INFORMATION SECURITY POLICY

UPL has emerged as a force to reckon with in the global crop protection space. It has taken leadership, determination and grit for us to reach this position. To contend with fierce competition and surge forward, UPL needs to protect its intellectual property – proprietary knowledge we utilize to deliver superior value to our customers. This knowledge resides in the form of information assets across functional areas and offices of UPL.

Information assets represent the competitive advantage of UPL. Leakage of these assets to our competition is equivalent to leakage of investments and potential profits. Information security breaches result in direct financial losses and can also damage the reputation and market standing of our company.

It is essential for all employees of UPL, group companies of UPL and third parties to comply with information security policies and procedures. Irresponsible and disrespectful handling of information assets will adversely impact our collective benefit. Consequently, non-compliance cannot be tolerated and will result in disciplinary action against offenders – termination of employment/ contract and legal action.

INFORMATION SECURITY MANAGEMENT SYSTEM

The information Security Management System (ISMS) provides a control mechanism for ensuring adequate protection of information assets. The ISMS consists of Apex, Baseline, Line of Business and Technology policies and procedures that explicitly state how employees are expected to imbibe information security into their work culture.

The ISMS will be made visible through periodic training, corporate intranet, and handbooks issued to employees. The ISMS shall be amended on a periodic basis to incorporate learning and address emergent threats. Management's interpretation of clauses in the policies and procedures will be final and binding.