

## Data Handling Policy

### 1. Purpose

The purpose of this policy is to define a system of categorising information in relation to its sensitivity, confidentiality and to define associated rules for the handling of each category of information to ensure the appropriate level of security (confidentiality, integrity and availability) of that information.

The policy aims to:

- protect information from accidental or deliberate compromise, which may lead to damage, and/or be a criminal offence.
- help to meet legal, ethical and statutory obligations.
- protect the interests of all those who have dealings with Threeshires Ltd and about whom it may hold information (including its staff, collaborators, business partners, etc.)
- promote good practice in relation to information handling.

### 2. Scope

- This policy covers all information held by and on behalf of Threeshires Ltd and the handling rules shall apply to employees of the Threeshires Ltd and to third parties handling Threeshires Ltd or Client information. Where Threeshires Ltd holds information on behalf of another organisation with its own information classification agreement shall be reached as to which set of handling rules shall apply.

### 3. Relationship with existing policies

- This policy forms part of Threeshires Ltd Information Security Policies. It should be read in conjunction with the “Information Systems Security Manual and Guidelines” and all supporting policies.

### 4. Policy Statement

- All Data held by Threeshires Ltd, in all formats including electronic and physical documentation, shall be deemed to be owned by Threeshires Ltd.
- All Data created by Threeshires Ltd, which is utilised by third parties, on Non-Threeshires Ltd equipment or storage, shall still be deemed to owned by Threeshires Ltd.
- Any third party must request permission to have access to and utilise data deemed to be held by Threeshires Ltd.
- All employees of Threeshires Ltd and third parties who handle information on behalf of Threeshires Ltd have a personal responsibility for ensuring that appropriate security controls are applied in respect of the information they are handling for Threeshires Ltd. Appropriate security controls may vary according to the classification of the information and the handling rules for the relevant category shall be followed.
- Automatic technical controls may be implemented to assist users in complying with these controls, but where technical measures are not implemented users are responsible for complying with this policy.

<b>Filename:</b>	Data Handling Policy	<b>Approved by:</b>	Nicola Rudko	<b>Issue Version:</b>	02
<b>Reference:</b>	PO16	<b>Position:</b>	Compliance Manager	<b>Issue Date:</b>	February 2022
<b>Category:</b>	Policies	<b>Signature:</b>		<b>Last Reviewed</b>	February 2022
This document is uncontrolled when printed					

## 5. Policy

- 5.1 All information held by or on behalf of Threeshires Ltd shall be categorised according to the Information Classification (Annex 1). The categorisation shall be determined by the originator of the information and all information falling into the classified categories shall be marked as such.
- 5.2 Information shall be handled in accordance with the Information Handling Rules (Annex 2) and where information falls within more than one category, the higher level of protection shall apply in each case.
- 5.3 Where a third party will be responsible for handling information on behalf of Threeshires Ltd, the third party shall be required by contract to adhere to this policy prior to the sharing of that information.
- 5.4 Where Threeshires Ltd holds information on behalf of another organisation with its own information classification, written agreement shall be reached as to which set of handling rules shall apply prior to the sharing of that information.

## 6. Responsibilities

- 6.1 The Data Protection Officer shall ensure that the Information Classification and associated Handling Rules are reviewed regularly to ensure they remain fit for purpose.
- 6.2 It shall be the responsibility of every individual handling information covered by this policy, to mark classified material as such, to apply the appropriate handling rules to each category of information, and to seek clarification or advice from a Senior Manager or the Quality Manager where they are unsure as to how to label or handle information.
- 6.3 All members of Threeshires Ltd shall report issues of concern in relation to the application of this policy, including alleged non-compliance, to the Data Protection Officer/Quality Manager.

## 7. Compliance

- Breaches of this policy may be treated as a disciplinary matter dealt with under Threeshires Ltd staff disciplinary policies. Where third parties are involved breach of this policy may also constitute breach of contract.

## 8. Data Storage

- All current and future data is to be solely stored within the United Kingdom.
- Confirmation by Microsoft Azure verified Threeshires Ltd Cloud Storage within the United Kingdom.
- All previous inceptions of data storage are within Piper Hole Farm Offices and Threeshires Ltd Mobile Equipment.
- No Threeshires Ltd Equipment is allowed to be used outside of the United Kingdom to access centrally held data and 'Conditional Access' Restrictions are active to limit connectivity.

<b>Filename:</b>	Data Handling Policy	<b>Approved by:</b>	Nicola Rudko	<b>Issue Version:</b>	02
<b>Reference:</b>	PO16	<b>Position:</b>	Compliance Manager	<b>Issue Date:</b>	February 2022
<b>Category:</b>	Policies	<b>Signature:</b>		<b>Last Reviewed</b>	February 2022
This document is uncontrolled when printed					

## 9. Third Party Data Access

- Threshires Ltd will allow, under authorised control, specific verified users access to shared data. This may utilise the Microsoft Cloud Sharepoint platform, that is only allowed to specific partner Domains and data area.
- The data within the shared area, shall only be classified as Public. (Annex 1)
- Breaches of this policy may be treated as a disciplinary matter dealt with under Threshires Ltd staff disciplinary policies. Where third parties are involved breach of this policy may also constitute breach of contract.

## 10. Restrictions

- Threshires Ltd Operational Mobile Field Equipment shall have 'Read Only' access to shared data.
- Only authorised equipment is allowed to connect to Threshires Ltd networks and data. Any non-authorised access will be deemed to be in breach of Threshires Ltd policies.

<b>Filename:</b>	Data Handling Policy	<b>Approved by:</b>	Nicola Rudko	<b>Issue Version:</b>	02
<b>Reference:</b>	PO16	<b>Position:</b>	Compliance Manager	<b>Issue Date:</b>	February 2022
<b>Category:</b>	Policies	<b>Signature:</b>		<b>Last Reviewed</b>	February 2022
This document is uncontrolled when printed					

**Annex 1 – Information Classification**

Level	Description	Protection Required	Examples
Personal	Non-business data, for personal use only	No Threshires Ltd requirement	
Public	Threshires Ltd information that is specifically prepared and approved for Client consumption. This is information which does not require protection and is considered ‘open’ or ‘unclassified’ and which may be seen by anyone whether directly linked with Threshires Ltd or not.	<p>Key security requirement: Availability</p> <p>This information should be accessible to Threshires Ltd whilst it is required for business purposes</p> <p>Back up requirements will need to be considered in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it?</p>	<p>Tenders, Processes and prepared information.</p> <p>Key Information Sets</p> <p>Press releases (not under embargo).</p> <p>Open content on Threshires Ltd web site.</p> <p>Fliers and publicity leaflets</p> <p>Published information released under the Freedom of Information Act responses</p> <p>Policies once they are approved, Annual Report and Financial Statements</p>
Restricted	Non-Confidential information where dissemination is restricted in some way e.g., to employees of Threshires Ltd, partners, suppliers or affiliates. Access to this information enhances Threshires Ltd	<p>Key security requirements: Availability</p> <p>This information should be</p>	<p>Some Operational meeting minutes</p> <p>Directory of contact details</p>

<b>Filename:</b>	Data Handling Policy	<b>Approved by:</b>	Nicola Rudko	<b>Issue Version:</b>	02
<b>Reference:</b>	PO16	<b>Position:</b>	Compliance Manager	<b>Issue Date:</b>	February 2022
<b>Category:</b>	Policies	<b>Signature:</b>		<b>Last Reviewed</b>	February 2022

Level	Description	Protection Required	Examples
	<p>operations by facilitating communication and collaboration between employees and external partners, but access is restricted and governed by appropriate policies or contracts</p> <p>The documents may be restricted to Threshires Ltd or to an external partner.</p> <p>Note that documents marked 'Restricted' might lose this marking over time</p>	<p>accessible to Threshires Ltd whilst it is required for business purposes</p> <p>Back up requirements will need to be considered in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it?</p>	<p>Procurement documents</p> <p>internal briefing papers</p>
Confidential	<p>Information which is sensitive in some way because it might be personal data, commercially sensitive or legally privileged or under embargo before being released at a particular time.</p> <p>This data has the potential to cause a negative impact on individuals' or Threshires Ltd interests (but not falling into Highly Confidential)</p> <p>It also includes information in a form that could not be disclosed under Freedom of Information legislation. Covers data about an individual and data about the Business.</p> <p>This information, if compromised, could:</p> <ul style="list-style-type: none"> <li>• cause damage or distress to individuals</li> <li>• breach undertakings to maintain the confidence of information provided by third parties.</li> <li>• breach statutory restrictions on the use or disclosure of information or lead to a fine, e.g.</li> </ul>	<p>Key security requirements:</p> <p>Confidentiality and integrity</p> <p>This information requires security measures, controlled and limited access and protection from corruption</p> <p>Back up requirements will need to be considered in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it?</p>	<p>Data contains private information about living individuals and it is possible to identify those individuals <i>e.g., individual's salaries.</i></p> <ul style="list-style-type: none"> <li>• Non-public data relates to business activity and has potential to affect financial interests and/or elements of Threshires Ltd reputation <i>e.g., tender bids prior to award of contract.</i></li> <li>• Non-public information that facilitates the protection of Threshires Ltd assets</li> </ul>

<b>Filename:</b>	Data Handling Policy	<b>Approved by:</b>	Nicola Rudko	<b>Issue Version:</b>	02
<b>Reference:</b>	PO16	<b>Position:</b>	Compliance Manager	<b>Issue Date:</b>	February 2022
<b>Category:</b>	Policies	<b>Signature:</b>		<b>Last Reviewed</b>	February 2022

Level	Description	Protection Required	Examples
	<p>for a breach of the Data Protection Act or Competition Law</p> <ul style="list-style-type: none"> <li>• breach contractual agreements</li> <li>• breach a duty of confidentiality or care</li> <li>• cause financial loss or loss of earning potential to Threshires Ltd</li> <li>• disadvantage Threshires Ltd in commercial or policy negotiations with others</li> <li>• prejudice the investigation or facilitate the commission of crime</li> <li>• undermine the proper management of Threshires Ltd and its operations</li> </ul>		<p>in general <i>e.g. access codes for lower risk areas</i></p> <p>Internal Reports Commercial Contract</p> <p>Data relating to living individuals, whether employees of Threshires Ltd or not.</p> <p>Data that is commercially sensitive to a project or a company providing research funds.</p>
Highly Confidential	<p>Has the potential to cause serious damage or distress to individuals or serious damage to Threshires Ltd interests if disclosed inappropriately.</p> <p><i>Refer to Impact levels of 'high' or 'major' on the Risk Measurement Criteria</i></p> <ul style="list-style-type: none"> <li>• Data contains highly sensitive private information about living individuals and it is possible to identify those individuals <i>e.g. Medical records, serious disciplinary matters</i></li> </ul> <p>Non-public data relates to business activity and has potential to seriously affect commercial interests and/</p>	<p>Key security requirements: Confidentiality and integrity This information requires significant security measures, strictly controlled with limited access and protection from corruption</p> <p>Back up requirements will need to be considered in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it?</p>	<p>Employee personal details Financial transactions</p> <p>Research data <i>Medical records,</i></p> <p>serious disciplinary matters corporate reputation <i>e.g. REF strategy</i></p> <p><i>access codes for higher risk areas</i></p>

<b>Filename:</b>	Data Handling Policy	<b>Approved by:</b>	Nicola Rudko	<b>Issue Version:</b>	02
<b>Reference:</b>	PO16	<b>Position:</b>	Compliance Manager	<b>Issue Date:</b>	February 2022
<b>Category:</b>	Policies	<b>Signature:</b>		<b>Last Reviewed</b>	February 2022

Level	Description	Protection Required	Examples
	<p>or Threshires Ltd corporate reputation <i>e.g. REF strategy</i></p> <ul style="list-style-type: none"> <li>• Non-public information that facilitates the protection of individuals' personal safety or the protection of critical functions and key assets <i>e.g. access codes for higher risk areas, Threshires Ltd Network passwords.</i></li> </ul>		<p><i>Threshires Ltd network passwords.</i></p> <p>papers relating to possible redundancies,</p>

Information may also be marked with a descriptor, which identifies the reason why the classification is applied. The expiry date for the current level may also be given. For example:

- Confidential - personal
- Confidential - commercially sensitive

Qualifying descriptors may also be used to incorporate/map to protective markings from other classification schemes, where employees are working with external partners, data and schemes. For example: Confidential - GPMS Secret.

<b>Filename:</b>	Data Handling Policy	<b>Approved by:</b>	Nicola Rudko	<b>Issue Version:</b>	02
<b>Reference:</b>	PO16	<b>Position:</b>	Compliance Manager	<b>Issue Date:</b>	February 2022
<b>Category:</b>	Policies	<b>Signature:</b>		<b>Last Reviewed</b>	February 2022

## Annex 2 Data Handling

Class	Description	Storage	Dissemination and access	Exchange and collaboration	Disposal
Public	Threshires Ltd information that can be seen by anyone.	Electronic information should be stored using Threshires Ltd provided IT facilities to ensure appropriate management, backup and access.	Information can be shared via the web after requiring approval. Electronic and hard copy information can be circulated freely subject to applicable laws e.g. copyright, contract, competition May be accessed remotely and via portable and mobile devices without encryption.	Information can be exchanged via email or file sharing without needing encryption.	Electronic information should be deleted using normal file deletion processes in accordance with any retention schedule. Printed copy should be disposed of and in accordance with any retention schedule.
Restricted	Non-confidential information where dissemination is restricted in some way e.g. information restricted to members of Threshires Ltd, project or partnership.	Electronic and paper-based Information must be stored using Threshires Ltd provided facilities.	Information can be shared via the web, but the user must provide Threshires Ltd authentication, or a federated authentication Electronic and hard copy information can be circulated on a need-to-know basis to Threshires Ltd Employees subject to	Information can be sent in unencrypted format via email. Information can be shared using Threshires Ltd IT facilities e.g. OneDrive, SharePoint, shared filestore. Information can be printed and circulated via Threshires Ltd internal mail service.	Electronic equipment holding this information must be disposed of using Threshires Ltd secure IT waste disposal service and in accordance with any retention schedule. Printed copy should be disposed of via Threshires Ltd confidential waste

<b>Filename:</b>	Data Handling Policy	<b>Approved by:</b>	Nicola Rudko	<b>Issue Version:</b>	02
<b>Reference:</b>	PO16	<b>Position:</b>	Compliance Manager	<b>Issue Date:</b>	February 2022
<b>Category:</b>	Policies	<b>Signature:</b>		<b>Last Reviewed</b>	February 2022



Class	Description	Storage	Dissemination and access	Exchange and collaboration	Disposal
			<p>applicable laws (e.g. copyright) and Threshires Ltd Regulations</p> <p>May be accessed remotely and via disk-encrypted portable and mobile devices without further encryption.</p>		<p>scheme and in accordance with any retention schedule.</p>
Confidential	<p>Information which is sensitive in some way because it may be personal data, commercial or legal information, or be under embargo prior to wider release.</p> <p>Includes data about individuals, and data about Threshires Ltd. May also include data provided to Threshires Ltd by other organisations e.g. research datasets</p>	<p>Information must be stored using Threshires Ltd IT facilities. Portable devices must have full disk encryption. Unencrypted removable media (e.g. USB sticks) must not be used. Encrypted removable media are not permitted without undertaking evaluation of other options and authorisation of the Quality Manager.</p> <p>Storage on Personally owned (e.g. home)</p>	<p>Access to confidential data must be strictly controlled by the Data Owner who should conduct regular access reviews.</p> <p>Some types of confidential information may be shared with authorised users via Threshires Ltd IT facilities, including remote access, subject to Threshires Ltd authentication. For web access encryption must be used.</p> <p>Confidential data must not be extracted from Threshires Ltd IT</p>	<p>The method to be used for exchanging confidential information must take account of the nature and volume of the data to be exchanged so that the impact of inappropriate disclosure can be assessed and an appropriate method selected. Approved data exchange methods are available from Digital Services. Confidential data must be encrypted prior to exchange.</p> <p>Exchange must be conducted using Threshires Ltd provided facilities. Duplicate copies of confidential information must be avoided. Where copies are necessary the protective marking must be carried with the data. Where paper copies are required for circulation or sharing, secure delivery methods must be used. Paper and electronic copies must be</p>	<p>Electronic equipment holding this information must be disposed of using Threshires Ltd secure IT waste disposal service and in accordance with any retention schedule. Printed copy should be disposed of in accordance with any retention schedule via Threshires Ltd confidential waste scheme or shredding facilities. Large accumulations of data should not be downloaded or copied.</p>


<b>Filename:</b>	Data Handling Policy	<b>Approved by:</b>	Nicola Rudko	<b>Issue Version:</b>	02
<b>Reference:</b>	PO16	<b>Position:</b>	Compliance Manager	<b>Issue Date:</b>	February 2022
<b>Category:</b>	Policies	<b>Signature:</b>		<b>Last Reviewed</b>	February 2022

Class	Description	Storage	Dissemination and access	Exchange and collaboration	Disposal
		computer is NOT permitted.	<p>systems and stored on local IT systems.</p> <p>If a portable device (e.g. a laptop, tablet or phone) is used to access Threshires Ltd confidential information, the device must be encrypted and require a password or PIN to access</p>	<p>marked 'Confidential' and the intended recipients clearly indicated. An optional descriptor, to state the reason for confidentiality, may be used. Electronic equipment holding this information must be disposed of using Threshires Ltd secure IT waste disposal service and in accordance with any retention schedule.</p> <p>Printed copy should be disposed of in accordance with any retention schedule via Threshires Ltd confidential waste scheme or shredding facilities.</p> <p>Large accumulations of data should not be downloaded or copied.</p>	
Highly Confidential	<p>Information which is sensitive and has the potential to cause serious damage or distress to individuals or serious damage to Threshires Ltd interests if disclosed inappropriately. Data contains highly sensitive private information about living individuals and it is possible to identify those individuals e.g. Medical</p>	<p>Information must be stored using Threshires Ltd IT facilities. Portable devices must have full disk encryption. Unencrypted removable media (e.g. USB sticks) must not be used. Encrypted removable media are not permitted without undertaking</p>	<p>Access to confidential data must be strictly controlled by the Data Owner who should conduct regular access reviews.</p> <p>Some types of confidential information may be shared with authorised users via Threshires Ltd IT facilities, including remote access, subject to</p>	<p>The method to be used for exchanging confidential information must take account of the nature and volume of the data to be exchanged so that the impact of inappropriate disclosure can be assessed and an appropriate method selected. Approved data exchange methods are available from Digital Services. Confidential data must be encrypted prior to exchange.</p> <p>Exchange must be conducted using Threshires Ltd provided facilities. Duplicate copies of confidential</p>	<p>Electronic equipment holding this information must be disposed of using the Threshires Ltd secure IT waste disposal service and in accordance with any retention schedule. Printed copy should be disposed of in accordance with any retention schedule via the Threshires Ltd confidential waste scheme or shredding</p>

<b>Filename:</b>	Data Handling Policy	<b>Approved by:</b>	Nicola Rudko	<b>Issue Version:</b>	02
<b>Reference:</b>	PO16	<b>Position:</b>	Compliance Manager	<b>Issue Date:</b>	February 2022
<b>Category:</b>	Policies	<b>Signature:</b>		<b>Last Reviewed</b>	February 2022



Class	Description	Storage	Dissemination and access	Exchange and collaboration	Disposal
	records, serious disciplinary matters	evaluation of other options.  Storage on Personally owned (e.g. home) computer is NOT permitted.	Threshires Ltd authentication.  Confidential data must not be extracted from Threshires Ltd IT systems and stored on local IT systems.  If a portable device (e.g. a laptop, tablet or phone) is used to access Threshires Ltd confidential information, the device must be encrypted and require a password or PIN to access	information must be avoided. Where copies are necessary the protective marking must be carried with the data. Where paper copies are required for circulation or sharing, secure delivery methods must be used. Paper and electronic copies must be marked 'Highly Confidential' and the intended recipients clearly indicated. An optional descriptor, to state the reason for confidentiality, may be used.	facilities. Large accumulations of data should not be downloaded .

Signature: 

Date:.....23.01.2022.....

Name: Mr James Lloyd  
Position: Managing Director

<b>Filename:</b>	Data Handling Policy	<b>Approved by:</b>	Nicola Rudko	<b>Issue Version:</b>	02
<b>Reference:</b>	PO16	<b>Position:</b>	Compliance Manager	<b>Issue Date:</b>	February 2022
<b>Category:</b>	Policies	<b>Signature:</b>		<b>Last Reviewed</b>	February 2022