PURPOSE OF POLICY

The purpose of this policy is to define how the retention and erasure of Information Data is managed in accordance with applicable legal, regulatory or contractual requirements for and on behalf of Marshall Aerospace and Defence Group and its subsidiaries (MADG).

POLICY AUTHORITY

This policy document is issued under the authority of the CEO.

Any guidance required in relation to this policy should be directed to the relevant compliance department that govern how the valued or protected information types listed below are managed.

The relevant compliance departments are listed in Appendix A of this document.

APPLICABILITY

This policy is applicable to all forms of media storage (e.g. Paper, Removable media, network storage areas and other repositories where information data is held).

All information Data is covered by this Policy. However, the following types of information data are subject to regulatory & legal retention and erasure controls (includes but not limited to):

- Personal Identifiable Information (PII)
- Security Aspects Letters (SALS)
- Controlled Technical Information (CTI)
- Financial (FIN)
- Export Control (ITAR/EAR)
- Contractual (CON)
- CopyRight/Intellectual Property (IP)
- Training Records (TRN)

DETAILED POLICY STATEMENT

The Confidentiality, Integrity & Availability of the Information Data **MUST** be preserved at all times.

Information Data **MUST** be collected only for specified, explicit and legitimate purposes, where necessary, kept up to date. It **MUST NOT** be further processed in any manner incompatible with the intended purpose.

Information Data **MUST** be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. When Information data is no longer needed for specified purposes, it **MUST** be deleted or where appropriate Marshall ADG will use anonymization to prevent identification of data.

Information data **MUST** be accurate and, where necessary, kept up to date. It **MUST** be corrected or deleted without delay when inaccurate.

Information Data **MUST not** be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

Information Data **MUST** be stored and processed in accordance with the Policies, Processes & Guidelines that govern its use. No Information Data **MUST** be stored or retained outside of the Systems designed to protect and manage it.

Information Data **MUST** be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

Information Data records **MUST** be regularly reviewed to ensure that they remain adequate, relevant and limited to what is necessary to facilitate the carrying out of your work.

To comply with external legislation and contractual obligations, we are allowed to retain the applicable types of information for only as long as is necessary to satisfy the Company's obligations.

Where data information is subject to two or more legal or contractual retention controls the one with the longest duration period **WILL** take precedence.

When Information Data in the form of individual records or data sets are destroyed, whether held in paper or electronic form you **MUST** ensure that they are safely and permanently destroyed following the specified Policies, Processes & Guidelines.

Please refer to, the list of legal & regulatory retention periods and the controlling compliance departments for advice & guidance.

Note: That the Company has regard to legal risk, so in some cases may keep records in some instances longer than that specified by law and regulation.

Appendix A

Marshall

Appendix A Compliance Department Listing

Issue: 4 Date: 29 April 2019

Information Asset Controllers			
Role	Notes	For example (but not limited to)	Email Address
Data Privacy Manager	Responsible for the management and control of Personal Identifiable information	Name, Address or salary of a person or persons	DataPrivacyManager@MarshallADG.com
Trade Control Officer	Responsible for the management and control of Company Assets that are subject to ITAR/EAR control	Exports of Data or services that relate to US defence. Including physical objects, as well as software and technology	ExportCompliance@MarshallADG.com
Security Standards and Assurance Manager	Responsible for the management and control of Company Assets that are subject to Security Aspects Letter controls	Documentation that is restricted to UK EYES only	ListX.Security@MarshallADG.com
Commercial Management	Responsible for the management and control of Commercially sensitive data or data where IP has been applied	Data supplied by the customer on the condition that the data will only be used in relation to their contract and will be removed once the contract has been completed	Commercial.Compliance@MarshallADG.com
Head of Financial Reporting and Control	Responsible for the management and control of Company Financial Information	Full Budgetary forecasts	
Cyber Security Manager	Responsible for the security of the ICT Technology Estate	Cyber security breaches or indications of hacking activities	Cyber.Security@MarshallADG.com
Data Privacy Manager	Temporarily responsible for capturing breaches for all other breach types	e.g Financial data until a Financial breach handler is in post. IP and contractual data, until the contact details have been confirmed Any other breach type not specified here.	DataPrivacyManager@MarshallADG.com

Definitions

MADG Marshall Aerospace and Defence Group and its subsidiaries

Removable media (includes but is not restricted to the following):

- CDs, DVDs, floppy and optical Disks.
- External Hard Drives (HDD).
- USB Memory Sticks (also known as pen drives or flash drives).
- Media Card Readers.
- Embedded Microchips and storage cards (including those on mobile phones and PDAs).
- MP3 and other music/media players.
- Digital Cameras.
- Backup Cassettes.
- Audio Tapes (including Dictaphones and Answering Machines).

Associated Policies

BMS1003- ICT Asset Management Policy - Backup
BMS1003- ICT Asset Management Policy – Restore - TBD
BMS0699 – Disposal Policy

Associated Guidelines

There are no Guidelines associated to this Policy at this time.

Associated Processes

BMS0699-U01 – Waste Disposal User Guide