TUDOR Business Services Ltd

Data Retention & Destruction Policy

INTRODUCTION & BACKGROUND

What does this Policy mean to me?

The quantity and volumes of information (whether in electronic, hard copy print or hand written form) our business creates, receives and manages is growing at an exponential rate. Our Customers, Shareholders, Business Partners and People trust us to ensure we keep only the information that is reasonable and appropriate for us to run and operate our business. This policy makes sure that this trust is well placed.

We have defined our commitment, where practically possible, to not just manage our retention of documents and but more importantly our commitment to the destruction of all documents and records that exceed our retention guidelines in a timely, consistent and uniform way.

This is a company-wide commitment. It is incumbent on each of us to ensure our compliance with this policy and to be vigilant in our destruction of the data that exceeds the agreed retention periods. Whilst, of course, not every schedule will apply to every area of Tudor, you should familiarise yourself with the retention periods applicable to the documents and records that you deal with on a day-to-day basis.

> Exceptionally, you may be alerted by the main office (in the form of a “Stop Notice”) that you are not to destroy documents which are relevant to a legal dispute. If you are aware of a potential dispute, documents which may be relevant to that dispute should not be destroyed, but if you are in any doubt, speak to the main office.

The Policy applies to all Tudor people and you are responsible for the information that you hold.

- If you are the Head of Department where information is stored, either on paper or electronically, then you must ensure that processes within your department adhere to this Policy.

- If you are the business owner or the system owner of any electronic system that involves the processing of information, then you must adhere to this Policy.

The Policy applies to information held in operational and production systems and in archive as well as that stored in system log files and in back-up. It also applies to all information held or processed by third parties on Tudor’s behalf, i.e. suppliers and data processors.

Who to contact about this Policy? Any questions regarding this Policy should be directed to your Data Protection Co-ordinator.

Impact of the Policy on Conditions of Employment
This Policy does not form part of your contract of employment.

POLICY FOR INFORMATION RETENTION

- Tudor shall retain information only for the specified retention periods set out in this Policy and shall then arrange for the prompt and secure disposal of that information.

- Information must not be retained for more than six years from the date of creation and customer information for no more than seven years following the closure of a customer account.

- Exceptions to this Policy must be approved by Tudor's Executives.

- All information must be disposed of in accordance with Tudor's security policies on document and data disposal.

- Electronic data must be disposed of in accordance with IS Security Standard ISS002 –Data Disposal and Sanitation

- Hardcopy information must be securely destroyed (using Tudor-supplied shredders or confidential waste bins.

Log Files

- Information held within log files created automatically during system operation shall be covered by this Policy.

- Entries shall be retained for the time required to meet the purpose of the log file, although information stored in the log files must not be kept beyond the retention periods stated in this Policy.

Back-Up Data

- Back-up data is data kept solely for the purpose of replacing other data in the event of their being lost, destroyed or corrupted.

- Data stored in back-up must not be kept beyond the retention periods stated in this Policy.

Payment Card Information subject to the PCI DSS Standard

- We must not store or retain the following credit card information in any form subsequent to a credit card transaction being processed.

- Personal identification number (PIN) or the encrypted PIN block.

- Card-verification code or value (three-digit or four-digit number printed on the front or back of a payment card, often referred to as CVV2, CV2, CSC or CVD) used to verify card-not-present transactions.

- Full contents of any track (full track, track, track 1, track 2, magnetic-stripe data) from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere).

One of the following for any system processing payment cardholder information will be implemented:

- A programmatic process (automatic or manual) to remove or sanitise the card holder data (to mask the Primary Account Number (PAN)), at least quarterly, stored cardholder data that exceeds requirements as defined in the this retention policy; or

- A manual review, conducted at least quarterly, to verify that stored cardholder data does not exceed requirements as defined in this retention policy.

- All cardholder data must be secured in the designated Tudor Secure Cardholder data environments.

Credit card data must NEVER reside outside of the Tudor designated Secure Card Data Environments. If such data is discovered outside of these designated environments, you must report it to the main office for investigation and arrangement for secure destruction.

Stop Notices
Exceptionally, data and documents must not be destroyed at the end of the retention period when:

- a Stop Notice has been issued for specified types of information (paper or otherwise), confirmed by the main office; or

- circumstances exist that would justify a 'Stop Notice' being issued, i.e. there is current, pending or threatened litigation for which the information might be required as evidence or the business is the subject of any regulatory investigation to which the record may be relevant. The main office will confirm if this is the case.

The Legal Department or Group Security will inform the business owners and system owners that a Stop Notice has been issued and those owners shall inform all appropriate users and resources with access to their systems to ensure compliance with the Stop Notice.

The business and system owner shall confirm compliance with the Stop Notice and will immediately inform the main office of any non-compliance. Once in place, and until the lifting of the Stop Notice, all information that is the subject of the Stop Notice should be retained in its existing form and must not be destroyed.

Electronic Mail and Instant Messaging
Individuals are responsible for applying Data Retention Policy requirements to emails sent and received from their Tudor business email account and to instant messaging conversations.

Emails and Instant Messages that contain no business information and are inconsequential (such as saying that you are running late for a meeting) are to be deleted promptly once they have been read and acted upon.

GUIDELINES FOR INFORMATION RETENTION

If you have data or a document that is not contained within the retention schedule in Appendix C, you should seek guidance from Tudor's Main Office.

- Information should be reviewed at regular intervals to determine which ones are to be retained or destroyed.
- Such intervals shall be at least quarterly.
- In the case of the winding up/striking off of any Tudor company, certain records need to be retained, e.g. by virtue of the Insolvency Regulations 1994 or for other reasons (e.g. if the registers contain information not capable of being obtained from Companies House in the event that the company is restored to the register) –a review should be undertaken of applicable legislation at the time of winding up/striking off.

When you submit paper documentation to archive storage, you must set a date for destruction for that documentation, and it is your responsibility, not the archives' to ensure that compliance is demonstrated.

EXEMPTION PROCESS

In exceptional circumstances, where any requirement or principle contained in this Policy cannot be met, an exception may be requested. Provided that the exemption request is reasonable, proportionate and justifiable in the prevailing circumstances and does not expose Tudor, its customers or employees to unacceptable risk.

Appendix A Definitions and Abbreviations

Definitions used in this Policy

"Closure of Customer Account " means the date at which the cancellation or termination of a Tudor customer account takes effect.

"Personal Data" means data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of intentions of the data controller or any other person is respect of the individual.

"Payment Cardholder Information" means any of the following information from a payment card:
(a) Sensitive Authentication Data,
(b) the primary account number (PAN), if not masked, truncated, or securely hashed, or
(c) the cardholder's name, payment card expiration date or service code when stored or used in conjunction with a PAN (as defined in (b)).

"PCI DSS" is the Payment Card Industry Data Security Standard, version 2.0 (Oct. 2010), and superseding versions as in effect and applicable to Tudor from time to time.

"Sensitive Authentication Data" is the security-related information from a payment card used to authenticate cardholders, such as;

a) validation code or value used to verify "card-not-present" transactions,
b) contents of any track of the magnetic stripe, or
c) personal identification number (PIN), if appearing in plaintext or otherwise unprotected form.
d)

Appendix B

Legislation and Regulation applicable to this Policy

Companies Act 1985 (as amended)
Companies Act 2006
Data Protection Act 1998 (and Ireland's Data Protection Acts of 1988 and 2003)
Limitations Act 1980