[COMPANY NAME]

POLICIES AND PROCEDURES

SUBJECT: **EU EMPLOYEE DATA PRIVACY POLICY**

PURPOSE:

To set forth the policy of _____ Corporation ("Company") in regard to its compliance with the Safe Harbor Principles of the U.S. Department of Commerce for the protection of employee data transferred from Company's subsidiaries and locations in the European Union ("EU") to the United States ("U.S.") as required by the EU Directive on Data Protection.

SCOPE:

This Employee Data Privacy Policy (the "Policy") applies to Company in its processing of employee data received from Company's subsidiaries and locations in the EU.

POLICY:

_____ Corporation is the U.S.-based public parent company of companies in many locations around the world, including the EU. The EU's comprehensive privacy legislation, the Directive on Data Protection (the "Directive"), requires that transfers of personal data take place only (1) where a relevant basis exists upon which a transfer may be made or (2) to non-EU countries that provide an "adequate" level of privacy protection for such data. The U.S. has not been recognized by the EU as a country that provides adequate protection for personal data. Nonetheless, the U.S. Department of Commerce, in consultation with the EU, has developed a "safe harbor" framework to assist U.S. companies in complying with the Directive. The safe harbor framework consists of seven "Safe Harbor Principles" with which Company must comply if it wishes to self-certify under the DoC's safe harbor. (Extensive materials regarding the Safe Harbor Principles can be found online at www.export.gov/safeharbor.) This Policy sets forth Company's procedures for complying with the Safe Harbor Principles in regard to employee data transferred from EU subsidiaries and locations.

This Policy, including the procedures discussed below, shall be communicated to all employees of Company's EU subsidiaries and locations and to all Company employees in the U.S. that process or otherwise have access to the "Employee Data" discussed below.

Compliance with this Policy is mandatory, and any employee failing to comply will be subject to disciplinary action, up to and including termination of employment.

PROCEDURES:

1. Notice

From time to time, Company receives personal data regarding employees of its EU subsidiaries and locations for the purposes of (a) general employment purposes (specifically, providing compensation benefits and related services, keeping updated organizational information, making employment-related decisions, and employee training) and (b) processing and investigating reports under Company's Business Ethics Program ("Employee Data"). For example, Employee Data could include one or more of the following: name, address, job title and other job information, location, compensation information, identification number (including, in some cases, national insurance number), employment history, and copy of employment agreement. Additionally, in the case of reports under Company's Business Ethics Program, Company may receive information about an employee's actions or inactions relative to a legal requirement or other legal or ethical issue covered by Company's Code of Conduct, Business Ethics Program, or Company policy.

Employee Data is transferred only to third parties acting as agents of Company for the purposes described above (i.e., general employment purposes or processing of reports under Company's Business Ethics Program). In no case does Company transfer Employee Data for any purpose not compatible with these purposes without first notifying the data subject. Further, except in limited and permissible circumstances, Company does not transfer to third parties Employee Data deemed "sensitive" under the Directive. Examples of circumstances in which the transfer of sensitive Employee Data is permissible include where the transfer is (a) in the vital interests of the data subject or another person; (b) necessary for the establishment of legal claims or defenses; (c) required to provide medical care or diagnosis; (d) necessary to carry out Company's obligations in the field of employment law; or (e) expressly permitted by an employee for a specific purpose.

Any employee of an EU subsidiary of Company may contact Company's Chief Compliance Officer or call the appropriate Business Ethics Program toll-free hotline with inquires or complaints regarding Company's processing of Employee Data or to "opt out" of the transfer of Employee Data as described in Section 2 ("Choice") below. An employee can obtain this contact information from Company's Business Ethics Program document or the employee's Human Resources representative or Local Compliance Officer.

2. Choice

Any employee whose Employee Data is to be transferred to third parties as described in this Policy may choose not to have his or her data transferred. The employee must communicate his or her desire to "opt out" by the means described in the last paragraph of Section 1 ("Notice") above. An employee exercising his or her right to "opt out" of the transfer of his or her Employee Data should be aware that, by doing so, he or she may lose access to compensation benefits or related services, the employee may be excluded from relevant organizational charts or other employee databases, and/or Company or its agent may be unable to provide training to the employee (which, in turn, may be required training under applicable Company or subsidiary policy). An employee may not opt out of the transfer of his or her Employee Data which is transferred by Company to a third party for the purpose of (1) meeting applicable legal requirements or (2) permitting the legitimate interests of Company in making promotions, appointments, or other employment decisions.

3. Onward transfer

In addition to the limitations of the transfer of Employee Data discussed above, Company transfers Employee Data only to those third parties who (a) have agreed in writing to provide at least the same level of privacy protection to the Employee Data as is required under the Directive or the Safe Harbor Principles and/or (b) adhere to the Safe Harbor Principles. Exceptions to this limitation on onward transfer include where an employee has granted Company express permission to transfer his or her data to the third party or where such transfer is necessary for the purpose of meeting an applicable legal requirement.

4. Security

Company takes reasonable precautions to protect Employee Data from loss, misuse, or unauthorized access, disclosure, alteration or destruction. Employee Data is maintained in secure electronic and manual files at Company, and access to these files is limited to Company employees for whom access is necessary to properly process the Employee Data consistent with the stated purposes. Employee Data that is transferred to third parties is done so by methods designed to reasonably reduce the risk that the Employee Data is lost, stolen, or inadvertently sent to a person or organization other than the intended recipient. Company retains Employee Data only as long as is necessary for its intended use, after which time the Data is deleted, destroyed, or returned. Company employees who are authorized to access the files for the stated purposes are trained periodically on this Employee Data Privacy Policy, with emphasis on the need to keep Employee Data private and secure and the potential disciplinary consequences for the failure to do so.

5. Data Integrity

Company personnel coordinate closely with personnel from Company's EU subsidiaries and locations (in particular the Information Technology and Human Resources personnel and Local Compliance Officers at these subsidiaries and locations) to ensure that Employee Data is up-to-date, accurate, complete, and reliable for its intended use.

6. Access

An employee whose Employee Data is processed by Company may request access to his or her Employee Data processed by Company for the purpose of correcting, amending, or deleting data that is inaccurate. Company may deny an employee's request to access his or her Employee Data where the burden or expense of providing access would be disproportionate to the risks to the requesting employee's privacy or where the rights of persons other than the requesting employee would be violated.

7. Enforcement

a. Recourse and remedies

As stated in the last paragraph of Section 1 ("Notice") above, employees in the EU whose Employee Data is processed by Company should report any complaints about such processing to Company's Chief Compliance Officer or by calling the appropriate Business Ethics Program toll-free hotline. Company will treat the complaint as a report under its Business Ethics Program, and the Chief Compliance Officer will initiate all of the procedures under that Program to investigate and resolve the complaint. (This process is described in detail in Company's Business Ethics Program document.) If the complaint is not resolved through this internal process, employees may report complaints to the U.S. Federal Trade Commission ("FTC") or the applicable EU Data Protection Authority ("DPA"). By voluntarily certifying that it will comply with the Safe Harbor Principles, Company has made itself subject to the dispute resolution, enforcement, and sanctioning powers of the FTC and has agreed to cooperate and comply with the applicable DPAs in regard to Company's processing of Employee Data.

b. Verification

To verify its compliance with the Safe Harbor Principles, Company, through its Internal Audit process, periodically (at least once a year) conducts a self-assessment to ensure that (a) this EU Employee Data Privacy Policy is accurate, comprehensive, prominently displayed, completely implemented and accessible, and conforms to the Safe Harbor Principles; (b) employees are informed of the internal arrangements for handling complaints and the independent mechanisms through which they may pursue complaints (see Section 7.a. above); and (c) Company has in place procedures for training the appropriate employees on the implementation of this Policy and disciplining those who fail to comply (see Section 4 above).

Company reserves the right to revise or amend this policy at any time. Any changes to this policy will be communicated to all appropriate employees and will not take effect until ten (10) days after such communication.

First Issued: