Group Lotus plc

Confidentiality Policy

August 2019

A5-A-2048 revision 2
Responsibility – Head of HR

Contents

1.0 Purpose

1.1 The purpose of this document is to detail the policy, principles and procedures for managing confidential information in the Company.

1.2 This policy applies to all employees, contractors, consultants and agency workers engaged to carry out work for or on behalf of a Lotus Group company.

This policy is non contractual.

2.0 Policy

2.1 It is the Company's policy to ensure that all confidential information is kept in a safe place and communicated to relevant parties only, in accordance with the Data Protection Act 1998, in preparation for the EU General Data Protection Regulations 2018 and relevant Lotus Group policies and guidelines.

2.2 Any breach shall be investigated and may result in disciplinary action.

3.0 Principles and Guidelines

3.1 It is the responsibility of the Company and all individual's engaged in its service to comply with all relevant rules, including but not limited to contractual clauses, the Data Protection Act 1998, EU General Data Protection Regulations 2018, Lotus' Confidentiality Classification System and any guidelines in relation to the use of company or people information which may be issued by the company from time to time.

3.2 Every individual shall at all times, during employment and indefinitely after its termination, observe strict secrecy as to the affairs and dealings of the company.

3.3 Individuals shall not use any of Lotus' secret and confidential information obtained during or in the course of their work in a manner which could jeopardise Lotus Group, its subsidiaries, associates or any related companies, or staff.

3.4 Individuals shall not release or divulge to any person or to third parties any information regarding Lotus or its products, expansion plans, business strategy, financial information, personal data or any operational matters without first obtaining the written approval of the Chief Executive Officer or any other authorised Director before its release.

3.5 All individuals have a duty to protect and control their department and the Company's confidential information and secrets from reaching the hands of those who are not required to have it, whether intentionally or unintentionally.

3.6 Any Intellectual Property Rights relating to the Company or any Group Companies or its activities shall not belong to any individual and shall vest absolutely in the Company.

3.7 Upon the request of the Company, the individual shall give full written details of all inventions and of all works embodying Intellectual Property Rights design or work and execute all documents and do all acts and things required to rest or perfect the vesting of all Intellectual Property Rights in the Inventions and the Information legally and exclusively in the Company or any nominee or assignee of the Company.

4.0 Procedure

4.1 Handling Confidential Information

4.1.1 Employees are responsible for understanding and operating in compliance with this policy.

4.1.2 The information must be transferred, used and stored via appropriate methods for the level of confidentiality and in accordance with the Data Protection Act 1998 and the future General Data Protection Regulations 2018.

4.2 Managing a Request for Confidential Information from a Third Party

4.2.1 Where an employee receives a request for confidential information from a Third Party, they should identify the type of information requested and the purpose of the request.

4.2.2 A Third Party could be, but not limited to: an individual, the parent company, subsidiaries, suppliers, banks, financial institutions, government departments etc.

4.2.3 Authorisation to provide the Third Party with the requested information must be obtained as in accordance with the Limits of Authority (D2-A-05)

4.2.4 When authorised appropriately the information can be sent to the requester, as per the appropriate method for the level of confidentiality, and in accordance with the Data Protection Act 1998 and the future General Data Protection Regulations 2018.

4.3 Managing Data Leakage

4.3.1 Where leakage of information occurs, the employee that discovers the leakage must report the breach to the Data Controller and/or Human Resources Department (HRD) as soon as possible.

4.3.2 The HRD will support the Department in investigating the breach and advise where necessary of formal action according to the Disciplinary Policy (A5-A-2037). NB *Data Breaches of personal data under GDPR*

*2018 article 31 will require **mandatory notification** without undue delay and within 72 hours to the Information Commissioner's Office (ICO) where likely to risk the rights and freedoms of a 'natural person'. Under article 32 where that risk is high the data controller must also notify the individual concerned.*

5.0 Lotus Confidentiality Classification System

5.1 All information within Lotus' control will be subject to a business impact risk analysis by the information or system owner, in order to gauge the effect of a loss of confidentiality, integrity or availability and shall be assigned a classification according to the standard information classification system detailed in the table below.

5.2 It is the departmental head or project managers responsibility to assess the risk for both Lotus and, if applicable, third parties to ensure classification rationale is understood by all parties involved and the information is treated as such.

5.3 All information falls into one of three classifications set out below, presented in order of increasing sensitivity.

Information Category	**Description**	**Examples**
C1 LOTUS UNCLASSIFIED	Information that may circulate freely outside of Lotus with no special protection. Information is not confidential and can be made public without any implications for Lotus. Integrity is important but not vital.	Product brochures widely distributed. Information widely available in the public domain, including publicly available Company web site areas. Financial reports required by regulatory authorities. e.g. Newsletters/press releases for external transmission
C2 LOTUS RESTRICTED/ CONFIDENTIAL	Routine business information, which Lotus wishes to keep within the Company; unauthorised disclosure outside of the Company would cause significant harm to the interests of Lotus.	Passwords and information on corporate security procedures. Know-how used to process client information.

	Information is restricted to management approved internal access and protected from external access. Unauthorized access could influence Company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital. Information under this category can only be disclosed to commercial partners, clients or suppliers if it is relevant to the business being conducted and the relationship is covered by an NDA	Standard Operating Procedures used in all parts of the Company's business. All Company developed software code, whether used internally or sold to clients
C3 LOTUS SECRET	This is information for which unauthorised disclosure (even within the Company) would cause serious damage to the interests of Lotus. Information collected and used by Company in the conduct of its business to employ people, to log and fulfill client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	Salaries and other personnel data Accounting data and internal financial reports Confidential customer business data and confidential contracts Non disclosure agreements with customers\suppliers Company business plans Project plans

5.4 Information assets will be marked with their classification in accordance with the criteria detailed above, so that people know how to apply the appropriate security protection.

5.5 Paper documents and electronic data must carry a classification, the business owner or author and a produced/last edited date.

5.6 Data hosts, such as USB's, logical drives, IT systems or networks will be classified according to the highest category of data held or in transit.

5.7 The appropriate level of Physical and Logical security are to be applied to protectively marked data, during production, storage, transit and destruction.

5.8 In cases where information is only sensitive for a specific period of time, the classification marking shall indicate a date or event after which the information can be de-classified or downgraded.

5.9 In cases where the text body of an e-mail message or attachments are considered to be classified C3, then this classification grade should be indicated in the subject of the e-mail message. Emails which do not state C3 in the subject line of an email will be considered either C2 or C1.

5.10 Third party information supplied to Lotus will be handled according to the owner's classification and handling instructions. In the absence of specific instructions information will be treated in accordance with the guidelines for handling C3 Lotus information.

6.0 Definition and Interpretation

Term	Definition
Confidential Information	All communications and information whether written, visual or oral, all materials relating to personal data of employees, potential employees, customers, suppliers, any invention, improvement, report, recommendation or advice given to the Company by the employee in pursuance of his obligations and concerning the business, associations, transactions or financial arrangements of the Group with any other persons or bodies, including other technical or commercial cooperation agreements.
Inventions	All patentable and non-patentable inventions, discoveries and improvements, processes and know-how, copyright works, new designs discovered or created by the employee in the course of or for the employment, or discovered or created by the employee as a result - whether directly or indirectly - of anything done by the employee in pursuance of his duties.
Trade Secrets	Any information in any form whatsoever

Term	Definition
	not generally known, and proprietary to the Company including but not limited to the information relating to their processes, operations, trade, products, research, development, manufacture, purchasing, business, business prospects, transactions, affairs, activities, know-how, intellectual property, accounting, finance, corporate planning, marketing and proprietary trade.
Patent	A grant made by a government that confers upon the creator of an invention the sole right to make, use, and sell that invention for a set period of time.
Data Protection Act 1998 (DPA)	Applies to "personal data" both manual and automated data.
E.U. General Data Protection Regulations 2018 (GDPR)	New legislation due to come into effect on 25 May 2018. Applies to the legal processing of "personal data", including manual, automated, online identifiers, pseudonymised, genetic and biometric with additional accountability requirements and individual's rights compared to the Data Protection Act 1998.
Natural Person	As per the E.U. General Data Protection Regulations 2018 - an identified or identifiable natural person ('data subject'); one who can be identified, directly or indirectly, in particular by reference to an identifier 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.

7.0 Roles and Responsibilities

Role	Responsibilities
Employee	Treat as highly confidential and hold strictly in confidence all information disclosed or that he has access to during the tenure of his employment and shall respect the confidence entrusted to him. Not disclose the information to any third party without prior written consent in accordance with the LOA, nor to be used by them in any manner which may, or likely to, cause loss or damage either directly or indirectly to any Group Company. Take all reasonable steps to minimise the risk of disclosure of the information. All reasonable precautions shall be taken to prevent unauthorised persons having access to the information and the employee shall make arrangement for the proper and secured storage of the information.
Head of Department or Project Manager	Assess the risk for both Lotus and, if applicable, third parties and to ensure classification rationale is understood by all parties involved and information is treated as such. To ensure staff are familiar with the confidentiality policy and confidentiality classification system. To implement company procedure and policy regarding confidentiality and identify confidentiality risks in the workplace.
Company	To identify principal risks and ensure the implementation of appropriate systems to manage these risks. To ensure that all confidential information are kept in a safe and secure place.