MARS

DATA PROCESSING POLICY (THE "POLICY")

OVERVIEW

This document sets forth Mars, Inc. and its subsidiaries', including Mars benefits trustees' ("Mars") Policy on the acceptable processing of Personal Data. In particular, it provides detail on the necessary data privacy and security requirements applicable to all suppliers to the extent that they collect, maintain and Process Personal Data. We refer to people covered by this Policy as "Suppliers".

DATA PRIVACY

- Suppliers will comply with Data Privacy Legislation, and use all reasonable endeavors to assist Mars in its own compliance with Data Privacy Legislation. This includes, without limitation, the preparation of necessary notifications, registrations and documentation which Mars may be required to make or enter into in order to comply with Data Privacy Legislation in connection with services provided by Suppliers to Mars.

- Suppliers will not do, or cause or permit to be done, anything in relation to the information provided to or processed by them which may result in a breach by Mars of any applicable laws, regulations, regulatory requirements, or the Data Privacy Legislation.

- Suppliers will only process the Personal Data in accordance with Mars' documented instructions, which may be specific instructions or standing instructions of general application in relation to the performance of their obligations under their agreement(s) with Mars, unless otherwise required by EU or EU Member State law to which a Supplier is subject. In such a case, the Supplier shall inform Mars of that legal requirement before carrying out the required Processing, unless that law prohibits such information on important public interest grounds.

- Suppliers shall put in place measures to ensure that any employees who have access to Personal Data do not process the data except on instructions from Mars, unless required to do so by EU or EU Member State law and that any employees who have access to Personal Data are reliable and have committed themselves to confidentiality.

- Suppliers will adopt all reasonable recommendations which Mars may make concerning measures, programs and procedures to be adopted to ensure ongoing compliance with the data privacy provisions of their agreement(s), including any company policies which Mars may have regarding information security which will be communicated to Suppliers.

- Suppliers will comply with the data transfer commitments set forth in "Privacy Shield Commitments" where applicable.

- Suppliers will not disclose the Personal Data to any other body (including any subcontractor) without Mars' express agreement in writing.

- Suppliers will not transfer Personal Data from the European Economic Area or relating to residents of the European Economic Area to any location outside the European Economic Area unless Mars has consented to such transfer and such transfer complies and continues to comply with the requirements for international data transfers under EU Data Privacy Legislation, or such transfer is required by EU or EU Member State law to which a Supplier is subject. In such a case, the Supplier shall inform Mars of that legal requirement before carrying out the required Processing, unless that law prohibits such information on important public interest grounds.

- Suppliers shall not subcontract any of their duties unless they have obtained Mars' prior express agreement in writing and the subprocessor is subject to a written agreement which is governed by EU Member State law to the extent that the agreement relates to European Personal Data. Any such agreement must impose on the subprocessor the same obligations that are imposed in connection

with services provided by Suppliers to Mars, including obligations to allow inspection and audit of their Processing activities. Any consent Mars gives for subcontracting will not relieve the Supplier of any liability for the performance of their obligations under any agreement in connection with services provided.

- Suppliers shall promptly notify Mars if they receive a request from a Data Subject to have access to Personal Data or exercise any other applicable Data Subject rights, or if they receive any other complaint or request relating to Mars' obligations under the Data Privacy Legislation. Suppliers will assist Mars insofar as possible in responding to any such complaint or request, including, without limitation, where authorised by Mars, by allowing Data Subjects to have access to their Personal Data or to have that Personal Data corrected, deleted, or blocked within the relevant time frames set out by applicable law; by providing Mars with any information Mars request relating to the Processing of Personal Data in connection with services provided by Suppliers to Mars; and by providing Mars with any Personal Data they hold in relation to a Data Subject, if required, in a commonly-used, structured, electronic, and machine-readable format.

- If Mars are required by the Data Privacy Legislation to carry out a Privacy Impact Assessment in relation to the services provided by Suppliers, the Suppliers will provide Mars with such support and information as Mars may reasonably require in carrying out such assessment.

- Suppliers will permit Mars (or their duly authorised representatives or any regulator to which they are subject) to inspect and audit their Processing activities in connection with the services they provide to Mars, (and/or those of any of their agents or subcontractors to whom they have been permitted by Mars to disclose the Personal Data), and comply with all reasonable requests or directions by Mars to enable Mars to verify and/or procure that they are in full compliance with their obligations in connection with services provided by them to Mars.

- Suppliers shall immediately inform Mars if in their opinion one of Mars' instructions infringes data protection provisions of the European Union or an EU Member State.

- If so requested by Mars at any time, Suppliers shall provide Mars with a copy of the Personal Data or (at our option) destroy it.

- Upon termination of the provision of services relating to Personal Data, the Suppliers shall delete or return all the Personal Data to Mars and delete any existing copies of the Personal Data, save where applicable law requires that the Supplier retain copies of such data. Where such Personal Data relates to EU residents, the Supplier may only retain copies where they are required to do so by European Union or European Member State law.

SECURITY

TECHNICAL AND ORGANISATIONAL MEASURES

Suppliers must at a minimum, implement and maintain appropriate technical and organisational measures to ensure the security and protection of Personal Data, taking into account the nature and sensitivity of the information to be protected, the risk presented by Processing, the state of the art, and the costs of implementation, in compliance with applicable Data Privacy Legislation. Such measures shall include appropriate physical, electronic and procedural safeguards to

- ensure the security and confidentiality of Personal Data;
- protect against any threats or hazards to the security or integrity of Personal Data; and
- prevent unauthorised access to or use of Personal Data.

Without limiting any other obligations in connection with services provided by Suppliers to Mars, and as a minimum standard, Suppliers will comply with the Massachusetts Code of Regulations, 201 CMR Sections 17.00 et seq., as applicable.

Suppliers will keep in force the security measures described in Exhibit A for so long as they are providing services to Mars. Where European Personal Data is processed, Suppliers warrant that such security measures meet the requirements of the applicable Data Privacy Legislation.

Suppliers shall promptly notify Mars of any reason why they cannot or are not likely to be able to comply with the security provisions in this paragraph, in which case Mars shall, at its sole discretion, be entitled to suspend or terminate the provision of any services provided by Suppliers.

DATA SECURITY BREACH NOTIFICATION

Suppliers must immediately notify Mars (security.response@effem.com / privacy@effem.com) if they know, discover or reasonably believe that there has been a Data Security Breach. In the event of a Data Security Breach, Suppliers will:

- immediately investigate, correct, mitigate, remediate and otherwise handle the Data Security Breach, including without limitation, by identifying Personal Data affected by the Data Security Breach and taking sufficient steps to prevent the continuation and recurrence of the Data Security Breach;
- provide information and assistance needed to enable Mars to evaluate the Data Security Breach and, as applicable, provide timely notices disclosing a Data Security Breach and comply with any obligations to provide information on the Data Security Breach to relevant regulators; and
- reimburse Mars for the reasonable expenses that Mars may incur as a result of such Data Breach caused by their acts or omissions or those of any of their authorized subcontractors, including but not limited to, the expenses incurred in investigating the Data Security Breach and notifying affected individuals, and providing these individuals with the support necessary under the circumstances, such as credit monitoring.

EXHIBIT A

LEGAL SECURITY RISK AND DUE DILIGENCE

Security Policies

- Suppliers must have a security policy demonstrating that they are committed to implementing an effective information security framework.
- Suppliers must validate that the security policy is fully implemented within their organizations.
- Suppliers' security policy and management must be compliant with ISO/IEC standards 27001:2005 and 27002:2005 (or equivalent standards). Suppliers' security must be certified by an accredited certification body.
- Suppliers must have a person or department responsible for security management.
- Suppliers must have sufficient resources and facilities made available to ensure security of information.
- Suppliers must have an effective system of recruiting and vetting personnel and training personnel in relation to security responsibilities and disclosure of information.
- Suppliers' staff and contractors must be bound to maintain the confidentiality of all appropriate data including Personal Data pursuant to executed confidentiality obligations, and for Mars data, and must be bound by confidentiality provisions at least as protective as those confidentiality obligations executed by Suppliers who are recipients of Mars data.
- Suppliers must have confidentiality policies in place to support implementation and enforcement of these obligations.
- Suppliers must have data privacy training required for personnel who have access to Personal Data. Suppliers must conduct such training at least annually.
- Suppliers must have an adequate procedure for authenticating the identification of intended recipients of information prior to disclosure.
- Suppliers must have an adequate procedure for authorizing and securing temporary removal of Personal Data.

Physical Security Measures

- Suppliers must require all persons to wear ID badges when on site.
- Suppliers must adequately secure (e.g., have measures been taken to make it resistant to attack) the site(s) where Mars data will be sent to and stored.
- Suppliers must adequately control (e.g. card readers, video surveillance) access to the building or room where the information is stored and/or processed .
- Suppliers must keep a list of personnel with access to facilities storing data. Suppliers must include third parties (e.g. maintenance firms) in such list.
- If applicable, Suppliers must take appropriate measures to ensure passers-by cannot read information off screens or documents.
- If access given to anyone outside the organization (e.g., to provide IT support), Suppliers must put appropriate security procedures in place to manage and oversee such access.
- Suppliers must lock away paper-based information at night, and maintain a list of personnel with access to such paper media.
- Suppliers must securely dispose of media and/or printed material when no longer required (e.g., through secure cross-cut shredding).

Computer Security Measures

- If applicable, Suppliers must have appropriate measures to ensure passers-by cannot read information off screens or documents.
- Suppliers must have authentication and logical access controls, including passwords, to control different levels of access to information depending upon requirements.
- Suppliers must require unique IDs for all personnel.
- Suppliers must have strong password requirements based on industry standards and appropriate to the data involved.

- Suppliers must physically or virtually separate Mars data from other clients' data. If Mars data is commingled with other clients' data, Suppliers must notify Mars.
- Suppliers must restrict access to data to a need-to-know basis.
- Suppliers must encrypt all laptops, removable media storage that store Personal Data, and hard drives.
- Suppliers must have appropriate security technologies in place to detect potential breaches or malware infections.
- If personnel are permitted to work remotely, Suppliers must have security features in place to secure remote connectivity.
- Suppliers must have effective antivirus and anti-hacking measures in place to prevent compromising the integrity of data or systems.
- Suppliers must have a program for identifying vulnerabilities and a program for applying patches in a timely manner.
- Suppliers must have pertinent logs secured and retained for at least 60 days for forensic analysis.
- Suppliers must have adequate procedures for secure destruction of systems and media used for data storage before being reused for other purposes.

Secure System Development Lifecycle

- Suppliers must have a secure coding program that ensures at a minimum that OWASP top 10 are addressed:
    - A1 Injection
    - A2 Broken Authentication and Session Management (was formerly A3)
    - A3 Cross-Site Scripting (XSS) (was formerly A2)
    - A4 Insecure Direct Object References
    - A5 Security Misconfiguration (was formerly A6)
    - A6 Sensitive Data Exposure (merged from former A7 Insecure Cryptographic Storage and former A9 Insufficient Transport Layer Protection)
    - A7 Missing Function Level Access Control (renamed/broadened from former A8 Failure to Restrict URL Access)
    - A8 Cross-Site Request Forgery (CSRF) (was formerly A5)
    - A9 Using Known Vulnerable Components (new but was part of former A6 – Security Misconfiguration)
    - A10 Unvalidated Redirects and Forwards
- Suppliers must have a change management process in place that requires all changes to be approved and tested prior to any change in production. The change management process must include roll back procedures.
- Suppliers must have adequate segregation of duties to prevent developers from making unauthorized changes to production.
- Suppliers must have an isolated development environment.

Dealing with Security Breaches

- Suppliers must have effective antivirus and anti-hacking measures in place to prevent the compromising of the integrity of data or systems.
- Suppliers must have an adequate procedure for secure erasure of systems and media used for data storage before being reused for other purposes.
- Suppliers must securely dispose of media and/or printed material when no longer required (e.g., through secure shredding).
- Suppliers must have an adequate procedure for authenticating the identification of intended recipients of information prior to disclosure.
- Suppliers must have an adequate procedure for authorizing and securing temporary removal of Personal Data, and security measures in place (e.g., when working from home or remotely).
- Suppliers must have an appropriate policy in place requiring all staff and system users to recognize and report breaches of security to the nominated security officer.
- Suppliers must have adequate procedures in place to manage and mitigate the risk arising from such breaches.

- Suppliers must have an adequate incident response procedure in place to ensure security incidents are investigated and resolved including lessons learned.

Business Continuity and Disaster Recovery

- Suppliers must have adequate business continuity and disaster recovery plans in place to provide effective protection against likely risks, for example, loss, damage, or corruption of information arising from:
    - Human error,
    - Computer virus,
    - Network failure,
    - Theft,
    - Fire,
    - Flood, and
    - Other disasters.
- Suppliers must have their business continuity and disaster recovery plans regularly tested.
- Suppliers must have adequate protection against possible loss of information due to failure of power supply (e.g. provision of uninterrupted power supply).
- Suppliers must have effective data backup and systems recovery operations that are independently tested.

Audit and Compliance Arrangements

- Suppliers must have tamper-proof audit trails maintained for all incident security actions affecting data.
- Suppliers must have regular random audit/assurance checks carried out to confirm security procedures are operating as expected.

PRIVACY SHIELD COMMITMENTS

Where EU Personal Data is transferred from a Mars US Entity, Suppliers warrant that as recipients of such Personal Data they are subject to the Privacy Shield and will:

- Only process the Personal Data in accordance with Mars' documented instructions and the consent provided by the individuals whose Personal Data they are Processing;
- Provide the same level of protection as the Privacy Shield Principles over the Personal Data the Company transfers to them;
- Notify Mars if they make a determination that they can no longer meet this obligation;
- Cease Processing or take reasonable and appropriate steps to remediate any inability to meet this obligation; and
- Assist Mars in responding to individuals whose Personal Data Mars transfers to them when they exercise their rights under the Privacy Shield.

COMPLIANCE

Mars reserves the right at its sole discretion to determine the appropriate action to be taken in the event that a Supplier violates this Policy. Such action may include the termination of any existing agreement to provide services to Mars.

FUTURE CHANGES TO THIS POLICY

Mars reserves the right to change this Policy at any time and for any reason.

DEFINITIONS

In this Policy, the following terms shall have the meanings set out below:

- "Data Subject" means a living individual who is the subject of any of the personal data;

- "Data Privacy Legislation" means all laws and regulations, in any country of the world, which protect the privacy rights of individuals, in so far as those laws and regulations apply to the Processing of personal data subject to this Policy, including without limitation data protection legislation enacted by the EU and EU Member States, US federal and state laws relating to data privacy, and similar measures;

- "Data Security Breach" means, (1) any unauthorized access to or acquisition of data that compromises the security, confidentiality or integrity of Personal Data, or (2) any unauthorized disclosure of, access to or use of any Personal Data, or (3) any unauthorized intrusion into systems containing Personal Data resulting in unauthorized access or access in excess of authorization;

- "Personal Data" shall mean any information which relates to an identified or identifiable living individual which is processed by a Supplier (and for this purpose an identifiable individual is one who can be identified, directly or indirectly, (i) from that information or (ii) from that information and any other information which is in the possession of, or likely to come into the possession of, the entity controlling the Processing of that information); and

- "Processing" shall mean any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.