# 4Thought Marketing Security Policies

**Table of Contents**

# Your Trust is Our Mission

At 4Thought Marketing, trust is the foundation of our relationship with you. We know that security and compliance are crucial to your success, and we take them seriously. We design our solutions with your protection in mind, meeting—and often surpassing—industry standards to ensure your data is safe. We stay ahead of evolving regulations to keep your data compliant and secure. We work hard to earn your trust by always acting in your best interests, focused on going beyond your expectations and safeguarding your business.

# Network Security

## Egnyte

Egnyte houses all file servers in industry-leading Tier II, SSAE 16-compliant colocation facilities with 24-hour manned security, biometric access control, and video surveillance. All servers reside in private cages that require physical keys to open. The servers are never equipped with USB ports or CD/DVD drives, ensuring that data cannot be copied or removed from the devices. All data centers hosting these servers are audited annually for potential risks and limitations. More information on Egnyte Security can be found at the bottom of this page in the "Vendor and Third Party Security Information" section.

## Data At Rest

4Thought Marketing stores all customer and internal data on Egnyte, which encrypts data at rest. All files stored on Egnyte RAID6 servers are automatically encrypted using AES 256-bit encryption. If someone gained access to data on the servers, the data would be impossible to read. The encryption key is stored in a secure key vault, a separate database decoupled from the raw storage layer. As a final precaution, administrators can replicate their data to a secondary Tier II, SSAE 16 compliant facility, where it is again replicated on RAID6 servers.

While 4Thought Marketing will accept Customer Secure classified files (data files with contacts) from customers via email (as a convenience and due to the customer's security choice), once received, Customer Secure files are never transmitted internally or back to our customers using email. All file transfers of data records occur via the secure Egnyte storage system.

## Data During Transmission

When communicating data to or from the Egnyte storage system, 4Thought Marketing utilizes transmission practices utilized by the most secure institutions worldwide by using 256-bit AES encryption to encode data during transmission. 256-bit AES encryption is the strictest standard the US government applies for TOP SECRET documentation and ensures that even if company data were intercepted, it would be impossible to decipher.

While 4Thought Marketing accepts Customer Secure classified files (e.g., data files containing sensitive contact information) from customers via email for convenience and based on the customer's security preferences, we ensure these files are never transmitted internally or back to our customers using email. All subsequent file transfers of these data records occur via the secure Egnyte storage system.

## AWS

AWS has an extensive security setup. You can read about this here – https://aws.amazon.com/security/. In addition to the standard security features offered by AWS, 4Thought Marketing also uses Amazon GuardDuty as our intrusion prevention and detection system. This covers all traffic to our AWS servers, which house our cloud apps, 4Segments, 4Bridge, and other applications.

## Offices

As of March 2020, coinciding with the onset of COVID-19, 4Thought Marketing transitioned from a traditional office model to a fully remote operational structure, closing our offices in Silicon Valley, Costa Rica, and India and discontinuing all corporate networks. This shift was adapted to ensure the safety and well-being of our team amidst the global pandemic. We have no plans to revert to a physical office model or re-establish corporate networks, as the remote work model has been embraced and integrated seamlessly into our business operations.

### DDOS Attacks (Denial Of Service)

4Thought addresses DDoS attacks by utilizing AWS Cloudfront, AWS WAF, and AWS Shield security tools, combined with AWS Best Practices for DDoS Resiliency. AWS WAF is a web application firewall that, deployed on CloudFront, helps protect against DDoS attacks by providing control over which traffic to allow or block by defining security rules. AWS Shield protects our applications from common, frequently occurring network and transport layer DDoS attacks. AWS shield allows attack traffic to be geographically isolated and absorbed using the capacity in edge locations close to the source. Additionally, if needed, we can configure geographical restrictions to help block attacks originating from specific countries.

## Physical Security

### Offices and Printers

As of March 2020, coinciding with the onset of COVID-19, 4Thought Marketing transitioned from a traditional office model to a fully remote operational structure, closing our offices in Silicon Valley, Costa Rica, and India and discontinuing all corporate networks. This shift was adapted to ensure the safety and well-being of our team amidst the global pandemic. We have no plans to revert to a physical office model or re-establish corporate networks, as the remote work model has been embraced and integrated seamlessly into our business operations.

### Mobile Data And Device Controls

345 million mobile devices are lost or stolen each year. For this reason, no customer data is stored on any 4Thought Marketing team member’s computers, including mobile devices. All employees without a

private locking office must abide by 4Thought Marketing’s Clean Desk Policy, which requires that all customer information be put away before leaving the desk for more than 5 minutes.

### Removable Media Controls

Recordable CDs, DVDs, Removable Storage devices, and USB sticks are not generally permitted at 4Thought Marketing. An Executive Team or Security Officer member can make temporary (defined limited time) exceptions. In such cases, a request will be made before the use of a recordable CD, DVD, Removable Storage device, or USB stick, and the risk will be assessed on a case-by-case basis. If a recordable CD, DVD, Removable Storage device, or USB stick is used, it will be kept securely until the Customer’s Secure Data can be stored as Data at Rest once again. Then, Customer Secure Data will be deleted from the recordable CD, DVD, Removable Storage device, and USB stick immediately after doing so.

### Equipment Disposal

For absolute surety when disposing of devices, all device data is wiped three times, once with a zero, once with a 1, and once with a random character as per DoD 5220.22-M. This is a secondary measure to eliminate temporary files and RAM storage because 4Thought Marketing does not store customer data on laptops or other devices; thus, equipment that is disposed of should theoretically hold no confidential data. This standard eliminates all software recovery possibilities except the most advanced hardware recovery methods.

## Access Control Policies

4Thought Marketing’s Access Control Policies are intended to:

- Enable 4Thought Marketing Team Members and contractors to access the systems necessary for their work

- Reduce business risk and safeguard security policy
- Enable effective tracing of bad actors
- Take preventive measures against bad actors
- Reduce financial losses and improve productivity

Our Access Control Policies include a comprehensive system for managing and auditing access rights. This involves regular reviews and updates to ensure access is granted based on current roles and responsibilities, with immediate adjustments made in case of role changes or employment termination.

## Access Control – Authorization

After hiring or contracting new team members, access to required systems will be granted under this policy. All IDs or User Names assigned for all systems shall abide by corporate naming conventions. Following best practices, naming conventions are considered security confidential to avoid giving bad actors unnecessary security insights. In general, authorization granted should be the minimum required to accomplish the tasks necessary for an individual. The definition of "tasks necessary" should include all probable tasks an individual will likely encounter over one calendar year. All system lockout times (such as Windows environments) should automatically lock out after 15 minutes of non-use. To the degree permissible by each system, all systems shall be set up to require passwords following the password control policy established herein.

## Access Control – Management

All system access shall be immediately adjusted upon any change in responsibilities. For company initiated terminations, all systems' access must be terminated prior to employee notification. For employee-initiated terminations, all systems must be shut down as soon as possible, but under no circumstances longer than 4 hours after notification. Completion of process is reported to the CEO.

## Access Control – Separation of Duty

To the degree permissible by each system:

- Each system shall have a "top-level" login/password reserved solely and exclusively for assigning user rights and access. Access to this password shall be reserved for the Security Officer, CEO, CTO, and assigned technical resource.

- Accordingly, individuals cannot assign user-level access when possible.

- When available, maximum logging for the top-level user password will always be turned on.

## Access Control Auditing – Annual Review

Annually (coincident with Confidentiality Agreement renewals), all user access rights and lockout times for all 4Thought Marketing systems shall be reviewed by either the CTO or Head of IT, as assigned by the Security Officer. The Security Officer will update the security log with:

1. The date, time of review, and the person's name and title.

2. Any access control violations discovered (left-over user or contractor logins for inactive team members).

3. Remedial Actions taken, including:
    1. Review of responsibility and points of failure for access control violations

    2. Managerial actions taken from both a policy and personnel perspective to avoid repetition.

# Password Policies

4Thought Marketing passwords should meet or exceed the following guidelines to the greatest degree the system being accessed permits these policies

## Password Creation

Strong passwords have the following characteristics:

- Contain at least eight alphanumeric characters.

- Contain both upper and lower case letters.

- Contain at least one number (for example, 0-9).

- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:”;'<>?,/).

Poor or weak passwords have the following characteristics:

- Contain less than eight characters.

- Can be found in a dictionary, including a foreign language, or exist in a language slang, dialect, or jargon.

- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.

- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.

- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.

- Contain common words spelled backward, preceded, or followed by a number (for example, terces, secret1, or 1secret).

- Are some version of “Welcome123” “Password123” “Changeme123”

## Password Protection – External

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is to create a password based on a song title, affirmation, or phrase. For example, the phrase, “This May Be One Way To Remember” could become the password TmB1w2R! or another variation. (NOTE: Do not use either of these examples as passwords!)

- Users must not use the same password for 4Thought Marketing accounts as for other non-company accounts (for example, personal email account, bank account, benefits, and so on).

- Where possible, users must not use the same password for various 4Thought Marketing access needs.

- User accounts that have administration or system-level privileges granted must have a unique password from all other accounts held by that user.

## Password protection – internal

- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential 4Thought Marketing information.

- Passwords must not be inserted into email or Skype messages.

- Do not reveal a password on questionnaires or security forms.

- Do not hint at the format of a password (for example, “my family name”).

- Do not share 4Thought Marketing passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.

- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

- Do not use the “Remember Password” feature of applications (for example, web browsers) except on your personal computer that you lock when not using.

- Any user suspecting that his/her password may have been compromised must report the incident and change all related passwords.

## Password Change

- All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.

- All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.

- Password cracking or guessing may be performed periodically or randomly by the Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user must change it to comply with the Password Construction Guidelines.

## Password Protection

- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential 4Thought Marketing information.
- Passwords must not be inserted into email or Skype messages.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (for example, “my family name”).
- Do not share 4Thought Marketing passwords with anyone, including administrative assistants, secretaries, managers, co-workers on vacation, and family members.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- Do not use the “Remember Password” feature of applications (for example, web browsers) except on your personal computer that you lock when not using.
- Any user suspecting that his/her password may have been compromised must report the incident and change all related passwords.

### Passphrases

Passphrases generally are used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key known by all and the private key known only to the user. The user cannot gain access without the passphrase to unlock the private key. Passphrases are not the same as passwords. A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!). All of the rules above that apply to passwords apply to passphrases.

## Application Development

### Security by Design Policy

We have established the following security policy for our software development team. This policy outlines our commitment to security and informs our clients and users of the principles guiding our development process.

1. **Secure-by-Design Principles**: Embrace the secure-by-design approach, where security is not an afterthought but a fundamental aspect of the software development process. This includes leveraging secure coding practices, utilizing security testing tools, and considering security in design decisions.

2. **Asset Clarification and Classification**: Prioritize the identification and classification of data our applications handle. Implement security controls commensurate with the data’s sensitivity and value.

3. **Proactive Threat Understanding**: Recognize and design against threats posed by malicious actors, such as cybercriminals and disgruntled insiders. Utilize threat modeling to anticipate and mitigate potential security issues.

4. **Adherence to Information Security Pillars**: Ensure all applications uphold confidentiality, integrity, and availability. This involves granting data access only to authorized users, safeguarding data integrity, and maintaining data and system availability.

5. **Comprehensive Security Architecture**: Develop a robust security architecture that addresses various risks. This includes considering each application feature and evaluating its security implications and potential vulnerabilities. Development, Staging, Production, and Demonstration environments are segregated, reducing risks of security misconfiguration and sensitive data exposure.

6. **Integrated Development and Security Teams**: Foster a collaborative environment where the development and security teams work in unison throughout the software development lifecycle. Security considerations should be integrated from the outset and at every stage of development

This policy is informed by best practices and guidelines from leading security organizations such as the Cybersecurity and Infrastructure Security Agency (CISA) and The Open Web Application Security Project (OWASP).

## Security Precautions

Application developers must ensure their programs contain these security precautions:

- Applications must support authentication of individual users, not groups.

- Applications must not store passwords in clear text or any easily reversible form.

- Applications must not transmit passwords in clear text over the network.

- Applications must provide some sort of role management, such that one user can take over the functions of another without having to know the other's password.

- Shared, default, and other non-individual account types are prohibited at the design level of 4Comply, 4Segments, 4Bridge, and other applications and systems at 4Thought Marketing

## Security Virtual Tour (VTour) Policy

1. **Purpose and scope:** The Security Virtual Tour (hearafter VTour) is designed to provide an overview of 4Thought Marketing's security posture without compromising the integrity and security of our systems. This document outlines the policy regarding the disclosure of security-related information, the conduct of VTours, and the process for requesting a VTour.

2. **Non-disclosure of sensitive information:** To protect our systems against unauthorized access, 4Thought Marketing strictly controls the disclosure of information related to our security rules, processes, architectural components, and vendor tools. Details beyond those publicly available on our website and its linked documents will be kept from being shared externally.

3. **Eligibility and access to VTour:** VTours are available to personnel who have undergone a vetting process by 4Thought Marketing. Eligible participants are required to adhere to the following conditions during a VTour:
    - No video recording, screen capturing, digital capturing, or taking specific written notes on the details presented.

- General observations regarding the existence and configuration status of the security measures discussed are permitted and encouraged.

4. **Requesting a VTour:** Interested parties wishing to participate in a VTour must submit the following information to security @ 4ThoughtMarketing .com:
    - Legal company name
    - Full names of the individuals attending (first, middle, and last)
    - Email addresses of the attendees (for scheduling purposes)
    - City, state, and country of residence of the attendees (for identity verification)
    - A list of specific items of interest to be included in the VTour

5. **Scheduling:** After receiving a request for a VTour, 4Thought Marketing will arrange the session as soon as possible, coordinating with the requesting party to finalize the date and time.

6. **Compliance:** Participation in a VTour indicates agreement to comply with the terms outlined above. 4Thought Marketing reserves the right to deny access to the VTour to any individual or entity that fails to meet our security and vetting standards.

## Patch Management

- We apply patches that are:
  - Critical within 48 hours (or faster)
  - Medium within 1 Week
  - Low/Very Low within 1 Month
- Virus Scan updates/patches are applied continuously by ESet.
- We currently utilize no open source software in our security stack

## Penetration & Network Viability Testing

4Thought Marketing conducts Network Viability Testing and Penetration Testing (pen testing) on all of its apps, servers, and websites using a combination of two tools for pen testing:

- Pentest-tools.com
- Detectify

Authenticated and Unauthenticated Tests We perform scans and penetration tests, both while unauthenticated emulating what a complete outside bad actor might accomplish, and also while authenticated confirming that a bad actor with access cannot abuse our systems. We resolve the resulting errors that are:

- Critical within 48 hours
- Medium within 1 Week
- Low/Very Low within 1 Month

These tests cover the OWASP Top 10 (as found at www.owasp.org) along with over 930 additional Pentests and Network Viability Tests. The OWASP Top 10 are designed to identify and target the most commonly exploited categories of application and website flaws, including SQL, LDAP, XPATH, and NoSQL injections, Cross-Site Scripting flaws, broken session management, remote code and command execution, malware, and more.

The testing is completed monthly by our technical team, and the results are recorded by 4Thought Marketing's security officer along with any repairs undertaken. These tests are specifically designed to detect issues with the following:

- Injection
- Broken Authentication
- Sensitive Data Exposure

- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Utilizing Components with Known Vulnerabilities
- Insufficient Logging & Monitoring

A copy of the latest NVT and Pen Test results can be requested from 4Thought Marketing's Security Officer.

## Application Development And Security

For more details about our cloud app development security and how we handle PII, please review the 4Thought Marketing Cloud App Security Document.

# Artificial Intelligence (AI) Policy

## Overview

Using generative AI services like OpenAI's ChatGPT and Google's Bard has become increasingly popular. At 4Thought Marketing, we recognize the importance of outlining the proper use of such tools. While we are committed to adopting new technologies to aid our mission and support our customers, we also understand the risks and limitations of generative AI chatbots. Our primary objective is to protect our employees, clients, suppliers, customers, and the company from potential harm.

## Eligibility

This policy applies to all 4Thought Marketing team members and all work they perform, whether on or off company premises.

## Strictly Prohibited Use

The industry is still determining the ability of AI to keep confidential information private. What you give generative AI, you can't get back. The AI can and may provide it to anyone and everyone without asking or even notifying you, 4Thought Marketing, or our customers. So, as a rule of thumb, we do not give generative AI *anything* confidential.

- Team members may not use AI for resume screening or other purposes related to new employee review and consideration.

- No customer data, customer emails, or any other non-public customer information of any type may be used with AI, including:

  - Customer confidential information
  - Partner confidential information (Oracle, Adobe, PathFactory, Microsoft, etc.)
  - 4Thought Marketing confidential information

## Limited Use

Generative AI is known to “hallucinate” inaccurate facts when pressed, plagiarize, and repeat and reflect inappropriate human biases.

Before publishing or otherwise publicly using any AI-created content, all team members will:

- Fact Check all AI-provided content
- When intended for publication, verify no plagiarized content has been utilized
- Review all content for discriminatory or biased statements

## Internal and Customer AI Notification

All AI-generated content must be clearly labeled as “AI Created” for transparency during internal and customer reviews.

When a Team Member creates an article or email that mainly consists of content generated by AI, it’s essential that all team members or customers who review that information can easily recognize it. In such cases, the words “AI Created” should be placed near the content. However, if the content is not primarily AI-generated, such as seed ideas, minor rewrites, or grammar reviews, this notification is not necessary. It’s up to the Team Member’s discretion to determine whether the content is predominantly AI-generated. Before publishing or submitting the content for Quality Assurance or Second Eyes Review, the “AI Created” notification should be removed.

## Ethical Use

Team members must use generative AI chatbots in accordance with 4Thought Marketing’s conduct and anti-discrimination policies. These technologies must not be used to create inappropriate, discriminatory, or otherwise harmful content to others or the company. Such use will result in disciplinary action, up to and including termination.

## Monitoring

4Thought Marketing’s Computer Use Policy and relevant monitoring policies still apply when using generative AI chatbots with company equipment.

## Legal Review

Annually, 4Thought Marketing will:

- Perform an AI legal review, ensuring that we abide by the new laws and regulations as they come into effect.

- Review and update these policies

- Remind all Team Members of these policies

# Governance, Risk, and Compliance

## SOC 2 Compliance

### SOC 2 Certification

As of June 2024, 4Thought Marketing is actively pursuing SOC 2 Type II certification to further solidify our commitment to security, privacy, and trust. SOC 2 is a rigorous auditing standard developed by the American Institute of Certified Public Accountants (AICPA) that evaluates organizations on the five Trust Services Criteria: security, availability, processing integrity, confidentiality, and privacy.

We have engaged with a reputable SOC 2 auditor to conduct a comprehensive examination of our systems and controls. This process involves a detailed assessment of our internal policies, procedures, and technological safeguards to ensure they meet the stringent requirements set forth by the SOC 2 framework. By undergoing this thorough audit, we aim to provide our clients with verified assurance that their data is handled with the utmost care and protected by industry-leading security practices.

### SOC 2 Transparency and Client Collaboration

We believe in maintaining open and transparent communication with our clients throughout this certification journey. We understand that you may have questions regarding our progress, the specifics of the controls we are implementing, or the estimated timeline for completion. We are more than happy to discuss these details and provide any additional information you may require. Your trust is invaluable to us, and we are committed to ensuring you feel confident in our services.

## Background Checks

Effective 2016, 4Thought Marketing conducts background checks on all operations personnel. Background checks are done in compliance with industry standards and by certified vendors. Details can be found here – 4Thought-Marketing-Employee-Security-Checks-20190222v1.1cm.pdf.

## EU-US Privacy Shield

In response to the evolving international data protection regulations, including the invalidation of the EU-US Privacy Shield, 4Thought Marketing has adapted its compliance strategies to ensure secure and lawful data transfer across borders. Recognizing the importance of maintaining the highest data privacy standards, we rely on Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) as our primary mechanisms for international data transfers. These measures align with GDPR and similar laws in other countries and demonstrate our commitment to upholding robust data protection practices, ensuring that our client's data is handled with the utmost care and security, regardless of geographic boundaries.

## Back-Up Procedures

In the unusual case of one of our critical data sources becoming corrupted or an individual accidentally deleting something, we have backup options for the essential data contained in these platforms. The following shows how our key data sources are backed up.

### Egnyte

Egnyte is our central file management system for our customer and company information. In the event of a Crypto-Ransomware attack, the versioning protocol in Egnyte recovery options can be used to retrieve non-corrupted data. More information on this can be read about here – https://helpdesk.egnyte.com/hc/en-us/articles/4417226750605-Ransomware-Recovery.

In the event of folder changes or accidental deletion, identical file versions can be used to retrieve data. More on that here – https://helpdesk.egnyte.com/hc/en-us/articles/360024950972-File-Versions.

Data is kept for retrieval for 3 versions, this can be set for up to 999 versions if required.

### Xp Dev

XP Dev is where we keep the source code for all applications we create. XP Dev is a secure environment used by developers around the world. If any data is lost or we need to revert the code to a previous version because of a malicious act, XP Dev backs up the code, which can be retrieved. More on this here – https://xp-dev.com/features/backups.html. Any deleted repositories will be saved for 30 days. Daily backups keep data available for one day.

### OneNote

OneNote stores notes and documents related to our customer interactions, as well as our internal processes. It, too, has a versioning setup that will allow us to revert any corrupted data to its pre-corrupted state and undo changes or deletion of data if required. More about this here – https://support.office.com/en-us/articles/enable-and-configure-versioning-for-a-list-or-library-1555d642-23ee-446a-990a-bcab618c7a37. These versions can be set to up to the last 50,000 versions of the page where data is stored.

### Email

Our email is backed up monthly as a part of our regular monthly security processes. We use CloudAlly for this backup, so we can always retrieve our emails if we have a Crypto-Ransomware attack, or important email(s), or an entire mailbox is accidentally deleted. More on CloudAlly here – https://www.cloudally.com/office-365-backup/. CloudAlly will keep all backed-up data for the entire time the subscription is active.

### Website

4Thought Marketing's website has an automated daily backup procedure, and these backups are stored for up to 30 days. No data is kept outside of these four key sources at 4Thought Marketing. Our Clean Device policy dictates that all documents that are customer or company secure are stored in Egnyte or OneNote. No code or emails are stored locally on any device.

## Email Policy

- All use of email must be consistent with 4Thought Marketing policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

- 4Thought Marketing email account should be used primarily for 4Thought Marketing business-related purposes; personal communication is permitted on a limited basis, but non-work related email shall be saved in a separate folder from work related email.

- Non-4Thought Marketing related commercial uses are prohibited.

- Sending or forwarding chain letters, or humor or joke emails from a 4Thought Marketing email account is prohibited.

- The 4Thought Marketing email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

- Team Members who receive any emails with this content from any 4Thought Marketing Team Member should report the matter to their manager immediately.

- All 4Thought Marketing, Customer or Partner data contained within an email message or an attachment must abide by our Data Protection Policy.

- Users are prohibited from automatically forwarding 4Thought Marketing email to a third party email system. Individual messages which are forwarded by the user must not contain 4Thought Marketing, Customer or Partner confidential information.

- 4Thought Marketing employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.

- 4Thought Marketing may monitor messages without prior notice. 4Thought Marketing is not obliged to monitor email messages.

- Users are prohibited from using third-party email systems and storage servers such as Google, Gmail, Yahoo, and Hotmail etc. to conduct 4Thought Marketing business or to store or retain email on behalf of 4Thought Marketing. Such communications and transactions should be conducted through the 4Thought Marketing approved email system.

- Users are prohibited from using third-party email systems and storage servers such as Google, Gmail, Yahoo, and Hotmail etc. to create or memorialize any binding transactions on behalf of 4Thought Marketing. Such transactions should be conducted through proper channels using 4Thought Marketing approved legal documents, Echosign, etc.

- Note that sending of data classified as ‘Customer Secure’ via email is strictly forbidden (see Data Categorization Policy).

- All devices run real time email scanning software. As per best practices the specific brand and configuration of email scanning software is considered security confidential.

## Risk Analysis And Mitigation

- 4Thought Marketing follows the NIST Guide for Conducting Risk Assessments as our model for Risk Analysis.

- 4Thought Marketing annually evaluates our Risk utilizing this guide, the results of which are considered confidential and for internal use/improvement only to not reveal to potential adversaries the areas that we evaluate as vulnerable vs strong.

- 4Thought Marketing is aware of the legal changes occurring regarding Privacy Shield and will adapt to and adopt new standards & regulations as they emerge.

## Policy Compliance & Measurement

The Security Officer will verify and measure compliance with all policies through various methods, including but not limited to, one-on-one conversations, conversations with departmental managers, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to policy owners.

### Security Training

4Thought Marketing is committed to regular security training for all employees. This includes annual cybersecurity awareness training and ongoing updates on security best practices to ensure our team is equipped to recognize and mitigate potential security threats. All new employees must complete security training as part of their initial onboarding. We also routinely perform practical phishing email tests for all employees and require additional training for test failures.

### Annual Policy & Confidentiality Confirmation

All 4Thought Marketing team members (both full-time contractors and employees) are required upon hire and annually (January 1st) to Echosign that they have reviewed and agreed to abide by these policies and to affirm/reaffirm a confidentiality agreement similar to the following. The Security Officer is responsible for confirming, logging, and storing all team members completing document signatures.

### Security Checks

All personnel are required to perform monthly security checks. These checks include updating antivirus and malware scans, verifying restore points, ensuring browser monitoring is active, among other tasks. The results are submitted to the security office every month.

## Data Categorization Policy

To ensure proper security assignment, all data held by 4Thought Marketing (whether temporary or permanent) is classified into one of six types:

1. Executive

2. Managerial

3. Internal 4TM

4. Customer Shared

5. Customer Secure Public

## Executive

**Policy:** Intended for the executives/partners of 4Thought Marketing only.

E**xample:** Board Information, Stock Information, Legal Issues

**Description:** Data should be classified as Executive when addressing confidential corporate issues and concerns best limited to the Executive Team.

## Managerial

**Policy:** Intended for the Management of 4Thought Marketing.

**Example:** Internal reports, processes, and policies under development, etc.

**Description:** Data should be classified as Managerial when it is appropriate only for Managers' or Executives' review.

## Internal 4TM

**Policy:** Available to all 4Thought Marketing personnel

**Example:** Policies, procedures, customer working papers.

**Description:** Data should be classified as Internal 4TM when it does not fall into any of the other classifications list herein.

## Customer Shared

**Policy:** Confidential. Stored in dedicated customer space accessible only to internal 4Thought Marketing team members and customer personnel via login and encrypted access. Destroyed after customer relationship is terminated. May be sent and received via normal email. May be sent to any known customer personnel.

**Example:** Customer processes and policies, project work papers.

**Description:** Documents should be classified as Customer Shared when there is a reasonable expectation that future access to the documents will be of value. Processes, policies, and project deliverables (excluding record based data – see below) are good examples of Customer Shared documents.

### Customer Secure

**Policy:** Stored securely as data at rest. Stored temporarily and as highly confidential. Destroyed routinely after project launch and project support is complete. May only be transmitted internally, or to the customer, via secure encrypted path (Egnyte). May only be distributed to customer personnel associated with the project in question.

**Example:** Customer Data such as Contacts, Accounts, Digital Body Language, Opps, Sales Notes, Passwords, etc.

**Description:** Any record based data received from a customer, or password to any system that contains record based data, should be classified as Customer Secure, unless written confirmation from the customer indicates otherwise.

### Public

**Policy:** Intended for public distribution via website, trade shows, sales reps, etc.

**Example:** Data sheets, White Papers, Website Information, etc.

**Description:** Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would results in little or no risk to 4Thought Marketing or its partners and customers. While little or no controls are required to protect the confidentiality of Public data, a level of control is required to prevent unauthorized modification or destruction of Public data.

## Change Management Policy

## Purpose

The purpose of the Change Management Policy is to ensure that a standard set of minimum requirements are established for changes and the tracking thereof, that are made to both production systems, supporting infrastructure, and other internal systems across the organization. Development, Development Staging, and Demo Systems are excluded from this policy. These requirements are meant to provide a level of consistency and to establish the rules for the creation, evaluation, documentation, implementation, and tracking of how changes are managed from the initial change request through to production deployment. These requirements have been established based on a subset of NIST SP 800-53 standards

## Audience

This policy applies to any individual, entity, or process that creates, evaluates, and/or implements changes to any 4Thought Marketing Information Resource, excluding development, development staging, and demo systems.

## Policy

- All Adopted Changes must be documented in the 4Thought Marketing “Infrastructure” Onenote along with related policies including those for maintenance, modification, backup, training, etc.

- Changes to both the physical and logical production environment must be documented and classified according to their:
    1. Importance

    2. Urgency

3. Impact

4. Complexity

- Change documentation must include, at a minimum:
   1. Date of submission and date of change
   2. Owner and custodian contact information
   3. Nature of the change
   4. Change requestor
   5. Change classification(s)
   6. Roll-back plan
   7. Change approver
   8. Change implementer
   9. An indication of success or failure

- All changes must consider all security policies found at 4ThoughtMarketing.com/Trust including but not limited to:
    - 4Thought Marketing Risk policies which can be found under the Risk Mitigation section
    - 4Thought Marketing third party vendor policies which can be found under the 3rd party vendor section

- Changes with a significant potential impact to 4Thought Marketing **Information Resources** must be scheduled.

- **Information Resource owners** must be notified and approve changes that affect the systems they are responsible for.

- Authorized change windows must be established for changes with a high potential impact.

- All changes must follow 4TM standard “Second Eyes” Testing processes.

- Changes with a significant potential (C.) Impact and/or significant (D.)Complexity must have usability, security, and roll back plans included in the change documentation.

- Change control documentation must be maintained in accordance with data retention policies

- Changes made to 4Thought Marketing customer environments and/or applications must be communicated to customers, in accordance with governing agreements and/or contracts, and policies published online referenced at https://4thoughtmarketing.com/legal/

- All changes must be approved twice by the Information Resource Owner, CTO, and Security Officer, first when the change is proposed, and second after completing second eyes testing prior to deployment.

- All team members are empowered to make Emergency changes (i.e. break/fix, incident response, etc.) which may be implemented immediately with the change control process and associated documentation completed retroactively.

- All documented changes must be reviewed to ensure successful implementation and to make sure compliance is maintained with developed baselines.

### Waivers

Any Waivers from these policy provisions may be sought from the CEO, and must be documented.

### Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and if relevant, related civil or criminal penalties. Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

## Download Policy

Downloading drivers and executables is only permitted from authorized vendors. Please do the following before hitting that “Download now” button:

1. Verify that the vendor the software in question is authorized.

2. Before downloading from an authorized source, confirm that it’s truly the vendor’s website by checking that the URL is from the main and exact URL of the vendor (for example Microsoft.com, Adobe.com, Oracle.com, or the other vendors we work with). Is it really from the company is it supposed to be from – if not, STOP.

3. If the source looks at all questionable, check with the Security Officer, before you download.

4. Always download new or unfamiliar programs first in the Sandboxie sandboxed environment and run a full ESET viral scan before you move it in your main desktop/files environment.

In general, we should not need to download apps too often. What we download should be updated or be associated with programs we use regularly. On the odd occasion where we need something special, please follow the above process carefully.

## Incident Response Plan

The public version of the incident response plan for 4Thought Marketing can be found here –Incident Response Plan. This plan is reviewed, and critical areas are tested annually

### Security Information And Event Management (SIEM)

4Thought Marketing utilizes AWS Cloud Trail for SIEM. AWS CloudTrail service enables governance, compliance, operational auditing, and risk auditing of AWS accounts. With CloudTrail, you can log, continuously monitor and retain account activity related to actions across AWS services. CloudTrail provides the event history of your AWS account activity, including actions taken through the AWS

Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. SIEM logs are required to be maintained a minimum of 12 months. More at AWS Security Incident Response Guide

## Security Incident Reporting Policy & Procedures

**1.0 Introduction** This policy aims to ensure staff within the organization can quickly identify, monitor, and rectify any weaknesses in its security regime. Each security incident presents unique circumstances requiring case-by-case examination by the Security Team.

**2.0 Policy Statement** It is essential that individuals understand how to report a security incident. Security incidents should be reported quickly through the appropriate channel so they can be dealt with swiftly, consistently, and professionally.

**3.0 Scope** All information security incidents, which include physical, personnel, and information assurance, are within scope.

**4.0 Definition of a Security Incident** A Security Incident is defined as ‘noncompliance with security policies and procedures, or any fact or event which you think could affect the organization’s personnel, physical and information security.’

**5.0 Roles and Responsibilities**

**5.1 Security** The Security Officer implements this policy across the organization.

**5.2 Partners and ETeam** Partners and ETeam are responsible for:

- implementing this policy on behalf of the Security Officer by ensuring their staff are fully aware of this policy and the operating procedures

- encouraging a ‘responsible’ culture which encourages staff to report all types of incidents

**5.3 Security Incident Team (SIT)** The Security Incident Team (SIT) is a fluid structure formed on an incident by incident. The team will consist of two or more of the following:

- Security Officer

- A Minimum of One Partner

- Head of the appropriate security area (for example, Website, PM for Customer, Physical Security/Operations, HR (Personnel Security))

- Communications and Media (optional if no customer reporting is required)

The SIT is responsible for:

- assessing the reported incident and contacting the person who has logged the call to find out more details before deciding on the appropriate action (if necessary)

- determining who will lead the investigation, if one is required

- examining all of the individual resolution plans submitted by the various representatives involved with remedying the incident and drawing these plans together into a single action plan to ensure that all actions are taken at the appropriate time

- passing the call to the appropriate area for action or closure if an investigation is not needed or it is not considered a security incident

- recording all actions on a timeline record to outline progress made against the action plan and creating a lessons learned paper for implementation

**5.4 Managers** Managers are responsible for:

- ensuring their staff understand and comply with the organization's policies and procedures

- instigating any initial action proportionately with the nature and seriousness of the occurrence and taking measures to secure any assets

- ensuring that incidents and breaches are reported in accordance with operating procedures

- co-operating in any subsequent investigation

**5.5 Staff** All staff are responsible for:

- ensuring that they understand and comply with the organization’s policies and procedures
- reporting any incident in accordance with these procedures
- co-operating fully in any incident investigations

**6.0 Failure to Comply** Failure to report a security incident that you are aware of could result in disciplinary action, possibly including termination. Serious or repeated security breaches, including deliberate or damaging behavior, will also be subject to disciplinary action and will likely result in termination.

## Disaster Recovery Plan

The public version of the disaster recovery plan for 4Thought Marketing can be found here – Disaster Recovery Plan. This plan is reviewed, and critical areas are tested annually.

**RTO:** As per section 2.2 of the Disaster Recover document, RTO is:

- 2 Hours for an emergency level of service
- 4 Hours for critical services
- 8-24 hours for recovery to full business as usual (8 Target, 24 for lowest importance functions)

**RTP:** In the event of a catastrophic failure, 4Thought's goal is to restore databases to:

- Any Moment within the last 24 Hours
- Any hour within the last three days
- Any day within the last 30 days.
- Manual backups are taken as well.

## Log Storage, Retention, Disposal

Log access is limited exclusively to necessary personnel (Typically the CEO, CTO, and Security Team). 4TM-created logs are currently stored indefinitely. AWS Cloud Trail logs are stored as recommended by AWS Cloud Trail documentation. All security logs are to be reviewed at a minimum every 30 days.

## Confidentiality & Non-Disclosure

This agreement (the "Agreement") is entered into by 4Thought Marketing SA ("Company") and the employee, prospective employee, contractor, or prospective contractor who has signed it at the bottom ("Team Member"). In consideration of the commencement and continuation of Team Member's agreement with Company and the compensation that will be paid, Team Member and Company agree as follows:

- Customer and Partner Confidential Information and Trade Secrets

In the performance of Team Member's job duties with Company, Team Member will be exposed to Confidential Information owned by Company's customers, suppliers, vendors, partners, and consultants ("Customers or Partners") specifically including but not limited to Oracle, Adobe, Salesforce.com, Software Representatives, and Amazon Web Services. "Confidential Information" means information or material that is commercially valuable and not generally known or readily ascertainable in the industry. This includes, but is not limited to: (a) technical information concerning a Customer or Partner's products and services, including product know-how, best practices, formulas, designs, devices, diagrams, software code, test results, processes, inventions, research projects and product development, technical memoranda and correspondence; (b) information concerning a Customer or Partner's business, including cost information, profits, sales information, accounting and unpublished financial information, business plans, markets and marketing methods, customer lists and customer information, purchasing techniques, supplier lists and supplier information and advertising strategies; (c) information concerning a Customer or Partner's Team Members, including salaries, strengths, weaknesses and skills; (d) information of any sort including data files, contact lists, marketing plans and processes, etc., submitted by a Customer or Partner with Company for study, evaluation, improvement, project work, or use; and (e) any other information not generally known to the public which, if misused or disclosed, could reasonably be expected to adversely affect a Customer or Partner's business.

- Nondisclosure of Trade Secrets

Team Member shall keep a Customer or Partner's Confidential Information, whether or not prepared or developed by Team Member, in the strictest confidence. Team Member will not disclose such information to anyone outside the Company without the Company's prior written consent. Nor will Team Member use any Confidential Information for Team Member's own purposes or the benefit of anyone other than Company. However, Team Member shall have no obligation to treat as confidential any information which: (a) was in Team Member's possession or known to Team Member, without an obligation to keep it confidential, before such information was disclosed to Team Member by Company or a Customer or Partner; (b) is or becomes public knowledge through a source other than Team Member and through no fault of Team Member; or (c) is or becomes lawfully available to Team Member from a source other than Company or a Customer or Partner.

- Return of Materials

When the Team Member's employment with Company ends, for whatever reason, Team Member will promptly deliver to Company all originals and copies of all documents, records, software programs, media, and other materials containing any Customer or Partner Confidential Information.

- Confidentiality Obligation Survives Agreement

Team Member's obligation to maintain the confidentiality and security of a Customer or Partner's Confidential Information remains even after Team Member's employee or contractor agreement with Company ends and continues for so long as such Confidential Information remains a trade secret.

- General Provisions

(a) Relationships: Nothing contained in this Agreement shall be deemed to make Team Member a partner or member of a joint venture of Company or a Customer or Partner for any purpose.

(b) Severability: If a court finds any provision of this Agreement invalid or unenforceable, the remainder of this Agreement shall be interpreted to best effect the intent of the Company and Team Member.

(c) Integration: This Agreement expresses the complete understanding of the parties with respect to Customer or Partner Confidential Information and supersedes all prior proposals, agreements, representations, and understandings. This Agreement may not be amended except in writing, signed by both Company and Team Member.

(d) Waiver: The failure to exercise any right provided in this Agreement shall not be a waiver of prior or subsequent rights. (e) Injunctive Relief: Any misappropriation of any of the Confidential Information in violation of this Agreement may cause Company irreparable harm, the amount of which may be difficult to ascertain, and therefore, Team Member agrees that Company shall have the right to apply to a court of competent jurisdiction for an order enjoining any such further misappropriation and for such other relief as Company deems appropriate. This right is in addition to the remedies otherwise available to the Company.

(f) Indemnity: Team Member agrees to indemnify Company against any losses, damages, claims, or expenses incurred or suffered by Company due to Team Member's breach of this Agreement.

(g) Attorney Fees and Expenses: In a dispute arising out of or related to this Agreement, the prevailing party shall have the right to collect from the other party its reasonable attorney fees, costs, and necessary expenditures.

(h) Governing Law. The laws of the State of California shall govern this Agreement.

(i) Jurisdiction. Team Member consents to the exclusive jurisdiction and venue of the federal and state courts located in California in any action arising out of or relating to this Agreement. Team Member waives any other venue to which Team Member might be entitled by domicile or otherwise.

(j) Successors & Assigns. This Agreement shall bind each party's heirs, successors, and assigns. The company may assign this Agreement to any party at any time. Team Member shall not assign any of their rights or obligations under this Agreement without the Company's prior written consent. Any assignment or transfer in violation of this section shall be void.

- Signatures

Team Member has carefully read this Agreement and agrees that all the restrictions set forth are fair and reasonably required to protect the Company's interests. Team Member has received a copy of this Agreement signed by the parties. Team Member understands and agrees that signing this agreement and re-signing it annually is a condition of continued relationship with the Company.

## Vendor & Third-Party Security Information

4Thought Marketing categorizes all vendors based on risk and reviews them according to our Third Party Risk Management Policy. Critical vendors that contain customer information are listed below:

**TechCello** (4Segments)
Security by TechCello

**Egnyte** (Temporary/Working Customer File and Data Storage)
Egnyte Security Architecture White Paper

Egnyte Security Framework

**Planview Adaptive Work (formerly Clarizen) for Project Status**
Planview Security Whitepaper
Planview Security Info Sheet
Planview Privacy and Encryption Information

**Amazon Web Services: 4Bridge, 4Segments, 4Comply, and all Eloqua Cloud Apps**
AWS Security Center
AWS Security Processes White Paper

# Sustainable Business Practices

## ESG, Sustainability, and Carbon Footprint

Our carbon footprint is minimal because 4Thought Marketing is a virtual software company. Our carbon usage falls into two categories:

- For our marketing and consulting services, our carbon footprint is the same as the average human being.

- We use AWS Cloud Services, committed to powering all its operations with renewable energy by 2025 and reaching net-zero carbon emissions by 2040. In June 2021, Amazon became the world's largest corporate purchaser of renewable energy, generating 65% of its electricity from renewable sources.

4Thought Marketing is committed to sustainability and reducing our carbon footprint. We are proud to partner with AWS, a leader in sustainable cloud computing.

## Child Labor and Slavery Policy Statement

4Thought Marketing is committed to respecting the human rights of all people, including children. We oppose child labor and slavery in all forms. We will not tolerate the use of child labor or slavery in our supply chain.

**Child Labor –** Child labor is defined as any work that is performed by a person under the age of 18 that is harmful or dangerous to their health or well-being or that interferes with their education or development. We will not do business with any supplier that uses child labor.

**Slavery –** Slavery is defined as any form of forced labor or servitude, including human trafficking. We will not do business with any supplier that uses slavery.

**Our Policy**

We have a zero-tolerance policy for child labor and slavery in our organization and our supply chain. All of our suppliers must sign and adhere to our Code of Conduct, which prohibits the use of child labor and slavery. We also regularly review our suppliers to ensure they comply with our Code of Conduct.

## Bribery/Corruption Policy Statement

4Thought Marketing is committed to conducting business ethically and complying with all applicable laws and regulations. We have a zero-tolerance policy for bribery and corruption in all forms.

Bribery is the offering, giving, or receiving of anything of value to influence an act or decision in a way that is improper or dishonest. Corruption is a broader term that encompasses bribery and other forms of misconduct, such as fraud, embezzlement, and abuse of power.

**Our Policy**

We prohibit all our employees and agents from engaging in bribery or corruption. This includes, but is not limited to:

- Offering, promising, or giving any bribe or kickback to any government official, public employee, or other person to obtain or retain business or other favorable treatment.

- Making any payment or providing any other benefit to a third party with the knowledge or understanding that the payment or benefit will be used to bribe or corrupt any person.

Engaging in any other form of misconduct intended to influence an act or decision improperly.

### Reporting Violations

We encourage all employees and agents to report any suspected violations of this policy to their manager or to our compliance department. All reports will be investigated promptly and confidentially.

### Consequences

Any employee or agent who violates this policy will be subject to disciplinary action, up to and including termination of employment. We may also report violations of this policy to the appropriate law enforcement authorities.

### Our Commitment to Ethical Business

We are committed to conducting our business ethically and responsibly. We believe that bribery and corruption undermine fair competition and harm the communities in which we operate.

## Environmental, Health & Safety

4Thought Marketing is committed to protecting the health and safety of our employees and the environment, even though we are a virtual organization with no physical office footprint. We will strive to minimize our environmental impact and create a safe and healthy work environment for all employees.

## Penalties and Punishments for Security Violations

In cases of security violations, our response scales according to the severity of the breach. For minor violations, retraining and reprimands are standard. Medium-level violations may warrant more significant disciplinary actions. Major violations, particularly those compromising data confidentiality or integrity, will likely result in immediate termination. In all cases, reporting violations is mandatory, and adherence to confidentiality agreements is crucial. Our approach aligns with recent trends in data protection, where penalties reflect the seriousness of the violations, the harm caused, and the level of cooperation.

## Acceptable Use Policy (AUP)

**1. Purpose and Overview**
This Acceptable Use Policy outlines the guidelines for using 4Thought Marketing(4TM) IT resources to ensure their secure, efficient, and lawful use. It applies to all employees and contractors using company technology and networks.

**2. Scope**
This policy covers all 4TM technology and IT resources, including but not limited to computers, networks, software, and email systems.

**3. Acceptable Use**
Users must employ 4TM’s IT resources primarily for job-related activities. Occasional personal use is permissible if it does not hinder job performance or compromise company security.

**4. Prohibited Use**
Prohibited actions include:

- Engaging in illegal activities.
- Accessing or distributing offensive, threatening, or harmful content.
- Utilizing IT resources for unauthorized personal gain.

**5. System and Network Activities**
Users should:

- Use secure passwords and change them regularly.
- Avoid public Wi-Fi for company activities.
- Report any suspicious system activities or security concerns immediately.

**6. Email and Communication Activities**

- Use email primarily for business communication.

- Avoid opening suspicious email attachments or links.
- Refrain from sending unsolicited mass emails or spam.

### 7. Software and Intellectual Property

- Adhere to software licensing agreements.
- Refrain from installing unauthorized software on company devices.

### 8. Confidentiality

- Protect sensitive company, client, and personal data.
- Share confidential information only with authorized parties.

### 9. Enforcement Procedures

Violations of this policy may result in disciplinary action, up to and including termination of employment.

### 10. Review and Revision Procedures

This policy will be reviewed annually and updated as necessary.

**11. Acknowledgment**
All users must read, understand, and acknowledge this policy, agreeing to adhere to its terms.

**Regular Updates**
The policy will be revisited and updated regularly to reflect new technological and legal developments.

This AUP is designed to be straightforward and to the point, ensuring that all employees and contractors of 4Thought Marketing are clear about their responsibilities and the expectations surrounding the use of company IT resources.

## Conclusion

4Thought Marketing continually enhances our security posture by adopting best practices and staying up to date with the latest developments in cybersecurity. This includes regular staff training, updates to our technological infrastructure, and ongoing improvements to our operational processes to mitigate risks effectively. Should you have any inquiries or need further details about our SOC 2 certification process or any other aspect of our security measures, please don’t hesitate to reach out to us.