4Thought Marketing Security Policies

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.

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 that is a separate database decoupled from the raw storage layer. As a final precaution, administrators have the option to replicate their data to a secondary Tier II, SSAE 16 compliant facility where it is again replicated on RAID6 servers.

Data Movement

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 in the world by using 256-bit AES encryption to encode data during transmission. 256-bit AES encryption is the strictest standard applied by the U.S. government for TOP SECRET documentation and ensures that even if company data was intercepted, it would be impossible to decipher.

Back up procedures

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

Egnyte

Egnyte is our main 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/218005607-Crypto-Ransomware-Recovery

In the event of folder changes or accidental deletion, the same 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 here is lost or we need to revert the code to a previous version because of a malicious act, XP Dev backs up the code and it 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 1 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 back to its pre-corrupted state, and undo changes or deletion of data if required. More about this here – https://support.office.com/en-us/article/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 entire time the subscription is active.

Website

4Thought Marketing's website has an automated daily backup procedure, these backups are stored by GoDaddy for up to 30 days.

No data is kept outside of these 4 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.

Network Security – Egnyte

Egnyte houses all file servers in industry-leading Tier II, SSAE 16 compliant colocation facilities that feature 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.

Network Security – AWS

AWS has an extensive security setup. You can read about this here. In addition to the standard security features offered by AWS, 4Thought Marketing also uses 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.

Network Security – 4Thought Marketing Office

By policy, *no confidential or customer data is stored* on 4Thought Marketing office servers, office hard drives, end-user computers or other potentially hackable storage devices

within the network. We do maintain a network firewall and virus scanning software, as a general precaution, but our general security philosophy is that ALL information of value is maintained in the cloud (eg on either Egnyte or AWS servers with 2nd factor authentication implemented). Thus, in the event our office network were to be hacked, or an employee device were to be hacked, lost or stolen, no customer data or other data of value is vulnerable on those devices.
Wireless access is permitted at 4Thought Marketing. WPA2 security or better, for login and encryption of information in transit is required.

In accordance with best practices, specifics such as system diagrams of available cloud servers, office/network DMZ Zones, specific brands of protective gear etc is considered security confidential.

Physical Security – 4Thought Marketing Office

Although no data is stored on 4Thought Market employee machines, our offices are in a high security facility with a 100% perimeter fenced (9 foot) and gated facility with video surveillance manned by (a minimum) of 6 full time guards on duty 24×7 (more on duty during business hours). All non-employee vehicles that enter the park are stopped by security, confirmed to be valid, logged, and must leave personal identification with the guard house while on premise. All vehicles that leave the park must stop at security to retrieve their identification and be logged out. Employees utilize an electronic security pass for vehicle access that is immediately next to the guard gate for visual secondary confirmation of proper access. Entry to the building is through two locked doors, one for the lobby/general area, the other for the physical facility. All employees without a private locking office are required to abide by 4Thought Marketing’s Clean Desk Policy which requires that all customer information be put away prior to leaving the desk for more

than 5 minutes.

Printer Security – 4Thought Marketing Office

4Thought Marketing maintains a consumer class printer in our office which is typically used less than once a month for legal documents for customers that don’t support Docusign/eSigning. This printer is powered down except when actively printing and is not attached to the network. It is used only by direct connection to the laptop in question. Printer use is extremely rare and as an organization we use almost no paper and by policy customer information is never printed.

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 are required to abide by 4Thought Marketing’s Clean Desk Policy which requires that all customer information be put away prior to 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. Temporary (defined limited time) exceptions can be made by a member of the Executive Team or the Security Officer. In such cases a request will be made prior to 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 Secure Data is able to be stored as Data at Rest once again. Then Customer Secure Data will be delete from the recordable CD, DVD, Removable Storage

device, USB stick immediately after doing so.

Equipment Disposal

For absolute surety when disposing of devices, all device data is wiped 3 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. Following this standard ensures the elimination all software possibility of recovery, and all 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

Access Control -Authorization

Upon the hiring or contracting of new team members, access to required systems will be granted in accordance with this policy.

All IDs or User Names assigned for all systems shall abide by corporate naming conventions. In accordance with 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 that an individual will likely encounter over one calendar year.

All lockout times for systems (such as Windows environments) should be set to automatically lockout after 30 minutes of non-use.

To the degree permissible by each system, all systems shall be setup to require passwords in accordance with the password control policy established herein.

Access Control –Management

Upon any change in responsibilities, all system access shall be immediately adjusted accordingly.

Upon termination, resignation, or other team member departure, access to all systems shall be immediately canceled. This cancelation of access will be reported to, and logged by the security officer.

Access Control -Separation of Duty

To the degree permissible by each system:

- Each system shall have a “top level” login/password that is reserved solely and exclusively for assigning user rights and access within the system. Access to this password shall be reserved to the Security Officer, CEO, CTO and assigned technical resource.
- Accordingly, when possible, individuals will not be given the right to assign user level access.
- 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.
Security Officer will update the security log with:

a. The date, time of review and name and title person conducting the review.
b. Any access control violations discovered (left-over user or contractor logins for inactive team members).
c. Remedial Actions taken including:
    a. Review of responsibility and points of failure for access control violations
    b. 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 8 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 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, or 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 create a password based on a song title, affirmation, or another 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 on a periodic or random basis by the Infosec Team or its

delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance 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 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.

Passphrases

Passphrases generally are used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, which is known only to the user.

Without the passphrase to unlock the private key, the user cannot gain access.

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

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 in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.
- Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

Penetration & Network Viability Testing

4Thought Marketing conducts Network Viability Testing and Penetration Testing (pen testing) on all of its apps, servers, and websites.

These tests are completed with tools from Detectify.

Detectify tests cover the OWASP Top 10 (as found at www.owasp.org) along with over 930 additional Pentests and Network Viability Tests, some of which are listed here. 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
- Using 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.

Oracle Eloqua Cloud App 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.

DDoS Attacks (Denial of Service)

4Thought addresses DDoS attacks through the utilization of 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.

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.**

EU-US Privacy Shield

4Thought Marketing complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States. 4Thought Marketing is in the final stages of certification with Privacy Shield and has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.

In compliance with the Privacy Shield Principles, 4Thought Marketing commits to resolve complaints about our collection or use of your personal information. EU individuals with inquiries or complaints regarding our Privacy Shield policy should first contact 4Thought Marketing here: security@4ThoughtMarketing.com.
4Thought Marketing is aware of the legal changes occurring regarding Privacy Shield and will adapt to and adopt new standards & regulations as they emerge.

Risk Analysis and Risk 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 so as to not reveal to potential adversaries the areas that we evaluate as vulnerable vs strong. The template that shows the areas covered (without annual assessment results) can be downloaded here.
- 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.

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
6. Public

Executive

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

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.

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.

4Thought Marketing 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 critial areas tested annually

4Thought Marketing 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 tested annually.

Security Incident Reporting Policy & Procedures

1.0 Introduction

The purpose of this policy is to ensure staff within the organization are able to 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 that they can be dealt with in a swift, consistent and professional manner.

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 ‘non compliance with security policies and procedures, or any fact or event which you think could affect the organisation’s personnel, physical

and/or information security’.

5.0 Roles and Responsibilities

5.1 Security

The Security Officer is responsible for the implementation of 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 that is formed on an incident by incident situation. 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/or Media (optional if no customer reporting required)

The SIT is responsible for:

- assessing the reported incident and contacting the person who has logged the call to find out more detail 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 breaches of security, which include deliberate or damaging behavior, will also be subject to disciplinary action and are likely to result in termination.

Written & Annual Policy Compliance and 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 on following. It is the responsibility of the Security Officer to confirm, log and store that all team members successfully complete document signature.

TEAM MEMBER Customer and Partner Nondisclosure & Confidentiality Agreement

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/or 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 Company without Company's prior written consent. Nor will Team Member make use of 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 Team Member’s employment with Company ends, for whatever reason, Team Member will promptly deliver to Company al 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 so as best to effect the intent of 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 a 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 to be in addition to the remedies otherwise available to Company.

(f) Indemnity: Team Member agrees to indemnify Company against any and all losses, damages, claims or expenses incurred or suffered by Company as a result of 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 and costs and necessary expenditures.

(h) Governing Law. This Agreement shall be governed in accordance with the laws of the State of California.

(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. Company may assign this Agreement to any party at any time. Team Member shall not assign any of his or her rights or obligations under this Agreement without Company's prior written consent. Any assignment or transfer in violation of this section shall be void.

- Signatures

Team Member has carefully read all of this Agreement and agrees that all of the restrictions set forth are fair and reasonably required to protect Company's interests. Team Member has received a copy of this Agreement as 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.

Team Member: Company:

_____ _____

(Signature) (Signature)

—-end Team Member Customer and Partner Nondisclosure & Confidentiality Agreement—

Vendor & 3rd Party Security Information

TechCello (4Segments)
Security by TechCello
Security and Load Testing Report

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

Clarizen (Project Status information only)
Clarizen Security Log
Clarizen Security Policies

Amazon Web Services (4Bridge, 4Segments, 4Clean and Marketing

Wiki Customers)
AWS Security Center
AWS Security Processes White Paper