# Acceptable Use of IT Systems Policy

## Thalia Document Ref: THALIA-ACCEPTABLE USE-IT 01

## Contents


2. Policy Statement ..... 2
3. Overview ..... 2
4. Acceptable Use ..... 2
5. Monitoring and Logging ..... 5
6. Policy Information ..... 6
7. Key Terms ..... 6
8. Applicable Policies & Standards ..... 7
9. FAQ ..... 8

# 1. Policy Statement

Acceptable Use of IT Systems - Policy Statement:

This policy is to ensure that all users are aware of and understand their obligations for accessing Thalia Waste Management's IT System, their responsibilities for looking after these systems, and the handling of Information including the potential consequences of breaching security requirements.

**Compliance with this policy is mandatory for all employees, contractors, subcontractors, consultants and suppliers who carry out activities for or on behalf of Thalia Waste Management and in respect of all types of information created for and/or by Thalia Waste Management, irrespective of the nature, media and format of storing or transmitting the information.**

**Key terms used in this policy are described in paragraph 6.**

# 2. Overview

Thalia Waste Management ("Thalia") provides staff with equipment such as laptop computers, tablets and mobile phones to access Thalia's IT System and Thalia's Information in order to perform their roles. Where required, Thalia also makes available IT Systems and Information to personal devices, subject to appropriate security measures being complied with.

It is critical that all those referenced above comply with this policy and the procedures within it to ensure the security of Thalia's IT Systems and Thalia's Information. Under no circumstances should attempts be made to disable or circumnavigate security controls.

# 3. Acceptable Use

All users with access to Thalia's IT System and Information are required to adhere to the following rules:

- All devices issued by Thalia are the property of Thalia and must be used in accordance with this and other Thalia policies and standards which are listed in section 7.
- All Thalia devices including, but not limited to, laptops, mobile phones and peripherals must be returned:
    - when employment ends;
    - if the user is provided an upgrade or replacement device; and
    - in any other circumstance, at Thalia's request.
- You **must not** keep a device if it has been replaced or upgraded; all devices must be returned to IT as soon as is practical when they are no longer being used.
- You **must** protect Thalia devices such as laptops, mobile phones and tablets from the risk of theft, loss or damage. Devices must not be left overnight in cars or unsecured in any office locations.

- You may make use of Thalia IT Systems for limited personal use such as web browsing, accessing social media or online shopping, but users **must not** download any non-work files to the Thalia IT System.
- You **must not** access personal email or cloud storage services from Thalia IT Systems.
- You **must not** forward Thalia business emails or files to a personal email address or to a non-business destination.
- Confidential information, for example, bank details, design documents etc. belonging to Thalia or anybody with whom Thalia has relations (including, but not limited to, employees, contractors, subcontractors, consultants, lenders, equity partners or suppliers of Thalia) should only ever be stored in the approved IT Systems like SAP and SharePoint with the appropriate levels of security.
- You **must** only store confidential information such as client bank details, design documents in the approved IT System such as SAP or SharePoint.
- Users **must not** install any software onto a Thalia device that has not been provided and approved by Group IT.
- Users **must not** interfere with scanning, installation or reboots of software updates or security protections
- Where a user wishes to send an email containing Personal Information or Personally Identifiable Information (PII), the appropriate level of encryption must be applied when transmitting outside the Thalia network. Please contact GroupIT.Security@Thalia.co.uk for advice on how to do this.
- If you need to send an email containing personal data you **must** make sure you have permission to do so and use the correct protection for this information. For details on this please see the Information Classification and Handling policy.
- You **must not** use Thalia IT Systems for the creation, collection, storage, downloading or displaying of any offensive, sexual, obscene, indecent or menacing images, data or material capable of being considered as such.
- You **must not** use Thalia IT Systems for inciting personal unrest, harassment, bullying, defamation or acts which contradict the diversity agenda or for any purpose contrary to Thalia's values or the Thalia Code.
- You **must not** attempt to access any Thalia IT System or information which you do not have permission to access.
- Whilst it may be acceptable for Thalia's Information to be processed or stored at a third party, sufficient arrangements must be put in place to ensure that Thalia is not disadvantaged or impacted if information is lost, stolen, altered or otherwise compromised. Third party processing and storage of Thalia Information must be approved by Thalia Group Legal, Group IT and Group Commercial.
- Confidential information, including personal data and Personally Identifiable Information (relating to, for example, employees, third parties and customers) must not be left visible on

screens or on desks when not in use. Such hard copy documents and all computer media containing such information shall be kept in a secure location when not in use, especially outside working hours. Confidential documents that are no longer needed must be shredded or disposed of in locked paper bins provided for the purpose. Please see the Data Protection and Document Retention Policy for more information.

- Users of a Thalia mobile device **must** ensure that it is protected with a passcode, password or other security authentication method.
- If you use a personal mobile device to access Thalia IT Systems such as Office365 you **must** ensure that it is protected with a passcode, password or other security authentication method.
- If you access Thalia IT Systems such as Office365 from a personal device, you **must not** download or upload files or documents from this device to the Thalia IT System. Thalia provides OneDrive and O365 Apps which will allow you to work securely without requiring a local copy.
- Where a Thalia mobile device, or personal mobile device containing Information (including email), has been lost or stolen, the IT team must be informed immediately and where possible remotely wipe data from the device. You should notify the relevant authorities of a theft and get a crime reference number.
- You should be careful when using any public wireless network as these can be used to steal information. Where public networks are provided such as airports and hotels, you **must** ensure you are connected to the genuine network provided by the venue.
- You **must not** share your login details to any other person under any circumstances. Any account which is being used by someone other than the named user will be disabled.
- Passwords used for Thalia IT Systems should be unique. They should not be written down, stored on a device or online without encryption or other form of obfuscation. Thalia does permit the use of password managers such as LastPass (contact Thalia Group IT for advice).
- You **must not** use the same password for Thalia IT Systems as you use for any personal accounts.
- Portable media such as USB storage devices should not be used for confidential information unless there is written approval from Group IT. If it is used the storage device must be encrypted and the information stored only for the length of time required and deleted immediately when no longer required.
- Users of collaborative or social media shall ensure that they comply with the rules of this policy and other Thalia policies and standards, in particular, HR-StandsEthics-PO-002 “Social Media Policy”. Users of Thalia information are responsible and accountable for the adequate protection of information that they create and use in collaborative and social media.
- Some Thalia IT System users have ‘privileged user accounts’ that have a higher level of access to the Thalia IT System and resources because their job responsibilities require such access. These accounts should only ever be used for the purposes for which they are provided and should never be used for normal work purposes.

- Users should only have local administrator rights if absolutely necessary and should only be active for the time required to perform the required operations.
- You must not contract for any IT service or software on behalf of Thalia without appropriate IT and legal approval in line with Thalia General Approvals Schedule
- You **must** handle any data in accordance with its classification or protective marking as defined by Thalia's Information Classification and Policy or the Government Security Classifications.
- Where Thalia data is not classified it should be treated as confidential and not stored or transferred to non-Thalia IT Systems without the appropriate legal approvals and technical controls such as data encryption and user authentication.
- You must report any incidents of possible misuse or violation of this policy to the IT Service Desk, your line manager, HR business partner or the Whistleblowing helpline. Reported incidents will be considered as confidential.

## 4. Monitoring and Logging

Thalia reserves the right to monitor and audit any and all use of the Thalia IT Systems, whether that use is business or personal.

**This activity logging is required to:**

- Administer and provide reliable information systems and services;
- Prevent or investigate breaches of security, data loss, unauthorised or unacceptable use of systems and services; and
- Prevent and detect breaches of law, regulation and of Thalia policies and standards.

In some circumstances, in support of the requirements above it may be necessary to monitor, review and act on any unacceptable use.

**Therefore, Thalia expressly reserves the right to:**

- Inspect the contents of any information stored on the Thalia IT System;
- Remove any non-Thalia equipment, software, information or data found to be breach of this, or any other Thalia policy;
- Monitor, intercept, review, block or divert any electronic communications;
- Monitor internet use, including sites visited, messaging, web traffic and emails; and
- Access data stored on the Thalia IT System by users no longer in the employment of, or working on behalf of Thalia.

All user activities may be monitored, therefore there shall be no expectation of privacy when using the Thalia IT System. Logs are available only to authorised personnel and kept for no longer than necessary and in line with current data protection regulations. Such records may be shared with

external agencies and authorities where legally required.

## 5. Policy Information

Thalia Group IT will monitor compliance with this policy, and whilst investigating suspected violations may recommend disciplinary action in accordance with company conduct, policies, or applicable laws.

Users should note that consequences may be sanctioned by Thalia and also by the appropriate regulatory entity and may include:

- suspension or termination of access to Thalia's IT Systems;
- disciplinary action, which could ultimately result in termination of employment;
- financial penalties;
- civil or criminal legal sanctions; or
- any combination of the above.

Thalia's Head of Information Security is the owner of this document and is responsible for ensuring that this policy is periodically reviewed. A current version of this document is available to all members of staff on the corporate intranet and should be made available to those without access.

## 6. Key Terms

| Term | Definition |
|---|---|
| User | Any person, whether an employee, contractor, temporary staff or employee of a third party organisation that is accessing Thalia IT Systems. |
| GDPR | General Data Protection Regulation. Mandated EU law that will impact all EU Organisations along with organisations who wish to deal with EU Organisations. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ |
| ISSG | Information Security Steering Group: the information security group mandated to provide overall governance for Thalia's security issues. |

| | |
|---|---|
| Personal Information | Information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion whether recorded or not, about an identifiable individual. |
| PII | Personally Identifiable Information: Personally identifiable information (PII), or sensitive Personal Information (SPI), as used in information security and privacy laws, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. |
| Asset | Term used to describe a physical item of value, such a laptop, desktop or mobile phone |
| Information | Means any information owned by Thalia or for which Thalia is responsible. This will be broad and far ranging. It will include all information relating to the business, affairs, customers, clients, suppliers or market opportunities of Thalia, its clients, its lenders, its employees, its consultants, its contractors, its co-equity partners, its suppliers and others with whom Thalia has a relationship. It includes information relating to the operations, processes, product information, know-how, technical information, designs, trade secrets or software of Thalia and any analysis, computations, findings or secondary data that is derived or generated from such information. |
| Thalia IT System(s) | Means the Thalia IT network and assets on it owned or procured by anyone acting with or on behalf of Thalia (so these would include, for example, Thalia employees, temporary employees, contractors, consultants or visitors). The term includes software systems such as Office 365, Email, SharePoint, PowerBI, Shared Drives, Work manager and SAP. |

## 7. Applicable Policies & Standards

- Thalia ISMS PO-01 Security Management Policy
- Thalia ISMS PO-03 Information Classification & handling policy
- Thalia Data Protection and Document Retention Policy
- Social media policy

- BYOD policy (to be available shortly)

## 8. FAQ

Q. Can I leave my Thalia laptop/phone in the office overnight?
A. Yes but it must be locked away in a drawer or locker, or secured to the desk with a Kensington lock and the key taken home with you.

Q. If my car is locked and alarmed is that not a safe place to store my Thalia laptop?
A. No, thieves will frequently break into cars to steal valuables, you must not leave Thalia equipment unattended in a car for any length of time.

Q. I'm going on holiday and may need to work, should I take my Thalia laptop or can I work from a personal device?
A. You should try to avoid working on holiday wherever possible, but if it is unavoidable you can use the Thalia O365 services from a personal device to access all Microsoft office services, including your documents in OneDrive to avoid having to take your Thalia laptop away with you. Depending on your destination you may need to contact Thalia ahead of time to advise you will need to access from a country so we are able to make sure your connections are not blocked.

Q. A colleague's machine is broken, can I let them use mine to work on?
A. You can allow a colleague to use your machine but they should always use their own logon to access it. You must not let another person use a machine with your logon credentials.

Q. Can I use my personal Mac or PC for work?
A. With Office365 you can use a personal device to access Thalia systems, however you must never upload from or download to this device, all work must be done within the O365 environment and the OneDrive location

Q. Can I use my personal email for work?
A. You must not use personal email accounts for any business purposes or attempt to access personal email accounts from a Thalia device.

Q. Can I use my personal phone for work?
A. Yes, you can use the O365 mobile applications for work on a personal phone. You must not jailbreak or root the device as this creates a significant security risk.

Q. I need to scan a passport for HR, how should I store this?
A. You should have a SharePoint site only you have permission for, upload the scan to there and select to share to the HR email you are required to. As soon as they have confirmed this has been completed, you should delete the file.

Q. I have a personal OneDrive, can I use that instead of the Thalia one?
A. No, you cannot use any personal cloud service for Thalia business.

Q. How long should I keep old emails and documents?
A. You should only keep these as long as you need. If there is a contractual or legal obligation to store them, you should put them safely in a SharePoint site. We recommend regularly reviewing your documents and emails and deleting all old ones you no longer need.

Q. How should I send documents?
A. The safest way is to share a link from OneDrive or SharePoint rather than sending as an attachment. If for some reason you cannot do this, you can attach the file, but if it contains confidential information you should password protect it or use the O365 message encryption.

Q. For my role I need to run long processes that may be impacted by the screen lockout, can I disable it?
A. No, you should not attempt to disable any security control, if you have a specific business need raise a ticket with IT who will find a suitable solution.

Q. I clicked a link in an email and entered my username and password, I think it may not have been genuine what should I do?
A. you should immediately report it to IT by calling 01276 455 455

Q. If I have a personal license for software can I install it on my Thalia device?
A. No, you cannot install any personal or unapproved software on a Thalia device. All software must be through the Software Centre or Non Standard Software request process. Please note most personal licenses including free software are not applicable for business use and using these on a corporate device could breach the terms of the license.

Q. Can I store data on a USB stick or hard drive?
A. You should not store any business data on an external device unless you have been given written permission to do so, and if you do the drive must be encrypted with Bitlocker, and the data removed as soon as it is no longer needed. Permission should be sought from Group IT.

## Revision Status

| Revision | Date | Amendment | Content Owner | Mandated By |
|---|---|---|---|---|
| 1.0 | Nov 22 | Issued for use | Edward Jones | Paco Hevia |