Information Security Policy

Version 1.2

Updated September 2021

Change Log

2017-03-08 – v0.1	Michael Perklin	First Draft
2017-03-30 – v0.2	Michael Perklin	Second Draft
2017-05-11 – v0.3	Michael Perklin	Third Draft
2017-08-01 – v0.4	Michael Perklin	Added Email Policy
2018-03-19 – v0.5	Ron Stoner	Added Strong Auth and Visitor policies
2018-09-12 – v0.6	Michael Perklin	Relaxed email signing policy
2018-10-31 – v0.7	Ron Stoner	Migrated policy and added updates
2020-07-16 – v1.0	Ron Stoner, Scott Seidel, Sean Martin	Clarified account policy, Going Public policy, and Strong Authentication
2020-07-28 – v1.1	Andy Evans	Legal Review
2021-09-13 – v1.2	Michael Perklin	Prepared for publication

Preface

Like a chain, the security of a company's information is as strong as its weakest link. Proper security requires the active and deliberate involvement of everyone at an organization from the CEO to the interns. Proper training in information security concepts and information security practices is a 21st century requirement for all companies providing financial services like ShapeShift. This policy describes the information security requirements for all information produced for ShapeShift's business operations and outlines the responsibilities for anyone who performs work for ShapeShift in any capacity.

Definition

ShapeShift Personnel – Throughout this policy, "**ShapeShift personnel**" means any ShapeShift employee, contractor, or agent who conducts business for or on behalf of ShapeShift.

Duties and Responsibilities of ShapeShift Personnel

ShapeShift personnel must fully understand and comply with all requirements and guidelines set out in this policy and to follow them any time they interact with ShapeShift's information.

If you require additional clarity on any part of this policy or your responsibilities to follow its requirements, you must contact ShapeShift's Security team and obtain full clarity before interacting with or producing ShapeShift's information. You may contact the Security Team at security@shapeshift.io.

	**Failure to follow all requirements set out in this policy may result in disciplinary action including termination of your contract or your employment with ShapeShift.**

1.0 – Information Classification Policy

In order to protect ShapeShift's information appropriately, you must first understand the information's sensitivity. Below is an outline of the various classes of information used by ShapeShift with illustrative examples.

Information Classes

- **Public** – Information classified as *public* falls in the least restrictive class of information and is information freely available to the general public. Examples of *public* information include the contents of press releases, ShapeShift's websites, the Switzerland or Market St addresses, public filings or records, and any other information that can be known by ShapeShift's adversaries without increasing risk to ShapeShift personnel, infrastructure, reputation, or ShapeShift's competitive position in the marketplace.
- **Internal** – Information classified as *internal* are nonpublic facts and knowledge that are needed by ShapeShift staff to do their jobs. This type of information would provide attackers targets for potential attacks against ShapeShift, employees, infrastructure, reputation, or competitive position in the marketplace. Examples of *internal* information include the physical location (address) of ShapeShift's offices, the identities of ShapeShift personnel, internal chat communications platform (including private messages), ShapeShift's policies, procedures, routines, and operations, and information that may be classified as *public* in the future once approved by Marketing.
- **Confidential** – Information classified as *confidential* are facts and knowledge that can be used to inflict harm, damage, or compromise to ShapeShift, its personnel, infrastructure, reputation, or competitive position in the marketplace. Examples of *confidential* information include architectural diagrams or schematics of ShapeShift's systems, source code, physical or Internet addresses of production systems.
- **Secret** – Information classified as *secret* are facts used for authentication or authorization of any actor (human or computer) within any system by ShapeShift personnel or infrastructure. Examples of *secret* information include passwords, passphrases, and private API tokens.
- **Cold-Secret** – Information classified as *cold-secret* are keys or seeds used for authentication, authorization, or identification of any actor within any system by ShapeShift personnel or infrastructure. Examples of *cold-secret* information include GPG keys, SSH keys, and 2FA tokens.
- **Top-Secret** – Information classified as *top-secret* are any cryptographic private key or seeds from which cryptographic private keys are derived that are used to gain access to blockchain tokens owned by ShapeShift. Examples of *top-secret* information include Bitcoin private keys, Monero private keys, and the private half of any BIP32 Extended Key.

1.1 – Ambiguous or Unclear Types of Information

Classification examples listed in section 1.0 dictate the classifications of the vast majority of information at ShapeShift, however, sometimes you may come across information that is either ambiguous or unclear as to the classification type. In these situations, you should contact the Security Team for guidance and in the meantime, treat such information as **Confidential**.

2.0 – Information Protection Policy

ShapeShift personnel are required to treat each type of information listed in section 1.0. This section outlines the protection requirements for each class of information:

2.1 – Protection Requirements

- **Public** – Information classified as *public* is not bound by any protection requirements and can be stored and disseminated freely without restriction.
- **Internal** – All *internal* information should be shared with only ShapeShift personnel, including contractors, vendors, or agents on an "as-needed" basis.
- **Confidential** – All *confidential* information must be stored *on ShapeShift-owned devices* in encrypted form using encryption compliant with ShapeShift's policy *2.2 – Information Encryption Requirements.*
    - When transmitted, *confidential* information must be transmitted in accordance with ShapeShift's policy *2.3 – Information Transmission Requirements.*
- **Secret** – All *secret* information must be stored on *ShapeShift-owned devices* in encrypted form using encryption compliant with ShapeShift's policy *2.2 – Information Encryption Requirements.*
    - *Secret* information should never be shared with anyone else (not even other ShapeShift personnel) unless exigent circumstances require it to be shared in an emergency situation to prevent the loss of funds.
    - *Secret* information must be protected with a passphrase to ensure that only authorized users are able to access it.
- **Cold-Secret** – All *cold-secret* information must only be stored on ShapeShift-owned, non-networked devices in encrypted form using encryption compliant with ShapeShift's policy *2.2 – Information Encryption Requirements.*
    - *Cold-secret* information should never be shared with anyone else (not even other ShapeShift personnel) unless exigent circumstances require it to be shared in an emergency situation to prevent the loss of funds.
    - *Cold-secret* information must never be entered into any device that has a network antenna of any kind. This includes laptops,

mobile phones, and tablets, as well as password managers on network-connected devices.
    - *Cold-secret* information must be protected with access control (i.e. a passphrase on devices, or stored in a safe) to ensure that only the owner of the cold secret is able to access it.
    - Backups of *cold-secret* information must exist and be made by an authorized user only. Backups must be stored in access-controlled locations that ensure only authorized users can gain access.
- **Top-Secret** – All *top-secret* information must only be stored on authorized ShapeShift-owned devices in encrypted form using encryption compliant with ShapeShift's policy *2.2 – Information Encryption* Requirements.
    - *Top-secret* information should never be shared with anyone else (not even other ShapeShift personnel) unless exigent circumstances require it to be shared in an emergency situation to prevent the loss of funds.
    - Backups of *top-secret* information must be maintained on non-digital devices that provide resistance to fire, flood, and electromagnetic pulses.

2.2 – Information Encryption Requirements

Where this policy requires information be stored or transmitted in encrypted form, the following requirements must be met by the storage cryptosystem:

2.2.1. Only the following encryption algorithms are authorized for the secure storage of ShapeShift information:
- AES with a key size no smaller than 256 bits
- RSA with a key size no smaller than 4096 bits

2.2.2. The encryption key that protects the encrypted information must be protected with a password that meets ShapeShift's policy *5.2 – Password* Policy.

2.2.3. Examples of approved encryption software include:
- Apple FileVault 2 Full-Disk Encryption with default settings
- Linux LUKS Volume Encryption in aes-xts-plain64 mode
- Encrypted OS X Disk Images with 256-bit AES keys
- Veracrypt 1.19 or later

2.3 – Information Transmission Requirements

When any information classified as *confidential* or higher is transmitted to another authorized user, it must be transmitted in encrypted form. The transmitting software must meet **any one** of the following requirements:

- The encryption algorithm and key size used by the transmission protocol must be compliant with the approved list in ShapeShift's policy *2.2 – Information Encryption Requirements*. While many other pieces of software may be compliant, a list of approved software is included here:

    - GPG
    - Apple Airdrop
    - Magic Wormhole
    - foxcry.pt

- or -

- The information must be encrypted in compliance with ShapeShift's policy *2.2 – Information Encryption Requirements* and the ciphertext is transmitted over a non-compliant protocol (i.e. Email, Skype, etc.)

- or -

- The information is placed on a ShapeShift-owned non-networked storage device (i.e. USB drive) and handed to the recipient in person. The information on the storage device (or the storage device in its entirety) is then immediately sanitized in accordance with ShapeShift's policy *11.0 – Data Sanitization Policy*.

2.4 – Destruction of Communications

When systems are breached, it is common for attackers to read through old emails, instant messages like Slack messages, and other communications in search of information that can help them exfiltrate funds or breach additional servers. As a result, ShapeShift has adopted a policy to restrict the lifetime of communications.

2.4.1. Email clients must be configured to automatically delete emails older than 6 months unless the email is flagged for permanent storage and/or in long-term archive folders

2.4.2. Slack channels must be configured to automatically delete messages older than 6 months unless the messages are pinned

2.4.3. Wherever possible, the contents of important communications should be archived in other long-term locations such as *git* repositories, or internal *Notion*.

2.4.4. The Security Team may make changes to the above data retention policy from time-to-time due to changing operational, legal, or security requirements.

3.0 – Social Media Policy

To-date, the most effective attacks against exchanges in the blockchain space are a result of spear-phishing attacks directed at exchange employees, contractors, or agents. As a result, ShapeShift has adopted a policy whereby all ShapeShift personnel are discouraged from disclosing their affiliation with ShapeShift unless they have undergone appropriate training and have received written permission from Marketing and Security. This is known as the "Going Public" process and is outlined in Section 3.1. The goal of this policy is to prevent the casual identification of ShapeShift personnel online, thereby preventing spear-phishing attacks from being launched.

Specifically you will never:

3.0.1. reveal your employment with ShapeShift on online directories (i.e. LinkedIn or similar services) unless you have been preapproved to associate your employment with ShapeShift by both the Security and Marketing teams.
3.0.2. tweet/update/message the public with any message that infers or implies your employment/engagement with ShapeShift unless preapproved by both the Security and Marketing teams.
3.0.3. reveal the locations of ShapeShift's offices online or to any non-ShapeShift personnel.

The above restrictions are intended to help protect ShapeShift's personnel from being targeted with attacks, but are not intended to make life difficult. It is okay to tell your family and close friends you work for ShapeShift since it's likely these people are not looking to launch spear-phishing attacks against you.
By contrast, a message posted on social media about your new job at ShapeShift will remain online indefinitely and will give attackers a new target for infiltrating our systems: **you**.

	**Do not disclose your employment at ShapeShift to anyone you would not be comfortable inviting into your own home.**

3.1 – Going Public

ShapeShift takes pride in our brand and vision of a decentralized, self-empowered world. We want our employees to advocate for and identify with our company in their own voice to communicate our story and our vision to the world.
Unfortunately, experience has shown that anyone associating themselves with cryptocurrencies or cryptocurrency companies will invite attacks from hackers looking to steal funds from the employee or their company. For this reason, it is policy at ShapeShift that you cannot identify yourself as a ShapeShift employee without first having undergone training and review by the Security Team.

Before "Going Public" with your employment at ShapeShift, you must demonstrate that your personal digital life is prepared for attack by cyber threats by first:

1. attending a "Going Public" training provided jointly by the Security and Marketing teams.
2. applying the knowledge and security best practices you learned in training to ensure all your personal accounts have been secured against common attacks.

3. subsequently meeting with a member of the Security Team to review the Going Public Checklist for verification.

Once approved by the Security Team, the Marketing team will conduct a final review and determine whether to approve the employee's request to publicly represent ShapeShift.

4.0 – Computer Access Policy

ShapeShift issues computers to its staff for business purposes. ShapeShift offers flexible work schedules allowing employees to work from home in pre-approved circumstances, and this can lead to employees using ShapeShift-owned devices for personal tasks. Your use of ShapeShift-owned devices must comply with the following:

4.0.1. All information stored on or accessed from ShapeShift-owned devices will be accessible to ShapeShift. If you aren't comfortable sharing that information with your coworkers, do not access it on ShapeShift devices.

4.0.2. You may not install or execute any application on ShapeShift-owned devices that do not have a valid license issued by the software's publisher. No software cracks, key generators, or workarounds may be used to circumvent any software's licensing mechanisms.

4.0.3. You may not use any revenue-generating software on ShapeShift-owned equipment. This includes cryptocurrency mining software, advertising "auto-clickers", and any other software that is designed to generate assets or value.

4.0.4. There are a variety of websites that are used to distribute malware to visitors. Due to this risk, you may not install any software from a website in the following categories:

- pornography
- Warez / Crackz
- Torrent sites

4.0.5. All ShapeShift computing devices that store or access information classified as internal or higher must be configured to automatically lock the user interface after no less than five minutes.

4.0.6. You must manually lock your device's user interface when leaving the device unattended. We recommended configuring a "hot corner" or a special key combination to lock the device manually on your device.

4.0.7. You may not open any file *received from non-ShapeShift personnel* except for those on the following lists:

- Plain Text Files with the following file extensions are approved:
    i. .txt
    ii. .csv
- Image Files with the following file extensions are approved:

i. .png
ii. .jpg
iii. .gif

For clarification, ***ANY*** files received from non-ShapeShift personnel with any of the following extensions are ***NOT APPROVED*** for opening:

i. Microsoft Office documents of any type (.doc, .docx, .xls, .xlsx, .ppt, .pptx, etc.)
ii. files with a .pdf extension
iii. Executable files of any kind
iv. Scripts of any kind (.js, .sh, .py, etc.)

Files received from other ShapeShift personnel (which includes employees, contractors, vendors, agents) **that are expected** are not subject to these restrictions. If there is **any** doubt whatsoever about the safety of **any** attached file, **Strong Auth** must be used before opening the file.

4.0.8. If you have a business need to open a file that is not listed above, you should first ask the sender to reformat the information into an approved file format. If reformatting the file into an approved file format is not possible, or does not accomplish the intended business objective, you may seek guidance from the Security Team.

If the file still cannot be reformatted, the file must be opened within a segregated environment away from your daily system(s). Compliant examples include virtual machine environments or dedicated "dirty system" computers where the file can be printed directly onto paper.

5.0 – Account Access Policy

This section governs how all ShapeShift personnel interact with their accounts on any system. An account is a set of credentials that grant access to a system for the purpose of carrying out ShapeShift business. This section outlines how ShapeShift personnel must interact with these accounts.

5.1 - Email Account Policy

ShapeShift provides @shapeshift.io and @shapeshift.com email addresses to employees who require them in order to conduct ShapeShift business. In addition to this @shapeshift.io email address, ShapeShift personnel are required to create an email account under an alias name, through a free email service such as Gmail ("**alias email**") in order to protect ShapeShift and ShapeShift personnel from database breaches. When signing up for any new account that requires an email address, ShapeShift personnel will choose

either their @shapeshift.io or “alias email” in accordance with this policy. Alias email accounts owned by ShapeShift.

5.1.1. If the account accesses a system or service that meets one of the following criteria, you should use your @shapeshift.io email address:
- The data stored on the system/service is clearly associated with ShapeShift AG
- The service/system provides a public face and/or social media presence for ShapeShift

5.1.2. If the service/system does not meet either of the criteria above and requires an email address, you should use your alias email.

5.1.3. Any account on a system/service that provides control of ShapeShift’s inventory tokens MUST be configured to use an “alias email.”

5.1.4. Passwords or passphrases on all accounts, including your alias email account must comply with ShapeShift’s policy *5.2 – Password Policy*

5.1.5. Account passwords and 2FA (defined below in section 5.1.7) tokens may NEVER be shared with any other person unless one of the following exceptions exists:
- The system does not support providing access to a common set of resources, and these resources must be shared by two or more personnel

- or -
- ShapeShift’s CISO or COO approves the sharing of credentials

5.1.6. ShapeShift-owned account usernames must always identify the person who will access the account; generic account names (i.e. *root*, *ubuntu*, *admin*) are unacceptable unless the system does not support customizing the usernames and/or does not support multiple users

5.1.7. If the account allows using a second-factor of authentication (2FA), you must configure the account to use 2FA in accordance with ShapeShift’s policy *5.3 – 2FA Token Policy*

5.1.8. Biometric identifiers (e.g., fingerprints, facial geometry, etc.) may **never** be used for authentication of an account. For clarification, biometric identifiers can be used as usernames to quickly fill a text field with an account’s username, but may never be used as an account password.

5.2 – Password Policy

All passwords at ShapeShift are classified as *secret* per ShapeShift’s policy *2.0 – Information Protection Policy.*

The following requirements govern the creation, storage, and use of ***All Passwords*** associated with ShapeShift devices, accounts ,or alias emails:

5.2.1 Passwords must be unique for every account (work or personal). The re-use of passwords is strictly prohibited.

5.2.2 Passwords should maximize the complexity whenever possible for the account that it is protecting. For example, if a system supports passwords with a maximum of 64 characters, the account password should be 64 characters long. Where no maximum is specified, at a **minimum,** *p*asswords must meet the following complexity requirements:
- Be at least 14 characters long or longer when possible
- Contain at least one numeral
- Contain at least one non-alphanumeric symbol
- Contain at least one capital letter

5.2.3 Must **only** be stored in an approved password database whose encryption meets policy *2.2 – Information Encryption Requirements.* Ask the Security Team for password databases approved for use at ShapeShift.
- *You may not use the "Remember Password" feature of a web browser, operating system, or other system.*

5.2.4 Passwords should be changed when there is reason to believe a password has been compromised.

5.2.5 Password cracking or guessing may be performed on a periodic or random basis by the Security Team. If one of your passwords is guessed or cracked during one of these scans, you will be required to change it immediately.

5.2.6 Devices that only support numeric PINs must be configured with a PIN consisting of 6 digits or more. No personal passwords should ever be stored in your ShapeShift password database. Personal passwords should be separated into another password database.

5.3 – 2FA Token Policy

2FA tokens help protect accounts in the event passwords are discovered by an unauthorized party. Even when we do everything right and protect our passwords judiciously, they can still be leaked without your knowledge or permission by poorly-written applications, cryptographic failures in encrypted channels, buffer overflows in middlemen services (see e.g., CloudBleed), or service database breaches. To mitigate this, ShapeShift mandates that all accounts that support 2FA must be configured with 2FA without exception.

5.3.1. If an account supports 2FA of any kind, you must configure it as follows: 2FA tokens must be stored in the Yubico Authenticator software.
- An exception is allowed for development / staging 2FA tokens used for software testing purposes. Development 2FA tokens are allowed to be stored in 1Password for specific teams.

- The TOTP module on your Yubikey (that is accessed by Yubico Authenticator) must be configured with a password to prevent unauthorized use.

5.3.2. A backup of the 2FA token should be made at the time of provisioning to ensure the account is accessible in the event of a lost token

5.3.3. 2FA backups must follow the same policy restrictions as the 2FA token itself

5.3.4. 2FA tokens must ***never*** be stored or backed up in the same location as the password for its associated account

5.3.5. Many sites allow for SMS (i.e., text messaging) or a voice phone call to be used as a 2FA. These options are easily faked by unauthorized parties, thus these two options may ***never*** be used as a 2FA option for any service used for ShapeShift business

Sometimes multiple forms of 2FA are available to be configured on an account. Below is the priority of 2FA options. If faced with multiple 2FA options, you should choose the first method that appears on the following list:

2FA Priority List

1. Native Yubikey One-Time-Passwords (OTPs / U2F)
2. GPG Signatures via Challenge/Response
3. TOTP Tokens (aka FreeOTP / Google Authenticator / Authy)

Prohibited Forms of 2FA

a. SMS/Text Messaging
b. Voice phone call

It is more secure to have NO 2FA at all than to use SMS-based 2FA

6.0 – Mobile Phone Authentication Policy

Due to the proliferation of attacks against cellular telephones used by cryptocurrency owners, ShapeShift has adopted a policy that prohibits any cellular telephone or smartphone to be used for authentication.

7.0 Strong Authentication Policy

At various times ShapeShift personnel may need to perform sensitive actions such as moving funds, altering access, or transmitting confidential information. For these types of requests, Strong Authentication is required.

Strong Authentication (aka StrongAuth) is a method for making sure you're communicating with the right person and not an impostor.

How to Perform Strong Authentication:

- In person: The request was made in-person from someone you know
- Audio + Visual call: The details of the request are spoken during the call, and you can both see and hear the requestor. This can be accomplished using any video conferencing system.
- A **validated and dated,** non-repeatable GPG **signed** message from the requestor's Yubikey.
    - Non-repeatable means that the GPG message is specific to the request being made, and cannot be reused for future requests. For example:
        i. A message that simply states: "Yes" can be reused for future requests.
        ii. On the other hand, a message that specifies: "Yes, send NewCo 1 BTC for invoice 1234 today 03/5/2020." cannot be reused

Strong Authentication applies to requests from ***anyone*** at ShapeShift regardless of title, function, or role. Any request that does not meet Strong Authentication requirements should **NOT** be completed. Department managers and the Security Team should be notified immediately when these types of requests do not comply with the policy.

Strong Authentication is required in these situations (ask yourself the following questions to confirm whether StrongAuth should be used):

1. **M**oney: Are you moving money? Are you communicating an address where money will be moved or stored at a later date?
2. **A**ccess: Does it involve a change in a user's access? Are you granting or revoking access for someone to a system?
3. **C**onfidental: Is the information being sent classified as Confidential per Section 1.0?

Remember: 15 seconds of Strong Authentication could potentially save 15 million dollars.

8.0 – ShapeShift Facilities Policy

While many of ShapeShift's personnel work remotely in countries around the world, ShapeShift does maintain facilities where some ShapeShift personnel carry out business and house confidential information. In order to protect this information, ShapeShift has implemented the following rules:

8.0.1. When ShapeShift's vendors require a physical mailing address for ShapeShift, the following PO Box must be given
1624 Market Street, Suite 226
#29882
Denver, CO 80202-5926

8.0.2. It is the responsibility of all ShapeShift personnel to ensure access doors at facilities lock after each use.

8.1 – Visitor Policy

While ShapeShift does allow visitors, contractors, and third parties on-site, we have policies in place to help mitigate our levels of risk. Since we deal with a lot of sensitive information on a daily basis the physical security of our assets is imperative.

8.1.1. All visitors, including family or friends, to ShapeShift facilities must sign in to the log book and be issued a visitor or contractor badge. This badge must be visible and on their person at all times.
8.1.2. All visitors, including contractors **MUST** be escorted the entire time while on-premises and are the responsibility of the host who signed them in.
8.1.3. Wireless Internet access for visitors may only be granted via the "GuestVisitor" access point. Instructions for granting temporary internet access to visitors are available in the company-wide shared password vault.
8.1.4. It is **EVERYONE'S** responsibility to stop anyone you don't recognize to ask them who they are in order to determine whether they belong on site. This is a great way to meet new staff members: "Hi, who are you?"
8.1.5. Visitors, including contractors are not eligible to use the various building facilities granted to us with our lease (gym, bike room, etc.).
8.1.6. Visitors will **NOT** be permitted in the server room, electrical room, or any rooms / closets / spaces dealing with office utilities under any circumstances. Contractors requiring access to these areas must be given permission by the Security Team prior to the visit.

9.0 – Key Management Policy

Cryptographic keys comprise the two most sensitive classes of information at ShapeShift. When maintaining existing systems, developing new systems, or otherwise interacting with blockchain systems in general, there are always two risks associated with private keys:

- Keys could be leaked to unauthorized parties
- Keys could be lost due to accidental replacement of files

Both of these events could lead to the loss of control of blockchain tokens. In order to minimize these risks, the following policy points must be observed by all ShapeShift personnel when interacting with private keys:

9.0.1. When a new seed/key is required to store ShapeShift funds, the key/seed must be created following the Security team's best practice guide for key ceremonies
    - *Exception: keys/seeds used for development purposes are not subject to this requirement*

9.0.2. The Security team must be informed about the creation of the new key so that it can be archived for business continuity reasons.
9.0.3. Development of new systems at ShapeShift should use hierarchical-deterministic seeds wherever it is possible. This minimizes the chances of losing individual keys.
9.0.4. Backups of development seeds should be maintained in password databases to ensure their confidentiality, integrity, and availability.

10.0 – Data Sanitization Policy

There have been many documented instances where a discarded device or disc – or even discarded paperwork – contained sensitive information that caused harm to a company. As a result, ShapeShift has adopted a Data Sanitization Policy whereby all devices or media that held any ShapeShift information classified as *internal* or higher must be thoroughly sanitized or destroyed prior to being recycled or discarded.

The following policies pertain to ShapeShift devices:

10.0.1. This policy pertains to any computing device (laptop, desktop, or similar device), mobile device (smartphone, tablet, gaming device), or storage medium (optical disc, flash drive, magnetic disk, etc.)
10.0.2. ShapeShift personnel shall not discard or recycle any device, media, or object without proper sanitization in accordance with this policy
10.0.3. Any device, media, or object that only holds information classified as *public* (and does not hold any other information classified higher than *public*) can be discarded without sanitization
10.0.4. Devices, media, or objects that held digital information classified higher than *public* must be sanitized in accordance with the following schedule:
- Magnetic media: 3-pass overwrite with random or pseudorandom data
- Flash media: 1-pass overwrite with random or pseudorandom data
- Optical media: Complete scratching of the surface of the disc followed by physical destruction of the disc
- Paper: Shredded in a paper shredder
- Whiteboards: thorough cleaning to remove all ShapeShift information. If the information cannot be completely removed, the whiteboard must be burned or destroyed
- All other objects: complete removal of all ShapeShift information, and/or burning/destruction of the object

10.0.5. ShapeShift Personnel who perform the sanitization of devices, media, or objects must complete a Data Sanitization Form and file it with ShapeShift's Information Security department. A copy of this form can be found in *Appendix A – Data Sanitization Form*.

Conclusion

The security of ShapeShift's information is a critical aspect of every employee's, contractor's, and agent's job; all ShapeShift personnel bears the responsibility equally. The guidelines and requirements outlined in this policy outline how we must all do our part to ensure ShapeShift's and our own security.

ACKNOWLEDGEMENT OF RECEIPT OF SHAPESHIFT INFORMATION SECURITY POLICY

I acknowledge that I have received a copy of the ShapeShift Information Security Policy (the "**Policy**"), have read it, understand its provisions, and agree to fully abide by it. I further understand that as a ShapeShift employee or contractor, it is my sole responsibility to abide by the requirements and guidelines in the Policy, and failure to do so may result in disciplinary or legal action as deemed appropriate by ShapeShift management. I further acknowledge that it is my responsibility to seek clarification about any aspect of the ShapeShift Information Security Policy should any aspect seem unclear and that ShapeShift may at any time modify, rescind, or revise any part of the Policy.

I acknowledge **that nothing in the Policy creates or is intended to create a promise or representation of continued employment or any other contractual rights or obligations**, and that my employment, position, and compensation at ShapeShift are "at-will", is not for any specific duration, and may be changed or terminated at the will of ShapeShift without cause or notice and that nothing in the Policy should be interpreted to the contrary. This is the entire agreement between me and ShapeShift on this subject; it supersedes any prior inconsistent representations or agreements and may only be modified in writing signed by me and an authorized representative of ShapeShift.

Date: _____

Print Name: _____

Signature: _____

Appendix A – Data Sanitization Form

The Data Sanitization form is on the next page.

[This page intentionally left blank]

ShapeShift

Data Sanitization Form

Date:	
Device Custodian:	
Device Make:	
Device Model:	
Device Serial:	
Sanitizing Personnel:	

Notes:

_____

_____

_____

_____

_____

_____

Signature: _____