.

It is inappropriate to hire an individual to influence the decision making of a HCP, Government Official or a business partner. If a candidate is interviewed for an internship or employment within the ordinary course of filling a position, the Compliance Office must be notified of the candidate's relationship to a HCP, Government Official or Curium's business partner. If a candidate related to a HCP, Government Official or Curium business partner is interviewed outside of the ordinary course of filling a position, any internship or employment offer must be pre-approved by the Compliance Office.

d. Political Contributions, Charitable Donations, Sponsoring Expenses

Curium Stakeholders may not make political contributions, charitable donations or Sponsoring expenses, whether in their own name or in the name of Curium, to obtain or retain business or to gain an improper business advantage. Any political, charitable or sponsoring contributions by Curium must be permitted under the law, permissible pursuant to the terms of this Chapter, made to a bona fide organization, and in the case of political contributions or charitable contributions connected to any HCP or Government Official or government entity made with the prior approval of the Compliance Office. In certain instances where there is heightened risk of corruption, the Compliance Office may require diligence to be conducted. The Compliance Office must be notified if a Government Official solicits a political or charitable contribution in connection with any government action related to Curium.

D. Relationships with Third Parties

Anti-corruption laws prohibit indirect payments made through a third party, including giving anything of value to a third party while knowing that value will be given to a HCP, Government Official or business partner for an improper purpose.

Curium Stakeholders who deal with third parties (e.g., distributors, agents, promoters, lobbyists, etc.) are responsible for taking reasonable precautions to ensure that the third parties conduct business ethically and comply with this Chapter. Curium Stakeholders retaining third parties that will be representing Curium before HCP's or governmental entities must discuss the engagement with the Compliance Office prior to hiring the third party. Any doubts regarding the scope of appropriate due diligence efforts in this regard should be resolved by contacting the Compliance Office.

In addition, once a third party is engaged, Curium Stakeholders who deal with third parties must always be aware of potential red flags. Red flags are certain actions or facts which should alert that there is a high possibility of improper conduct by a third party. A red flag does not mean that something illegal has happened, but rather that further investigation is necessary. Red flags are highly fact-dependent, but some examples of red flags are:

- Unusual or excessive payment requests, such as requests for over-invoicing, up-front payments, ill-defined or last-minute
- payments, success fees, unusual commissions or mid-stream compensation payments;
- Requests for payments to an account in a country other than where the third party is located or is working on behalf of the Company;
- Requests for payment to another third party, to a numbered account without associated name or in cash or other untraceable funds;
- Requests for political or charitable contributions;
- The third party is related to a HCP or a Government Official or has a close personal or business relationship with a HCP or a Government Official;
- Any refusal or hesitancy by the third party to disclose its owners, partners or principals;
- The third party uses holding companies or other methods to obscure its ownership, without adequate business justification;
- The third party expresses a desire to keep his representation of the Company or the terms of his retention secret; or
- The third party has little experience in the industry but claims to "know the right people".

- If a Curium Stakeholder has reason to suspect that a third party is engaging in potentially improper conduct, the Curium Stakeholder shall report the case to the Compliance Office immediately. Curium shall conduct an investigation and stop further payments to the third party if the Curium Stakeholder's suspicions are verified through the investigation.

E. Transparency on Interactions with Healthcare Professionals

For purposes of this Code of Conduct, a Healthcare Professional, or HCP, is broadly defined as any person in a position to purchase, prescribe, administer, recommend, or arrange for the purchase of a Curium product, including, but not limited to, doctors, nurses, office practice managers, pharmacists, medical directors, practice managers, and pharmacy benefits managers, as well as any individuals employed by such entities who are in a position to influence, recommend, or arrange for the purchase, sale, or prescription of Curium products, or who are affiliated with: (i) formulary or pharmacy & therapeutics committees and boards; (ii) tender committees; (iii) committees associated with the development of treatment protocols or standards (e.g., developing clinical guidelines); or (iv) healthcare institutions, medical committees, or other medical or scientific organizations.

Building long-term relationships with our customers is critical for our success. We achieve this by establishing Curium as a trusted partner that can always be counted on to act openly and honestly. This applies especially in our interactions with HCP's who can influence customer decisions about our products and services. We must ensure these interactions are guided by the highest standards of integrity. We may only engage the services of HCP's when there is a legitimate business need and value for Curium and must never pay more than an appropriate market rate for services rendered. Providing something of value to a HCP in return for a favorable decision or other business advantage is prohibited. Anything of value offered or provided to a HCP must be made openly and properly documented and must comply with all applicable laws (which may impose a prior approval or reporting process).

Curium Personnel shall comply with the disclosure requirements of any grant, remuneration, gifts or any other benefit allocated to HCP's and for such purpose shall communicate all pertinent information to the Compliance Office and other internal organization in charge of loading and officially declaring the grant to health governmental agencies using the official centralized dedicated platforms in each jurisdiction.

Q&A
Q: We will host an international conference and would like to hire a doctor to make a speech. Is that okay?
A: Yes, as long as there is a genuine need for the speech and the compensation is consistent with fair market value. There should be no real or perceived connection to the purchase of Curium products. The services should be properly documented and may need to be disclosed to the doctor's institution and reported to the government according to local laws and procedures. Consult the Compliance Office for guidance.

Q: A customer has asked Curium to make a charitable donation to a non-profit charity and indicated that such a donation would help secure Curium as a vendor of choice. Can Curium make the donation?
A: No. Even if the donation were used by the charity for a legitimate charitable purpose, donating Curium money in return for preferential customer treatment would not be appropriate and would violate the law.

F. Recordkeeping and Internal Controls

These rules require that all expenditures made by Curium are accurately reflected in Curium's financial records and that all payments made with Curium funds, or on behalf of Curium, have been properly authorized. Curium Stakeholders must follow all applicable standards, principles, laws and practices for

accounting and financial reporting. Curium Stakeholders must be timely, accurate and comprehensive when preparing all reports and records required by management and/or applicable law. In particular, Curium Stakeholders should ensure that no part of any payment is to be made for any purpose other than that to be fully and accurately described in Curium's books and records. Curium Stakeholders should use best efforts to ensure that all transactions, dispositions, and payments involving Curium funds or assets are properly and accurately recorded in the Company's financial records. No undisclosed or unrecorded accounts are to be established for any purpose. False or artificial entries are not to be made in Curium's books and records for any reason. Finally, personal funds must not be used to accomplish what is otherwise prohibited by these rules.

Curium will conduct periodic audits of its books and records to monitor compliance with these rules.

G. Compliance Procedures and Training

In addition, Curium may set up anti-corruption compliance training programs to educate Curium Personnel about the requirements and obligations of anti-corruption laws and these rules. All Curium Personnel of the Company should participate in such training.

H. Reporting Requirements and Whistleblower Protection

Curium takes its commitment to anti-corruption compliance very seriously and expects all Curium Stakeholders to share that commitment. Curium therefore expects and requires any Curium Stakeholder who has knowledge of, or reason to suspect, any violation of these rules to contact the Compliance Office immediately. Reports may be made anonymously, unless local procedures demand otherwise in certain cases (e.g., harassment complaints).

As a reminder, it is Curium's rules that, if the report of known or suspected violations is made honestly and in good faith, no adverse employment-related action will be taken against any Curium Personnel in retaliation for reporting a violation or suspected violation of anti-corruption laws or this Chapter.

Chapter 3 – Antitrust Matters

A. General Provisions

Competition or antitrust laws are aimed at ensuring a true and free competition with our competitors, on an equal footing with no unfair advantages. These laws are based on the principle that a competitive marketplace promotes consumer welfare and efficiency. Competition laws are very complex, global in reach and their application to a particular situation can vary based on a range of factors (e.g., market share, business rationale, timing relative to other market events). It is very important that you work closely with the Compliance Office to make sure we are not inadvertently engaging in anti-competitive activities.

Curium operates in markets with particular characteristics and a limited number of competitors. This imposes greater constraints on Curium's actions than might otherwise be the case.

Any Curium Stakeholder who becomes aware of any potential antitrust violation, or who is solicited to commit a potential antitrust violation must immediately call the Compliance Office.

Q&A
Q: I will be meeting a competitor at a conference next week. Am I allowed to talk about a deal I know we're both bidding on?

A: No. Any exchange of information that might manipulate the normal competitive conditions of the market in question, or coordinate the activities of competitors, can be viewed as a violation of competition law. Sharing sensitive business information is unacceptable.

B. Basic Antitrust Rules

ALWAYS
If you have any concerns about antitrust laws, call the Compliance Office.
Engage in vigorous competition with your competitors.
Call the Compliance Office if a competitor shares with you information about its prices or bidding plans.
Avoid even the appearance of impropriety in dealings with competitors or in relation to a bid opportunity.
Terminate any discussion or meeting that appears improper and call the Compliance Office.
NEVER
Exchange pricing information with a competitor.
Discuss bids with competitors.
Divide or allocate customers or markets or bid opportunities with a competitor.
Condition the purchase of one product on the purchase of another product.
Hesitate to contact the Compliance Office for guidance and advice.

C. Purpose and Reach of Antitrust and Competition Laws

Antitrust laws are designed to preserve a competitive economy. A core principle is that it is most efficient (and customers are better off) when the forces of supply and demand determine prices and output, and each competitor takes its own business decisions freely and independently.

Competition law reaches conduct beyond national borders. For example, inappropriate conduct with a competitor relating to Curium's business in Europe will infringe EU antitrust law, regardless of whether it takes place at a trade fair in Hong Kong or at Curium's premises in France.

D. Consequences of Antitrust Violations

For Curium:

- Significant monetary fines (e.g., the European Commission has the power to fine companies up to a maximum of 10% of their previous year's global turnover).
- Private damages: any customer that can prove it has been harmed by Curium's behavior may commence a lawsuit (including class actions, in some jurisdictions) seeking damages.
- Certain violations constitute criminal conduct and may be punished by criminal sanctions.
- Legal fees.
- Business disruption.
- Reputational damages.

For Curium employees:

- Job duty changes, loss of opportunity for promotion, or job loss.

- Jail time, monetary fines, disqualification of executives (e.g., Article L. 420-6 of the French Commercial Code provides for imprisonment and fines for individuals who fraudulently play a personal and significant role in designing, organizing or implementing anticompetitive practices).

E. Relations with Competitors

1. Contact with competitors must be kept to a minimum

Meeting and interacting with competitors is not unlawful in itself. However, even legitimate cooperation with competitors may pose antitrust risks. Great care must be taken with regard to the content of the exchanges that occur during (legitimate) interactions with competitors. If interaction with a competitor takes place, for example, because the competitor is also a customer or supplier, or because the competitor is participating in a trade show or a trade association meeting, restrict the scope of your exchanges with this competitor to what is strictly necessary and abide by the rules of conduct set out below. Even the appearance of collusion can be very costly to Curium.

Q&A
Q: Can Curium enter into a joint production agreement for generators with a competitor?
A: It depends on the facts. This arrangement would need to be closely reviewed by the Compliance Office.

2. Never discuss or agree on the following items with competitors

- Prices and discounts: these include prices, discounts and rebates, price lists, credit terms, etc.
- Costs of specific products.
- Sales volumes or market shares, sales or service territories, conditions of sale.
- Allocation or sharing of customers, territories or products.
- Unless approved in advance by the Compliance Office, information about production, notably production rates, the opening and closing of manufacturing sites or other premises, plant capacity, capacity utilization and delivery schedules.
- Unless approved in advance by the Compliance Office, market plans relative to entering or exiting markets or product categories.

3. Do not coordinate bids or Requests for Quotations ("RFQs") with competitors

- Bid rigging is always illegal. Companies must respond to customers' bids and RFQs independently. Under certain circumstances, competitors can form consortia or other forms of cooperation in order to submit a joint offer. Always consult with and obtain approval from the Compliance Office before entering into any cooperation with a competitor in connection with a customer's bid.
- If a competitor contacts you about how Curium intends to respond to a bid or RFQ, simply say that you do not intend to share Curium's information and immediately call the Compliance Office.
- If a customer provides you with the price offered by the competition, do not attempt to verify this price with competitors.

4. Never exchange confidential or competitively sensitive information

- Exchanging competitively sensitive information with competitors is prohibited, especially if the information concerns prices, inventory, profits, strategies, costs or terms of sale.
- If you receive unsolicited sensitive information from a competitor, make note of how and from whom you obtained it, do not communicate with that competitor regarding its content and call the Compliance Office.

- Information concerning competitors may only be obtained from public announcements or from sources other than your competitors themselves; you must document the source of any information concerning competitors, in order to be able to prove that it was legitimately obtained.
- If you receive competitively sensitive information from a competitor, or such information that you think was sent by a competitor, immediately call the Compliance Office.
- You must obtain approval from the Compliance Office before sharing any competitively sensitive information outside the Company.

Q&A
Q: Can Curium pick up the phone and check how a competitor plans to respond to a specific RFQ?
A: NO!

F. Relationships with Customers or Distributors

Because Curium operates in markets with particular characteristics and a limited number of competitors, you should be aware that the following practices may raise potential antitrust risks.

1. Prices and sales terms

- Excessive pricing: High prices that have "no reasonable relation to the economic value of the product" are a problem if a competitor is placed at a disadvantage (e.g., by having to pay more for input products).
- Predatory pricing: Pricing below cost may be illegal if the objective or effect is to force competitors to exit the market.
- Discriminatory pricing: Curium may not discriminate between its customers if this affects competition. Concerns may arise if a supplier gives non-competing customers a price advantage over competing customers. Price discrimination means applying different prices and price components to similarly situated customers. Customers are not similarly situated if they buy the products at significantly different points in time, buy significantly different quantities or grades, require additional resources to supply, or use the product for different ends.
  A possible justification for pricing decisions may be to show that the purpose of the act was actually something other than harming a competitor or affecting competition (e.g., cost savings, meeting competition, changed market conditions, etc.). Call the Compliance Office if you have doubts or questions in relation to a specific situation.

Q&A
Q: Can Curium apply a higher price for Mo-99 solely because the customer is also a competitor?
A: NO!

2. Discounts and rebates

It may be inappropriate for Curium to use discounts or rebates to lock in customers. Potentially problematic discount/rebate plans include: rebate schemes with long reference periods (e.g., more than 1 year); rebates based on Curium's share of a customer's total purchases; rebates based on all products purchased from Curium; rebates based on increasing purchase volumes; rebates based on what a customer would have purchased from other suppliers. However, volume-related savings, reduced packaging or shipping costs may justify certain decisions.

The laws in this area are complex and you should check with the Compliance Office in order to structure product offerings and incentives in compliance with applicable law.

Q&A
Q: Can Curium condition the offer of a discount scheme on the customer's commitment to purchase from Curium for at least three years?
A: It depends on the facts. Consult with the Compliance Office regarding any rebate structure.

3. Tying/bundling

- "Tying" refers to conditioning the sale of one product on the purchase of another.
- "Bundling" refers to selling two or more distinct products together (it includes situations where goods are sold together for less than the sum of their individual prices).

Tying is likely to create antitrust issues and bundling also may raise antitrust issues. These activities require a careful analysis of their compliance with law and must always be submitted to the Compliance Office before being proposed to a customer.

Q&A
Q: Can Curium agree to sell PET products only on condition that the same customer agrees to also buy SPECT products?
A: This is unlikely but it depends on the facts. Consult with the Compliance Office if you wish to engage in any tying/bundling practice.

4. Exclusivity provisions

Always contact the Compliance Office if you want to apply exclusivity provisions. Potential areas of danger:

- Requiring customers to buy all of their requirements of that product from Curium.
- Requiring distributors not to carry competitors' products.
- Requiring customers to allow Curium to match competing offers.
- Restrictions on passive sales (unsolicited sales outside an exclusive sales territory) are always prohibited.

5. Resale prices

In most countries, irrespective of market conditions, once Curium has sold a product to a distributor (or customer), it cannot control the price at which its distributor (or customer) re-sells the product.

- Setting a specific or minimum resale price is illegal in most jurisdictions. It can limit competition between distributors and facilitate collusion.
- Recommending resale prices (e.g., recommended price lists) is usually permissible as long as your resellers decide independently whether to observe specified resale prices.
- Using the implicit or express threat of sanctions to enforce compliance with recommended prices may turn the recommendation into a potentially unlawful resale price maintenance agreement.

Consult with the Compliance Office to explore the extent to which you may have the ability in the applicable market to influence the resale price of Curium products.

Q&A
Q: Can Curium apply higher prices because a distributor refuses to adhere to Curium's recommended price lists?
A: NO!

6. Termination/refusal to supply

Companies with strong market positions may not terminate or refuse to supply a customer (absent any creditworthiness concerns or breach matters) if to do so would cause harm to competition. Danger areas include:

- Refusing to supply an existing customer (refusal to supply a new customer must be reviewed on its facts with the Compliance Office).
- Where the customer competes (or may compete) with Curium.
- Where the customer wants to develop the product for a new market.

G. Relationships with Suppliers

When dealing with suppliers, Curium must respect their freedom to select their own customers. Bear in mind that:

- In most cases, Curium may not impose exclusive obligations on its suppliers.
- Curium's ability to extract excessively low prices might be considered abusive.

Q&A
Q: Can Curium refuse to source molybdenum from a supplier unless the latter agrees to stop selling the same to Curium's competitors?
A: NO!

H. Membership of Trade Associations

Trade association meetings can be perfectly legitimate and are not, in and of themselves, prohibited. However, trade association meetings present special risks, especially where competitors and/or distributors are present. The simple fact of participating in a meeting where inappropriate subjects are discussed can be dangerous.

ALWAYS
Get the agenda in advance of the meeting and consult with the Compliance Office if any agenda item appears to raise antitrust concerns.
Request a copy of the minutes of each meeting you attend. Review it carefully and send any amendments you deem appropriate. If you do not receive minutes, prepare your own.

NEVER
Attend meetings that do not have a clear and defined agenda.
Raise any matter or make any statement at the meeting that you think may involve competitively sensitive information without consulting with the Compliance Office in advance.
Prepare any report summarizing or benchmarking the information exchanged during the meeting without consulting with the Compliance Office in advance.
Attend a meeting at which prohibited topics are discussed. If such topics are raised outside the agenda, strongly request that the discussion stop immediately. If the discussion continues, leave the meeting, ask for your departure to be recorded in the minutes and immediately inform the Compliance Office.
Discuss prohibited topics with competitors during lunches, coffee breaks or other informal gatherings held before or after these meetings.

Q&A:
Q: Can Curium attend trade association meetings where competitors discuss future SPECT prices or other competitively sensitive topics?
A: NO! Even passive participation without clearly distancing yourself from what is being discussed can put Curium at risk of being found liable of an antitrust violation.

Chapter 4 – Trade Compliance Matters

A. General Provisions

As a global company, our business relies on moving people, products, technology and information all around the world every day. These activities are regulated by international trade laws that place different restrictions on our activities depending on factors such as the place of origin, content, destination, end use, alternative uses, and the parties involved. All Curium products and technology must be transferred in accordance with the import and export law requirements of the countries in which we operate. All employees are responsible for conducting their import and export activities in compliance with applicable laws and regulations and all parties involved in our transactions, including the end users of our products, must be screened to ensure that we can do business with them. In each case, employees involved in trade or export activities on behalf of Curium must ensure that all documentation for import, export and tax purposes is complete and accurate. Each supervisor and manager is also responsible for ensuring employee understanding and compliance with the trade compliance laws associated with the activities where the employee is engaged. Where there is any question about the legality of importing or exporting a product or component, or exchanging sensitive technology, consult with the Compliance Office.

Q&A

Q: A customer has asked me to prepare two invoices – a sales invoice with the actual price and a separate shipping invoice reflecting a lower price. Is this ok?

A: No. Documentation prepared for shipping purposes is used by government agencies in several ways, including determining tax and customs duties. These records, like all records for Curium, must be complete and accurate in all respects. Misrepresentation of the facts can result in substantial fines and sanctions.

Q: I am invited to a customer meeting in Iran as a Curium product specialist but have been informed that certain conditions need to be fulfilled for me to travel to Iran as a US citizen. That sounds complicated. I also hold a UK passport. Could I just travel to Iran using my UK passport?

A: No. Using your UK passport does not eliminate your obligations to comply with US export law as a US citizen.

B. Conformance to Laws and Regulations

We ensure compliance with laws and regulations and work closely with regulators. As a global company operating in one of the most highly regulated industries, we face an increasing variety of laws and regulations in every market where we operate. Our success depends not only on compliance with the laws and our own procedures but also on avoiding any suggestion of having violated such laws or procedures. Our products are developed, manufactured, marketed, sold and serviced in accordance with quality-controlled processes and procedures. As a Company employee, or if you act on behalf of Curium in any way, you must fully understand and comply with all quality and regulatory processes and procedures that are relevant for your work.

Q&A

Q: In many countries we rely on the distributor's view about the need for regulatory approvals. How do we ensure that these views are accurate?

A: Consult the Quality and Regulatory group to verify what is required in a specific country and/or region. If regulatory approvals are required, make sure the products have the necessary approvals. If the products do not have the necessary approvals, submit a request to initiate a regulatory submission.

Q: How do we know if a certain product has received a marketing authorization in a specific country or region? **A:** You must work with your local Quality and Regulatory team to verify that the product has a valid certificate for the intended country/region.

C. Export Controls Compliance

Most countries place restrictions on the export of goods or technology for national security and non-proliferation reasons, and items with potentially dangerous end-uses (e.g., biological weapons and chemical weapons precursors) may require government approval prior to export. Because of the nature of our products, however, many Curium products may be exported to any country in the world with no prior authorizations, with the exception of countries and certain customers (individuals or entities) subject to foreign-policy controls, embargoes, and sanctions.

Production equipment, computers, chemicals, and other non-production goods may be subject to restrictions, however, even if used to make pharmaceutical products. This is because of the "dual-use" nature of these types of items. For example, Curium may use laboratory equipment to develop new medicines, but someone else might use the same equipment to develop a biological weapon. Therefore, it is important to remember that the export of any articles, technology, or software, and, in the United States, the "release" of technology to a non-U.S. national, must be in compliance with applicable law and Company procedures.

In addition, Curium radiological products, and the transportation of such products, also may be subject to nuclear regulatory controls in the various jurisdictions in which the Company operates.

D. Economic Sanctions and Embargo Compliance

1. Company rules

Under Curium's rules, all Curium Stakeholders must comply with applicable laws and regulations regarding economic sanctions, embargoes, and other restrictions on transactions with certain countries, groups, and individuals. These rules and the sanctions on which they are based apply to trade in goods and services, investments, financing of trade transactions and the supply of technology associated with goods and services. No Curium legal entity, regardless of country in which it is located, and no Curium Stakeholder, regardless of citizenship or residency, will engage in transactions involving countries embargoed or subject to comprehensive sanctions by the EU or U.S., unless approved by the Compliance Office in advance. The Company has implemented safeguards to prevent and detect shipments to sanctioned and embargoed countries, including denied parties screening.

Any employee that wants to engage in activities involving countries embargoed or subject to comprehensive sanctions by the EU or U.S., whether or not within the scope of any other authorization or applicable regulation, must first consult with and obtain approval from the Compliance Office.

2. Summary of US Sanctions

US sanctions apply to US citizens, wherever they are located, permanent residents, entities organized under the laws of the US, and persons and entities located in the US. The sanctions also apply to trade in US goods, services, and technology by any person. Importantly, non-US made products that contain more than 10% controlled US content, by value, may be restricted for export to countries subject to US embargoes or sanctions, regardless of which Curium legal entity is selling such goods. The sanctions also apply asset freezes and other forms of financial sanctions on specified individuals and entities. US sanctions apply, for example, to the clearance of US dollar transactions through the jurisdiction of the US.

3. Summary of EU Sanctions

EU sanctions apply to EU nationals, corporate entities and persons or businesses in the EU. EU sanctions restrict the sale for export out of the EU of covered goods, services and technology. They also impose wide-ranging asset freezes and restrictions on the provision of credit or other economic resources to various named individuals or entities. EU sanctions include provisions prohibiting any involvement, directly or indirectly, in efforts to circumvent sanctions.

EU sanctions are agreed centrally but enforced by each EU Member State. Member States can impose additional sanctions measures beyond those of the EU, although examples of this practice are limited. Member States can also vary in their interpretation of the sanctions measures passed by the EU. In all, it is essential for Curium Stakeholders to consider not only the EU sanctions but their interpretation and, possibly, imposition of additional measures by Member State governments.

It is important to remember that non-EU European jurisdictions, including the UK, Switzerland and Norway, are outside the control of the EU institutions imposing sanctions and may have a different approach to the substance and the interpretation of the sanctions.

4. Denied Parties Screening Rules

The EU and US also impose targeted sanctions and export controls on individuals and entities that have been designated under sanctions targeting terrorists, narcotics traffickers, organized crime syndicates, and weapons proliferators, wherever they are located. In many cases, the sanctions prohibit EU and US persons from engaging in virtually all transactions with such designated individuals and entities. Under Curium's rules, in coordination with the Compliance Office, each business unit must consult our Denied Parties Screening software prior to engage with any customers and business partners.

5. Special Obligations of US Person Employees

No US person (which includes US citizens, US permanent residents, US corporate entities, or persons located in the United States), wherever located, will engage in any trade transaction, or otherwise "facilitate" or participate in any activity that violates US trade compliance laws or regulations, including any transactions or prohibited activities involving any countries embargoed by the United States. For US persons and US entities, this prohibition on facilitation includes performing any of the following activities, unless such US person activities are approved by licenses or other approvals issued by the US Department of Treasury's Office of Foreign Assets Control ("OFAC"): selling, shipping, brokering,

financing, approving, supporting (e.g., technical, warranty/claims, or legal support), processing, arranging, advising, referring an order or other business opportunity to any non-US entity, or restructuring transactions to permit or assist a non-US entity or person to perform such transaction.

Anti-Boycott Compliance

Anti-boycott regulations require any US company and its subsidiaries to refuse to participate in unsanctioned foreign boycotts of countries friendly to the United States. Importantly, the receipt of a boycott related request may require Curium to file reports with the US Department of Commerce, and the US Department of the Treasury even if the Company expressly rejects the request.

Any requests received by a Curium Stakeholder to support a trade boycott of any country must first be reported to the Compliance Office prior to acting on the request. The Compliance Office will provide you the necessary information to determine what actions, if any, may be lawfully taken with respect to the request. Examples of boycott related requests may be found at https://www.bis.doc.gov/index.php/enforcement/oac/7-enforcement/578-examples-of-boycott-requests.

E. Who to Contact

Any questions or concerns related to this Chapter or potential non-compliance events must be directed or reported to your direct supervisor or manager and the Compliance Office.

F. List of Countries/Territories Subject to Comprehensive Embargoes or Comprehensive Sanctions

- Crimea region of Ukraine
- Iran
- Sudan
- Cuba
- North Korea
- Syria

Note that under certain circumstances it may be possible to sell Curium products to a customer in one or more of the countries listed above (e.g., after obtaining a specific license, or after confirming that the specific contemplated activity is legal). Consult with the Compliance Office in advance to determine if the contemplated transaction may be undertaken in full compliance with applicable law.

Chapter 5 – Information Matters

A. Personal Information

1. Introduction

The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (The General Data Protection Regulation) aims to harmonize the data protection Law. As a regulation, the General Data Protection Regulation (hereinafter "GDPR") is directly applicable in all European Union member States. Under the GDPR, Curium is identified as a Controller, that is to say a legal person which determines the purposes and means of the processing of personal data.

Curium's compliance with the GDPR and other similar regulations through all employees' commitment is essential as these regulations severely sanction companies that do not comply.

Curium expects from any of its business partners, that its personal data are collected and processed in a lawful way.

Finally, we need to manage and protect our assets and information to safeguard our business and reputation. Curium's assets cover a range of property which includes information and computers, telephones, software, product plans, strategy documents and similar items, all of which are key to the success of our Company. Everyone entrusted with Curium property is responsible for its protection and correct use. Concerning electronical devices provided to you by Curium, please make sure you read Curium Group IT Policy (please refer to **Appendix 2**).

INTELLECTUAL PROPERTY – Curium's intellectual property is one of our most valuable assets and helps differentiate us from our competitors. You must be vigilant in safeguarding our patents, trademarks, copyrights, trade secrets, know-how and all other proprietary information. Any unauthorized use or disclosure of these could harm our business.

CONFIDENTIAL INFORMATION - Employees and other persons working for Curium must protect confidential information from improper use or disclosure, and communication of confidential information shall be limited to individuals who need it in order to carry out their work. Confidential information obtained from others must be treated in the same way as we expect them to treat information received from us and in accordance with the terms applicable to its disclosure. Any unsolicited third-party proprietary information should be refused. If you inadvertently receive such information, notify the Compliance Office immediately.

COMMUNICATION TOOLS AND SOCIAL MEDIA - Take special care to use the business communications tools primarily for business purposes and in line with applicable policies and guidelines. Do not use internal open social media channels to share confidential, personal or commercial information about Curium, its customers or third parties. When you speak about yourself in external social media, you must not spread any Curium information that is not intended for the public. Nor should social media be used in a way that could harm Curium's brand or reputation.

COMMUNICATING ON BEHALF OF CURIUM - Only authorized representatives may communicate externally on behalf of Curium, including via social media. Any request from third parties (analysts, banks, journalists, press agencies, etc.) must be answered by a "No Comment" and the request directed to the Compliance Office or the VP of Branding and Communications.

Q&A

Q: I have just joined Curium from a competitor and brought with me lots of information which I think could be useful to share. Is this OK?

A: No. You are not allowed to share information if it is of a confidential nature. Sharing this information would expose you and Curium to risk as well as cause harm to your former employer.

Q: One of our customers has heard rumours about our new product for which we consider a patent application. What can I tell the customer?

A: You should consult with the Compliance Office before discussing the new product with the customer as this may jeopardize Curium's right to obtain the patent.

2. Which personal data might be collected by Curium?

The GDPR refers to the protection of natural persons with regards to the processing of their personal data.

"Personal data" are any information relating to an identified or identifiable natural person such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The above definitions are very broad. Personal data information might vary depending of the field of industry of each company. Personal data likely to be processed by Curium mainly concern employee's information (names, phone contacts, addresses etc.) followed by personal data collected in the frame of day-to-day interactions with our business partners. It would not be expedient to exhaustively list all personal data susceptible to being processed. For this reason, please always refer to the terms defined above if questions arise concerning the application of these personal information rules.

3. Why is Curium collecting and processing personal data?

CURIUM is collecting and processing personal data to:

- Provide information and services to its employees;
- Provide information and services to its business partners;
- Contact and interact with its business partners;
- Operate its business and especially comply with applicable law, regulations and requirements of regulators, governments and authorities (e.g., pharmacovigilance obligations); and
- Perform its contractual obligations, as diverse as they might be.

Many legitimate business purposes can therefore justify the collection and processing by Curium of personal data. However, please take into consideration that the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is generally prohibited (exceptions to be presented below).

4. How does Curium collect and process personal data?

Curium is implementing appropriate technical and organizational measures to ensure a level of security appropriate to the risks identified by the IT department.

For example:

- The pseudonymization and encryption of personal data;

- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

In practice it means:

- The access to server rooms only with key and the securing of IT rooms with alarm;
- The mandatory use of individual credentials and passwords for confidentiality and tracking purposes (pharmaceutical audit trials);
- The restriction of users' access for specific tasks they are involved in;
- The challenge of personal data usage and potential substitutions of user-related data by random codes;
- The encryption of hard disk or cloud solution;
- The regular checking of backups for recovery;
- The regular evaluation of technical and organizational measures on effectiveness and plausibility;
- Monitoring of network activity, remote accesses, firewall usage and antimalware protecting tools, private secured network to transfer data, up-to-date supported systems and hardware to ensure latest protections; and
- Implementation and update of Company policies and processes to reflect changes in regulations and duties, especially related to data handling and protection.

5. For how long will Curium retain personal data?

Curium will keep personal data in accordance with what is demanded by the nuclear and pharmaceutical regulations, applicable laws and systems consistency and, otherwise, as short as necessary in relation to the purposes for which they are collected or processed, following on this GDPR requirement. The preservation time of personal data may be shortened if a data subject (whether external or internal to Curium, identified or identifiable natural person whose personal information is collected by Curium (hereafter a "Data Subject")) withdraws his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not comply with the GDPR requirements. Preservation time imposed by specific regulations will however prevail on that right of Data Subjects to shorten or withdraw the retention of personal data.

6. Does Curium share personal data?

Curium may disclose personal data in the following situations:

- between its subsidiaries and affiliates (companies controlling, controlled by, or under common control of a Curium company) for legitimate business purpose;
- with its third-party service providers such as processors, that is to say natural or legal persons, public authorities, agencies or other bodies which process personal data on behalf of the Controller;
- to conduct surveys, provide technical support, and transmit communications;
- to comply with its legal obligations, including in response to lawful requests (e.g., court orders, in connection with any legal or regulatory process, or to comply with relevant laws by public authorities, such as to meet national security or law enforcement requirements);
- to protect and defend Curium rights and property, to defend Curium against a legal claim; to investigate, prevent, or take action regarding possible illegal activities, suspected fraud, safety

of person or property, for audit purposes, or a violation of these rules (See also **Appendix 2**: Curium IT Policy); and

- with Data Subject's permission, to share information with specified third parties.

7. How does Curium protect personal data?

Curium, acting as the Controller, commits to respect GDPR's obligations on all personal data that Curium may have to collect, stock and process.

Curium therefore commits (and expects from all its employees) to:

- treat personal data of each concerned Data Subject in a lawful, loyal and transparent way;
- acknowledge all the personal data collected and processed;
- require and confirm that collected and processed personal data are indeed necessary in regard to the field of activity of Curium;
- ensure the respect of the rights of persons of whom personal data are involved (right to access, right to erasure, right to rectification, right to restriction of processing, right to data portability, right to object);
- ensure its ability to share personal data in respect of the GDPR;
- only call on processors with sufficient warranty regarding the implementation of technical and organizational measures, and which meet the requirements of the GDPR, including the security of processing and all other rules applicable to processors;
- respect and command respect of the GDPR if personal data are transferred outside the European Union.

Trust, including responsibility for the privacy of individuals, is at the heart of our business and a long-standing Curium value. Curium is committed to protecting the privacy and confidentiality of any personal information to which we gain access in the course of our business. Any collection or processing of personal information must be for specific and legitimate business purposes with due consideration to principles of proportionality and transparency. We value personal information entrusted to us and we work hard to protect it. Personal information of employees, customers or patient information is confidential and must be kept accordingly. When you are involved in accessing or processing personal information, you must familiarize yourself and comply with relevant legal and contractual requirements. Consult the Compliance Office if you need guidance.

Q&A

Q: What is "personal data protection" and why do we need to be concerned about it?

A: While the exact definition varies from country to country, generally personal data is any information relating to an individual – a name, a photo or an email address for instance. In the online environment, where vast amounts of data are instantly transferred around the world, it is increasingly difficult for individuals to maintain control over their personal information. Almost everything we do online allows for the collection of data. In many countries, including in the EU, data protection is a fundamental right that trumps other interests. Additionally, there are very restrictive regulations for protected health information, such as the United States Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations for protected health information. Employees accessing a US customer's (or its patient's) protected health information (whether from within or from outside of the United States) are bound to comply with HIPAA regulations, which include having documented evidence of HIPAA training. Fortunately, except in specific pharmacovigilance actions, Curium has no need to receive

protected health information in connection with marketing and sale of Curium products. When in doubt, consult the Compliance Office for guidance.

Q: What if there is a business need to share personal information with third parties?
A: Provided there is a legitimate business need for doing this, you must ensure that the third party can protect the personal information properly and will use it only to provide services to us. Make sure there is an appropriate contract in place that addresses protection of personal information and ensures compliance with local regulations, which may include mandatory notification to authorities regarding personal data sharing.

Q: I have been diagnosed with an ongoing medical condition. How do I ensure this information is kept confidential and only given to people who really need it?
A: There is a balance between the employer's need for information and the employee's right to respect for their private life. You may ask your HR Manager to provide assurance that the health information is being kept in a specially protected manner and that access to this information is limited to managers or HR Personnel that genuinely need it to carry out their job.

8. Exceptions

As already mentioned, in order to operate its business and comply with applicable law, regulations and requirements of regulators, government and authorities such as pharmacovigilance obligations, Curium might collect and process personal data without the detailed consent of the Data Subject (See also **Appendix 2**: Curium IT Policy).

9. Data protection responsible person

The data protection responsible persons are the representatives of the Compliance Office and any delegated person delegated by the Compliance Office, all of them reachable at the following email addresses: Compliance.Office@curiumpharma.com and Privacy.Office@curiumpharma.com (hereafter referred to as the "Responsible Person").

It is important to ensure that the data protection Responsible Person is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

Data Subjects may contact the data protection Responsible Person regarding all issues related to the process of their personal data and to the exercise of their rights under the GDPR. The data protection Responsible Person is bound by secrecy or confidentiality concerning the performance of his tasks.

10. What is expected from Curium Personnel?

Curium expects its Personnel to:

- Contact the data protection Responsible Person if you have any query regarding the collection and processing of personal data by Curium.
- Immediately inform the data protection Responsible Person if there is any query of a Data Subject regarding her/his personal data.
- Handle over to the data protection Responsible Person all demands regarding personal data in a clear and understandable way, and in a reasonable time. Queries from Data Subjects must always

be managed by the data protection Responsible Person and not directly by other employees unless formally delegated.

- Define essential personal data you need in respect to your specific context. It is indeed important for Curium to rely on processes and measures enabling, from the start, an optimal protection of personal data and therefore a minimization of the information to be collected. It might be the opportunity for you to update your personal data requests (for example, to review forms you might send to your customers or other business partner which, as of today, request personal data that are not reasonably necessary).
- If the Data Subject has not been requested to give consent to the collection and processing of his/her personal data (through a form, specific article of a contract or any other medium), you shall save written statements, emails, forms which can evidence that Data Subject agreed to the collection and processing of her/his personal data for specific purposes. Do not hesitate to make screenshots and collect in a unique folder all evidence of such agreement, or which may be useful to share with the data protection Responsible Person.
- Strictly follow the Social Media and Password policies discussed below.

B. Social Media

Social media are now part of the business and its performance. Curium recognizes the importance and usefulness of social media while remaining aware of the risks they can involve. Curium's Personnel must acknowledge that due to Curium's activity in the field of healthcare, they are all responsible to protect and ensure the professional reputation of the Group. You must therefore be aware of the importance of social media (such as Facebook, LinkedIn, Twitter, YouTube, Instagram, personal blogs and other websites) and follow the below guidelines whenever you are using social media:

- As a representative of Curium, you are expected to share the values of the Group, even in the private sphere. Therefore, your use of social medial should never denigrate Curium and always be in the spirit of our corporate values;
- Except as requested in connection with authorized Company campaigns, do not mention Curium in your interactions on social media (except to mention your current or former position within Curium);
- Be aware that your action, as a representative of Curium, can have impact on the Group image and might remain public for a long time;
- Use your best judgment when interacting on social media in order to always act with decency and never be inappropriate or harmful to Curium, its employees or its business partners, nor create a hostile work environment;
- Never interact on behalf of Curium on social media if you have not been authorized (in writing) to do so by a person entitled to provide you with such authorization. If duly authorized, all communication through Curium social media should be correct, clear and approved by the sales and marketing department and the VP of Branding and Communications (who may also require approval by others, e.g., the Compliance Office);
- Get appropriate permission and authorization before referring to or posting images of Curium employees or business partners (current or former ones);
- Identify yourself as a Curium representative (when speaking on behalf of Curium and if authorized to so);
- Only share publicly available information. Exclude information considered confidential or with a confidential nature. Should you have any question about the confidentiality of information, please check with your supervisor or the Compliance Office;

- Always remember that social media may generate press and media attention as well as legal questions;
- Make sure to inform the marketing department and the Compliance Office about any positive or negative remarks about Curium's products you might come across (and keep a record of it). Never interact directly when such situation occurs.
- Social media should not interfere with your responsibilities at Curium and, except for very limited personal use that will not interfere with Curium's business, Curium's computer systems are to be used for business purposes only.

C. Password Rules

Usernames and passwords are the primary mechanisms that protect Curium information technology systems and other resources from unauthorized use. These rules apply to all computing resources administered by Curium.

1. Principles

It is important for you, as an account holder and/or system administrator, to construct secure passwords and to ensure the safe management of your passwords in order to reduce the risk of dissemination of information to undesirable or unauthorized parties.

Computing accounts must be protected by strong passwords.

- Never write down your username and password (including under electronic form) unless following IT's recommendation regarding a specific vault system;
- Never share a password with anyone, including your colleagues (even in the IT department) and/or other Curium Stakeholders, and never include them through email;
- Never include a password in a non-encrypted stored document;
- Never hint at the format of your password;
- Never use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other Curium computing resources on non-Curium equipment, and avoid doing so on Curium's equipment;
- Never use your corporate or network password on an account over the internet which does not have a secure login;
- Report any suspicion of your password being broken or detected to the IT department;
- If you have the possibility to modify your password, don't use common acronyms, common words, names of people, or parts of numbers easily remembered; and
- Specific Curium applications might recommend passwords rules. If applicable, make sure to follow these rules.

2. Roles and responsibilities

Each department is responsible for implementing, reviewing and monitoring internal practices to ensure compliance with these rules. The Chief Information Officer is responsible for enforcing these IT rules and is authorized, through the IT department, to set and maintain specific password creation and management standards for Curium systems and accounts.

3. Consequences and sanctions

Violations of these rules may lead to disciplinary measures up to and including termination of employment, according to applicable local law.

APPENDIX 1- ESCALATION POLICY

PURPOSE

Escalation Policy identifies those events which are required to be promptly notified to Curium's CEO, to the Compliance Office (compliance.office@curiumpharma.com) and, where applicable, to the Business Line CEO or to the VP Head of Quality. These are events that are likely to have a material impact on Curium, whether financially, operationally or reputationally ("**Material Events**"). We expect the Executive Management of the respective business units to use their discretion in deciding what constitutes a Material Event that needs to be escalated. While we include examples of these types of the events in this policy to provide guidance, please note that we do not consider this an exhaustive list.

The principal areas covered by this Escalation Policy include, but is not limited to:

- Health and safety of our workforce, including critical radiation safety incidents, other accidents and injuries, environmental incidents (e.g. leaking radio-active water) and other major events including causes of abnormal levels of absenteeism *(Appendix 1);*
- Critical product quality incidents in GMP and nuclear production activities, including inspections by regulators *(Appendix 2);*
- Major operational incidents affecting Curium's ability to deliver to customers, including major outages at key suppliers *(Appendix 3);*
- Critical actions in contravention of our Code of Conduct, especially regarding anti-bribery, corruption and anti-competitive behaviour;
- Major customer (>5% sales), supplier (>5% cogs) or key employee (Salary >EUR150k) losses or;
- Problems with key investment projects.

This Escalation Policy also applies to information received from Curium CMOs, CROs, CLOs sites, and other suppliers of GMP and nuclear goods and services (taken together "Third Party Sites").

SCOPE

This Escalation Policy applies to all departments and Personnel that are operating within nuclear production facilities, the GMP requirements and supporting services/activities, whether under the Curium Quality System, or not. This includes Curium'S Molybdenum Production Facility (MPF), all SPECT manufacturing sites (hot and cold products), our radio-pharmacies and our PET cyclotrons and laboratory units, and local, regional and central administration offices across the world (taken together "Curium Sites").

1. DEFINITIONS

1.1. **Business Line CEO**: The Chief Executive Officer of each Curium Business Unit where the Material Event occurs

1.2. **CEO:** The Chief Executive Officer of Curium

1.3. **Chairman:** The Chairman of the Board of Curium

1.4. **Compliance Office**: means the office of compliance composed of the Group Chief Legal Officer, the SPECT US General Counsel and the SPECT International General Counsel.

1.5. **Executive Management:** Senior employees of Curium who have delegated executive responsibility for their respective operating unit and the authority to establish, implement and monitor the integrity and efficacy of appropriate policies and procedures to ensure adequate levels of health and safety, product quality and adherence to the local regulations and the Curium Code of Conduct.

1.6. **CLO:** Contract Laboratory Operations

1.7. **CMO:** Contract Manufacturing Operation

1.8. **CRO:** Contract Research Operation

1.9. **OPCO:** The Operating Committee, with delegated authority from the Board of Directors of Curium (through Curium BidCo)

1.10. **VP Head of Quality:** means, within each Business Unit, the person in charge of supervision and oversight of the Quality, Assurance and Regulatory compliance.

2. REQUIREMENTS

2.1. The CEO, the Business Line CEO, the VP Head of Quality and the Compliance Office expect to be promptly notified or made aware of a potential or confirmed Material Event at Curium Sites and Third-Party Sites.

2.2. This Escalation Policy will be issued and implemented at all Curium sites. Each site will include a specific notification process relevant to that site. All employees should defer to their respective Executive Manager for guidance on the policy. Notification must go directly to the CEO and the Compliance Office if Executive Management is not adhering to the Escalation Policy.

The procedure will be clear on the relevant chain of command for notification for that Site including relevant contact details, which must be updated periodically.

Communication should be:

- For items listed in Appendix 1 and Appendix 3: to the Business Line CEO by phone (or voice mail in the absence of answer) in the first instance, followed by a written report;
- For items listed in Appendix 2: to the VP Head of Quality by phone (or voice mail in the absence of answer) in the first instance, followed by a written report;
- For contraventions to the Curium Code of Business Conduct: to the Compliance Office by phone (or voice mail in the absence of answer) in the first instance, followed by a written report;
- For commercial or project related items: to the CEO by phone (or voice mail in the absence of answer) in the first instance, followed by a written report.

All notifications to the above recipients (the "Recipients") must be copied to the Compliance Office for centralization purposes.

Where required, the Recipients will be in charge of reporting to the OPCO all notices of Material Events received since the previous OPCO and to summarize the progress report of all reported Material Events that have not been solved within the 30 days after their notification. All (progress) reports will be sent to the Compliance Office for centralization purposes.

This Escalation Policy must be communicated to all Curium Site employees.

2.3. Executive management are not only expected to notify. They have primary responsibility for and are expected to take appropriate actions as necessary to mitigate against, avoid or react to Material Events to mitigate risks and loss. This may also include executing on the disaster recovery plans or events in particular for those which may result in a product shortage in the market.

2.4. Standard operating procedure (SOP) is to be defined (See Section 4), communicated and followed in respect of all escalations.

3. THE SOP(S) GOVERNING THE NOTIFICATION PROCESS MUST INCLUDE THE FOLLOWING:

3.1. Examples of the types of incidents requiring notification, including but not limited to those noted in Appendix 2.

3.2. All notification must be made not later than 24 hours after occurrence or detection/knowledge of the Material Event.

3.3. A distribution list shall be maintained per Site and updated as needed, to assure that the CEO, the Compliance Office and, where applicable, the Business Line CEO or the VP Head of Quality are informed.

4. THE FOLLOWING POINTS ONLY APPLY TO MATERIAL EVENTS LISTED IN POINTS 1.2.2 AND APPENDIX 2

4.1. The standard form for the consistent reporting of the information related to the events listed in points 1.2.2 and Appendix 2:

4.1.1. Site (if multiple sites)

4.1.2. Name, strength, dosage form of product

4.1.3. Affected batch(es) with lot number and expiry date

4.1.4. Protocol Number, Clinical Study Number

4.1.5. Date of discovery of incident

4.1.6. Date of initiation of notification

4.1.7. Origin of the incident (e.g., stability testing, investigation, product complaint trend, AE, CAPA, report from regulatory agency)

4.1.8. Clear and concise description of the event (including the actual result and the specification, as appropriate)

4.1.9. Initial impact evaluation (e.g., safety, compliance, drug shortage)

4.1.10. Activities completed and planned related to the incident

4.1.11. Is this event limited to one site or does it have the potential to be global? (i.e., global impact because raw material, equipment, supplier used by multiple sites)

4.1.12. Approval by quality head or designee

4.1.13. Corrective action, lessons learned, training programs updated and updates to policies and procedures, if any

4.2. For the Material Events listed in Appendix 2, the Escalation Policy includes the requirement for documented acknowledgement of receipt (through confirmatory email) by the VP Head of Quality who on a case by case basis will define the criteria for closing the incident reported (e.g., activities planned have been completed, sites impacted by a global event have initiated appropriate actions, acknowledgement of receipt by head of quality). The VP Head of Quality will track incidents to closure.

4.3. The VP Head of Quality will maintain the documented record of confirmation of receipt of the notifications received from each recipient.

4.4. Notifications, which become confirmed events will be discussed at management reviews (e.g., Quality Council) to provide an update on the status of the situation and will be reviewed during audits to assure that the appropriate notifications and actions have taken place.

4.5. Each Site shall ensure that all Notification forms (as the case may be through an electronic system) have the appropriate fields and are consistent with drug and medical device regulatory requirements.

4.6. References :

- 21 CFR Part 211
- 21 CFR Part 820
- Guidance for Industry – ICH Q10 Pharmaceutical Quality System
- Directive 2001/83/EC for Medicinal Products for Human Use

Appendix 1: HEALTH AND SAFETY

1. Critical radiation safety incidents when external notifications are required

2. Critical accidents and injuries that result in or are probable to result in reportable lost time injury

3. Elevated absenteeism greater than 15% over the prior 3 months period

4. Environmental incidents (e.g. leaking radioactive water, improper treatment of radioactive waste, transport incident) when external notifications are required.

APPENDIX 2: CRITICAL PRODUCT QUALITY INCIDENTS IN GMP AND NUCLEAR FACILITIES

including but not limited to:

1. Stability result out of specification (OOS) or out-of-trend (OOT) within or at expiry date, or a stability OOS or OOT result
2. Investigations (OOS) and/or lab investigations (OOS/OOT) potentially impacting distributed product which is probable to result in customer impact > 50K in lost revenue
3. >1 rejection of batches of the same product within 30 days
4. ANY sterility test failures/media-fill failures
5. An unusual, unanticipated or higher than expected frequency of Adverse Events (AEs) > 15% over last 3 months period
6. A product quality complaint that may indicate a significant quality issue
7. A significant upward trend of product quality complaints
8. A significant upward trend of adverse events which may be related to product quality
9. Any issue that would require filing a Field Alert Report or other regulatory communication Issues potentially requiring a recall
10. Initiation of correction or removal of a product from commercial distribution which is probable to result in customer impact > 50K in lost revenue
11. Recall or device deposition of an investigational device when external notification is required
12. Initiation of a GMP inspection by a Regulatory agency
13. Critical internal or external audit or regulatory inspection observation that is reasonably expected to result in oral or written citation of a regulator
14. Overdue commitments made to regulatory authority 3 days before the due date of the commitment
15. A trend of late APRs > 15% over last 3-month period
16. Receipt of FDA 483, Warning Letter, or similar regulatory communication
17. Critical failure of a validation or revalidation study
18. Labeling errors affecting distributed finished product when external notification is required
19. Quality issue with potential for a drug shortage or long-term impact to product supply when external notification is required
20. Counterfeit or tampering report when external notification is required
21. Quality issue potentially delaying product transfer or launch
22. Information from Suppliers which may impact distributed product which is probable to result in customer impact > 50K in lost revenue
23. GMP computer system validation issue potentially impacting distributed product
24. Disqualification of any non-compliant GMP contractor organization

N.B.: References to 50K are either in EUR or in USD.

APPENDIX 3: MAJOR OPERATIONAL INCIDENTS AFFECTING CURIUM'S ABILITY TO DELIVER TO CUSTOMERS

2.1. Manufacturing line down which results in customer impact > 50K in lost revenue

2.2. Fire or flood when external notifications are required

2.3. Explosion when external notifications are required

2.4. Power outage which results in customer impact > 50K in lost revenue

2.5. Major outages at key suppliers – irradiation, targets which is probable to result in customer impact greater than 50K in lost revenue

2.6. Workers strike, go-slow, walk out lasting more than 2 hours

2.7. Events of force majeure which results in customer impact > 50K in lost revenue

N.B.: REFERENCES TO 50K ARE EITHER IN EUR OR IN USD.

APPENDIX 2 – IT POLICY

CURIUM'S INFORMATION TECHNOLOGY POLICY

1- Presentation of the Policy/Policy statement

a. Purpose: The purpose of this Information Technology Policy (the "IT Policy") is to give instructions and set up rules about the use of Curium Devices and associated IT infrastructure (including but not limited to the Emails exchanged through this IT infrastructure) to the Users and to establish guidelines and procedures for a safe, appropriate and correct use of the Devices and Emails. This policy prohibits inappropriate or unauthorized uses of Curium Devices or Emails, aiming to minimize disruptions to services and activities and comply with applicable policies and laws. Moreover, this Policy is aimed at informing Users that the Devices and the Emails as well as the use by Users of such Devices and Emails may be monitored by the Company through those modalities specified herein below.

b. Objectives: The objectives of the IT Policy are to ensure that the Company Devices are used correctly by Users and to maintain the confidentiality and ensure compliance with laws of our data and to maintain the integrity, cyber security and viability of our IT systems. It also aims at minimizing potential business risk from inappropriate uses such as breaches in confidentiality, improper disclosure of commercially sensitive data, breaches of customer confidentiality, conflict of interests, unauthorized business activities or the protection of personal data and copyright. Moreover, this Policy aims at allowing Curium to protect and defend its rights and property, to defend itself against a legal claim, to investigate, prevent or take action regarding possible illegal activities or suspected frauds, to protect the safety of person or property, to prevent misconducts taking place or detect those which have taken place, to allow audits correctly being carried out or detect suspected violations of laws, regulations or internal policies. It finally aims at setting the rules allowing the Company to access the Devices and Emails of a User if and when required and in a manner compliant with applicable laws.

c. Scope: This IT Policy applies to all Users, all employees, executives, (sub-) contractors and consultants, and generally any individual who use Devices in every country.

d. Definitions and abbreviations :

Word	Definition
Company	Refers to all Curium Group entities.
Devices	Includes the Company owned mobile phones and end users computers (incl. desktops, laptops or tablets).
Emails	Emails which are on the professional mailbox of Users.
Information Technology (IT)	Is the use of any computers, storage, networking

	and other physical devices, infrastructure and processes to create, process, store, secure and exchange all forms of electronic data.
Intranet	Is a private extension of the internet that is confined to an organization.
IT Department	Is IT function within Curium.
User	Is a person who is working for Curium as an employee, executive, (sub-)contractor or consultant or any other individual and who has been provided with a Company Device for a professional purpose.

2- Guidelines and procedures

a. Quick/Brief reminder: General do's and don'ts:

DO'S	DON'TS
For every Device Users have been provided with, keep their passwords safe.	Leave their equipment or computer session unlocked or unsecured.
Consider password-protecting sensitive documents.	Let their work be seen or heard by unauthorized persons.
Use a secure internet connection	Use a potentially dangerous public connection.
Use a VPN if accessing Curium systems from outside our network.	Use direct portable drive (memory sticks) sharing with read/write access on Curium devices unless from known or trusted sources.
Check when necessary that the site Users are accessing is secure – they shall look for the padlock icon or "https" in the URL address.	Visit websites that could be harmful to Curium network or that are linked to illegal activities.

b. Correct uses of the Devices:

- The Devices shall be used for a professional purpose;
- Personal uses shall be limited and shall not have a negative impact on Curium;
- Internet browsers shall be primarily used for professional purposes, personal uses are allowed but they shall be limited, and sites visited shall not be illicit or harmful to Curium;
- The uses of the Devices shall comply with the applicable local law;
- Users of the Devices shall notify their IT Service Desk immediately if their Device is unaccounted for, lost, or stolen, to minimize Curium's exposure;

- When receiving an Email on their professional mailbox, Users shall exercise care when opening attachments or links such as URL, .exe or .zip files and they shall not open files from unknown sources;
- Users shall use the internet function on their Devices in an appropriate manner and in order to further their professional goals and objectives;
- Users who discover any obvious or malicious defacement of Curium websites or stakeholders' websites shall immediately report this to the IT Department;
- Users who have reasons to believe that their voicemail, Emails, internet or any other account or Devices they have been provided with, have been accessed without their permission or if their password is known to someone else, must immediately change their passwords and report the incident to the IT Help Desk;
- Curium takes all reasonable practical actions to block inappropriate internet sites. However, it is recognized that due to ever evolving technology and new material it is not possible to guarantee that all inappropriate sites will be blocked. Therefore, Users must take personal responsibility for the sites they access;
- To effectively manage Curium services and reduce risk, Users must use corporate accounts for conducting Curium's business.

c. Forbidden uses of the Devices and Emails:

- The Devices shall not be used by people other than the person it was granted to;
- The Devices shall not be used to access, download or store inappropriate or illicit content (such as recreative films, games, pornographic, illegal or discriminatory content for instance) or any content that could be harmful to Curium;
- The Devices shall not be left unattended in a public space due to safety and confidentiality matters;
- The configuration of the Devices shall not be altered;
- Audio or video files shall not be stored on the Devices unless the content is relevant to professional matters;
- Unless managed by the IT Department, users shall not install applications from the internet on the provided devices;
- Users shall not share their passwords with anyone and shall not try to obtain other individuals' passwords;
- Users shall not use the Company Devices in ways that violate local policies, rules or administrative orders.
- Users shall not use their professional Email account to circulate chain letters or spams or to disclose any sensitive, personal or confidential information (unless with the proper contractual protections in place);
- Users shall not use their Emails for activities that could directly or indirectly be harmful to the interests of Curium, present a conflict of interest or constitute violations of Curium's Code of Business Conduct or other Curium policies.

d. General etiquette: When traveling or in public spaces, Users are invited to use their Devices in silent mode. In the workplace, Users can use the Devices with the

sound on, but they have to minimize the noise disturbance for the other persons working. When attending meetings, the Devices shall not be used in a way that they would constitute disruptive elements.

e. Protection of the Devices: Devices are provided to Users with protective cases. Users shall keep that physical protection and ask for a new one if the provided one appears damaged and cannot protect the Device correctly. Users shall always use a password on Company Devices to protect from inappropriate use and it shall never be disabled.

f. Monitoring of use: The IT Department or those service providers which may be identified by Curium are authorized to check if Users comply with this IT Policy and will monitor and conduct verifications for this purpose. Also, for business reasons and in order to carry out legal obligations in its role as an employer, use of all Curium's communication systems, including personal use, could be monitored to the extent permitted or required by law and as necessary and justifiable for business purposes.

In particular, Curium, for the purposes of managing and providing for maintenance of its IT infrastructure as well as verifying its functionality, confidentiality and security, is required and bound to periodically perform checks on the functioning of the Devices and if required conduct inspections.

For monitoring and verification purposes, the IT Department or those service providers which may be identified by Curium have the right to access the content of the Devices, including Emails. The logs and contents of the Devices and Emails may be accessed under the following circumstances:

- Request of judicial or regulatory authority;
- Public security request;
- Preventive and/or defensive inspection activities (Corporate bodies, Supervisory bodies) requiring a data collection approach in order to limit the associated risks, anomalies and/or discrepancies observed ;
- Business continuity requirements (data recovery in the prolonged absence of the person concerned);
- Request from the Curium Compliance Office;
- Licenses controls and supplier's audits;
- Need to defend the Company's rights and property;
- Need to defend Curium against a legal claim;
- Need to investigate, prevent or take action regarding possible illegal activities or suspected fraud;
- Need to protect the safety of person or property;
- Audit purposes;
- Need to detect suspected violations of laws, regulations or internal policies;
- Need to prevent misconducts taking place or detect those which have taken place.

Any access must be authorized by a responsible person from the Curium Compliance Office. Where available, accesses must be monitored through the activity log-in. If required under the circumstances, accesses can be initiated remotely and out of the User's knowledge.

The IT Department members or those service providers which may be identified by Curium may have to access in the course of their duties. The IT Department or those service providers which may be identified by Curium may reserve the right to restrict or block internet and mailbox access under given circumstances.

Curium may disclose any type of content acquired to the monitoring according to terms and conditions under this Policy to comply with its legal obligations, including in response to lawful requests (e.g. court orders, in connection with any legal or regulatory process, or to comply with relevant laws by public authorities, such as to meet national security or law enforcement requirements) and/or to protect and defend its rights and property, to defend itself against a legal claim, to investigate, prevent, or take action regarding possible illegal activities, suspected fraud, safety of person or property, for audit purposes, or a violation of its policies.

The temporary storage of data relating to the use of electronic devices is justified by the purposes of managing and providing for maintenance of its IT structures as well as verifying the functionality and security on the system. Temporary storage will be limited to the time necessary to achieve it an in any case not more than 6 months. Any possible extension of the retention period shall be considered as exceptional and may take place solely in relation to:

- very particular technical or safety requirements;
- the indispensable nature of the datum when exercising or defending a right in judicial proceedings;
- the obligation to keep or deliver data in order to comply with a specific request by a judicial authority or judicial police.

Any IT Department activity aimed at automatically and continuously monitoring the User's activities is in any case forbidden. Web surfing activities by the Users are not monitored in order to control remotely the work activities.

In case of preventive checks (checks to verify compliance with internal rules) and checks providing for access required by continuity needs, Users concerned must be informed in advance (also via electronic device or by telephone) for the purpose of guaranteeing correctness and transparency.

With reference to defensive checks (*i.e.*, monitoring carried out in the presence of the Company's need to defend its rights and proper, to defend itself against a legal claim, to investigate, prevent or take action regarding possible illegal activities or suspected fraud, to protect the safety of person or property, to

prevent misconducts taking place or detected those which have taken place, for audit purposes or in case of suspected violation of laws, regulations or internal policies) or those requested by Public Authorities (State Police, etc.) or in case of incidents which call for immediate and urgent intervention, a prior notice is not required, since it can prejudice the defence or the ascertainment of rights or responsibilities in the proceedings or the activity of Curium. In case of this type of incidents, the information shall be given subsequently. When carrying out checks and verifications, the persons in charge, including those service providers which may be identified by Curium, must guarantee the maximum confidentiality of the data acquired, also incidentally, during the verification, under penalty of disciplinary sanctions depending on the seriousness of the event. Data may thus be notified solely and exclusively to individuals internal and external to Curium to whom disclosure is required for the purposes pursued with the access (by way of example, in the cases mentioned, to Law Enforcement, to persons in charge of corporate functions responsible for legal actions or for solving technical problems).

g. Privacy matters: During the monitoring and verifications carried out by the IT Department, some personal data may be processed by the Company. This personal data will be handled with care and in compliance with applicable local laws and regulations, such as GDPR and other specific local regulations issued by national data protection authority governing the use of e-mail and the internet in the workplace.

h. Data acquired through the monitoring: any data which may be acquired by Curium through the monitoring of Devices, including Emails, according to this Policy may be used for any purposes in connection with the employment relationships of its personnel, including - but not limited to - disciplinary purposes.

3- Responsibilities/Policy owner

The policy owner is the Corporate Compliance and Control unit of the Legal Department who is responsible for drafting and reviewing this IT Policy as well as answering questions. This IT Policy is available on Curium intranet. The Chief Information Officer/the IT Department is responsible for ensuring adherence by Users to this IT Policy. When Users receive a Device, the HR Department shall send them a copy of the IT policy and an acknowledgement of adherence shall be requested.

Any technical question regarding this IT Policy must be directed to the IT Department. Any question or communication as regards the content of this IT Policy must be addressed to the Compliance Office per email at the following address: compliance.office@curiumpharma.com.

4- Enforcement and compliance checking

a. Enforcement: Users are responsible for complying with this IT Policy. The IT Department will check compliance through monitoring and verification. Should the IT Department find, during its verifications, content on a device which is deemed to be inappropriate, illegal, unauthorized or harmful to Curium's interests, or which constitutes a potential threat for Curium, it has the right to delete such content with a three (3) business days prior notice or has the right to copy and store such content for further use under any legal action; provided that if the IT Department deems the content to present an imminent harm to Curium, it may take action more quickly and without advance notice.

b. Sanctions: Users must comply with this IT Policy. All failures to comply will be investigated and appropriate action will be taken. For Users who are employees, the violation of the IT Policy may result in disciplinary sanctions and/or even termination, subject to the application of and as permitted by local laws. For Users who are not employees, all failures to comply will be dealt with in accordance with the terms of their engagement and/or contract.

   Users may be also required to remove any content which is deemed to constitute a breach of the IT Policy and a failure to do so may in itself result in appropriate disciplinary/other suitable action being taken.