GLOBAL BUSINESS INFORMATION PROTECTION POLICY

Executive Summary

Private business information is among the most valuable of UPL's assets. It can give us an edge over our competitors in the market. Like any other asset, though, it must be carefully protected. If we fail to preserve the confidentiality of our private business information, the reputation and competitiveness of our Company could be damaged.

This policy has been adopted to explain the rules by which UPL manages and protects its private business information, and with which all UPL employees must comply.

This policy augments, and is in addition to, UPL's Global Intellectual Property Policy, Information Security Policy (ISP) and the Information Security Management System developed in accordance with the ISP.

The term "UPL" or "Company" referred to in this policy refers to UPL Limited and all its subsidiaries and this policy applies to all UPL employees worldwide

1. Scope of the Policy

This policy sets forth rules designed to protect the confidentiality of UPL's private business information, as well as confidential information disclosed to UPL by business partners and other third parties. UPL conducts business in many jurisdictions and has always protected--and intends to continue to protect--all UPL confidential information to the full extent permitted by law (e.g., trade secret law) in all relevant jurisdictions. While this policy may not be necessary to achieve legal protection for UPL information, the implementation of this policy may nonetheless serve as a useful management tool to memorialize and structure UPL's ongoing approach to respecting confidential information.

Along with protecting confidentiality of UPL's private business information, the policy ensures that access to such information by authorized UPL personnel with a need-to-know is not unduly limited. To meet this purpose, the policy provides guidelines which can be adopted by relevant functions/departments at UPL when classifying their information or data into four basic categories – Highly-Confidential, Confidential, Restricted and Public.

As used in this policy, Highly Confidential means any information which is not publicly available, and the improper disclosure of which could damage UPL's business. Highly Confidential information includes, without limitation, the following:

- Sales, Marketing, and Supply Chain Information
    - Plans
    - Forecasts
    - Sales call reports
    - Customer lists
    - Customer data

    - Pricing
    - Production volume
    - Supply chains and vendor information
    - Distribution channels and distributor data
- Non-public Financial Information
    - Internal financial statements (for example, financial statements prepared at a regional level, or at a product level)
    - Budgets and forecasts
    - Margins
    - Cost information
- Administrative Information
    - Corporate organization
    - Salary and other compensation information
- Technical Information
    - Manufacturing and formulation processes, capacity, assets, and plans
    - Know-how
    - Active ingredient specifications
    - Formulation compositions
    - Research and Development plans and prospects
    - Pipeline plans and prospects
    - Source code
    - Design specifications
    - Non-public patent applications (for example, provisional patent applications, or unfiled draft patent applications)
    - IDFs (Invention Disclosure Forms)
    - FTO Analysis Report
    - Laboratory notebooks
    - Results of evaluation, experiment, and field trial
    - Inbred lines, parental germplasms, experimental lines
    - Microbial strains and populations
    - Circuit designs
    - Program algorithms
    - Any experiment protocols or experiment designs

2. Employee Obligations

a. Confidentiality and Use Agreements: All UPL employees must preserve the confidentiality of UPL's Highly Confidential information as well as other confidential information to which they may have access (for example, confidential information disclosed to UPL by a third party). Likewise, all UPL employees must limit their use of such information solely to performing their job responsibilities for UPL. New employees should sign an appropriate written confidentiality and use agreement when they join the Company either as a standalone document or as part of their employment agreements. If a confidentiality and use agreement is not signed when an employee joins the Company, he or she may be required to sign such an agreement at any time thereafter as permitted by applicable law. Where required or where UPL deems appropriate, such agreements may

inform employees of both their responsibilities and rights (e.g., "whistleblower immunity"). Note, however, that all employees are obligated to maintain the confidentiality and limit use of UPL's Highly Confidential information as well as other confidential information to which they may have access, regardless of whether they have signed a written confidentiality and use agreement.

b. Third Party Confidential Information: UPL respects the intellectual property of third parties and will not disclose or use third party confidential information for any purpose without permission. To the extent that any UPL employee has or knows confidential information belonging to former employers or other third parties, that information may not be disclosed to UPL, may not be stored on UPL networks or in UPL offices, and may not be used or disclosed for any reason in connection with the performance of job responsibilities for UPL without permission of the information owner. Such employees must educate themselves about the contractual limitations and obligations imposed on the third-party confidential information to which they have access. If an employee accidentally gains access to third party confidential information, they should immediately report the same to their manager or any member of the legal team.

Protecting UPL from unwanted and unintended use of third-party confidential information--as well as protecting UPL from unfounded allegations of information misuse--might involve development of additional, specific procedures as a risk management measure when circumstances warrant. For example, in unique situations UPL might determine to implement a "clean room" environment and/or erect "ethical walls" with respect to information sharing between certain employees, lateral hires, and projects. Such additional measures might be implemented solely out of an abundance of caution.

c. Invention Assignments: All inventions or other intellectual property of any kind created or discovered by an employee in the scope of his or her employment while employed by UPL, or using UPL's resources, equipment, or property, belong to UPL. Assignment of such intellectual property rights and their ownership are further detailed in the Global Intellectual Rights Policy.

Please refer to the Global Intellectual Rights Policy established by the IP team for this purpose.

d. Exit Interviews and Procedures: When an employee leaves the Company, the employee's supervisor, the Human Resources Department, and the Information Technology Department will work together to: (i) collect the employee's key cards, devices, all analyses, studies, personal notes and other documents prepared in relation to the employee's scope of employment; (ii) take reasonable steps to ensure that Company data are wiped from the employee's personal devices; and (iii) disable the employee's network access and physical access. During the employee's exit interview, the employee should be reminded of his or her continuing confidentiality and non-use obligations, contact information for the employee should be obtained, and the employee's future employment plans should be discerned. If necessary and appropriate, the employee's supervisor should see those relevant customers, suppliers, and other business partners are notified of the employee's departure. In the event

that the departing employee (1) regularly created or accessed UPL private business information while working for UPL and (2) will be working for a competitor of UPL in the future, addition investigative steps and instructions may be necessary (e.g., consultation with Legal, forensic inspections, execution of formal separation agreements) as permitted by applicable law.

3. Third Party Disclosure Management

a. Confidentiality Agreements: UPL's information and data should be shared strictly on a need-to-know basis with only those third parties who hold the responsibility to achieve the project objectives. At the time of sharing such information or data, in consultation with Legal, confidentiality and use agreements should be put in place with third parties. Confidentiality and use agreements must ensure that adequate provisions are in place to limit the information disclosed to third parties to the minimum necessary and that there is an explicit legal agreement which covers the exchange and use of UPL information. No UPL information should be disclosed to third parties including customers, external technical advisors, or vendors without executing a confidentiality and use agreement. The confidentiality and use agreement must not only impose a non-disclosure obligation on the third party to maintain the exchanged information in confidence, but also impose a non-use obligation on the third party to limit the use of any exchanged information solely to the narrowly defined purposes necessary to achieve project objectives. In appropriate circumstances, and with respect to certain UPL information expressly defined in the confidentiality agreement, such non-disclosure and non-use obligations may be perpetual in duration, for as long as the exchanged information remains confidential.

b. Public Disclosures: UPL believes in maintaining an active dialogue with its shareholders, external institutions and the public at large. In doing so, UPL personnel may be required to give public speeches, make external publications, trade show presentations, etc. At such times, it is imperative that only authorized personnel with best judgement and experience engage in such activities to ensure that no Highly Confidential or other confidential information is disclosed. Relevant UPL departments should conduct a review of communications being made in such scenarios. It is expected that prior to attending such public events, UPL personnel reach out to the organizers of these events to familiarize themselves with the nature of the event and ensure that UPL's participation will not put its Highly Confidential information at risk.

c. Disclosures to regulatory authorities: Various regulatory bodies, including securities market regulators, stock exchanges, authorities regulating product registrations etc. impose obligations on companies to adequately disclose material information through making filings, issuing press releases or other documentary submissions. UPL will comply with all government regulations that impose such obligations. This means that UPL submits all the information necessary for government review whether that information is classified as Highly Confidential, Confidential, Restricted or not.

UPL's compliance team and the regulatory staff, to the extent applicable, are accountable for ensuring that information submitted to such government regulatory authorities are

appropriately categorized and compliance with the demands of the authorities is monitored. As per this policy, no information will be withheld such that it has a material impact on the outcome of a regulatory review and any subsequent approval, but professional judgment will be exercised in the way the data are presented, i.e., confidential treatment by the regulatory authority will be requested where permitted and desirable, sensitive information might be submitted in summary form where permitted, and sensitive information might be withheld if not legally required to be submitted.

There may be some countries where UPL decides that the regulatory authorities are not sufficiently protective of confidential information and in these cases, UPL may choose not do business in those territories. This decision will be a commercial one, made by the relevant business team, with due regard to commercial, legal, and regulatory considerations.

4. Identification and classification of information

Identifying and classifying information appropriately is key to protecting information and at the same time ensuring that information can be accessed and used safely for the operations of the corporation. The accountability for identifying and classifying information including any Highly Confidential information rests with the relevant team who owns such information. When new information or a new product or concept is developed, a decision should be made by the relevant team on how to classify such information. The decision-making team is responsible for designing and developing a robust classification system, implementing it internally within the organization and communicating its decisions to the relevant personnel.

Teams may classify information as – Highly Confidential, Confidential, Restricted or Public, based on its nature and the extent of access that can be given to people within the organization of such information.

Classification	**Nature and Access to Information**	**Examples**
1. Highly Confidential	As defined above. Specific teams that have identified the information as Highly Confidential should have access.	As defined above – primarily in the Technical Information section of the definition.
2. Confidential	Available only to a limited number of specified personnel/staffs of the senior management in UPL.	Employee details such as compensation structures, certain financial data, information w.r.t Company structuring etc.
3. Restricted	Available to relevant group of personnel/staff, but not to the public. Restricted information is usually available to a broader group of employees than Confidential information, which is more limited in accessibility.	Technical information required for day-to-day business etc.

4. Public	Available to the public at large.	Annual accounts, Company policy and procedures etc.

Information classified as Highly Confidential, Confidential, or Restricted may qualify as a trade secret and/or for other protections under applicable law.

5. Implementation, Measures, Detection and Response

a. Implementation of Specific Procedures: The heads of the regional businesses and global functions are authorized to adopt, or delegate to the appropriate teams the adoption of, more specific procedures consistent with this policy, as needed, to protect Highly Confidential information in their scope of responsibility.

b. Physical and Digital Security Measures: At UPL, various efforts in the form of physical security measures shall be taken to protect its Highly Confidential and other valuable information at all times. These measures are in addition to the ones mentioned above in this Policy, i.e., executing confidentiality agreements, identifying and classifying information, conducting exit interviews, etc.

Key UPL offices shall have appropriate physical barriers installed, as needed, with limited and strict visitor access to ensure that no unauthorized personnel enter the premises. Measures appropriate to the facility in question, such as maintaining logbooks, conducting security checks, escorting visitors, and limiting their access inside the premises, issuing company badges, and retention and disposal of documents in a compliant manner, shall be adopted and followed.

All physical embodiments of Highly Confidential information, whether a prototype, working model or actual embodiment in use, shall be maintained in a restricted area that is under lock and key and out of public view. Employees or contractors shall put working materials or files containing Highly Confidential Information in a locked desk or filing cabinet when not in use.

Digital or electronic safety of Highly Confidential Information is also paramount. Relevant teams and stakeholders should liaise with local IT teams to set up safety processes/systems, as required, for adequate protection.

c. Information Sweep or Audit: To ensure successful implementation of this policy, relevant teams who own Highly Confidential information should routinely conduct internal audits or "sweeps" to determine whether the measures in place are effective and whether additional measures need to be put in place. While conducting such sweeps, teams should include in their scope, major company devices, relevant documents, electronic servers, as well as physical locations including offices, laboratories, manufacturing facilities, vendor/customer sites etc. In particular, relevant audit teams must be formed to carry such internal audits and sweeps.

Such an exercise will assist in taking stock of all the Highly Confidential information available to the relevant team and providing both general and targeted feedback on what can

be done to both strengthen the protection of current information and ensure ongoing implementation of protections measures in the future.

The key questions that a team should ask themselves for conducting an effective Highly Confidential information sweep should be: What are the measures in place to protect the information? Where is the information located? Who has access to it? What can be done to further safeguard such information? Should further awareness sessions be carried out for employees to strengthen their understanding of protection measures? Is better document labeling required to protect information? Are all policy statements in this policy being followed?

On the basis of routine information audits conducted by relevant teams and stakeholders, the procedures to be followed by the teams may be modified, or the policy itself may be updated and, if required, formal programs may be instituted for specific needs of such teams.

Please refer, for example, to the Information Security Management System, established by the IT team for this purpose.

d. Detection and Response Plan

Relevant teams should put in place appropriate mechanisms, including setting up of focused committees or working groups, to timely detect leakage of UPL private business information. It is the responsibility of all employees and third parties using UPL information to note and report any such incident to supervisors or other appointed contact persons in the relevant teams. Further, relevant teams should coordinate with their local Legal, HR or the IT department, as appropriate, for further assistance with investigation and response, depending on the kind of breach.