

DATA RETENTION POLICY

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 of Cambridge (Holdings).

POLICY AUTHORITY

This policy document is issued under the authority of the Group Company Secretary. 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.

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)
- Copy Right/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 of Marshall of Cambridge (Holdings) 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.

Definitions 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).