Security Training

Part 2: Information Security Policy

This section will teach you how to follow ShapeShift's InfoSec policy, and why each requirement is necessary to keep us all safe

Computer Access (section 4.0)

- ShapeShift-owned devices are always accessible to ShapeShift.
- Don’t put anything on these devices you’re not comfortable sharing with your coworkers.

Computer Access (continued)

- Your hard drive **must** be encrypted (FileVault Enabled from Tech Setup)

- If you need software to perform your job, ask you manager.
    - ShapeShift will purchase it.
    - Do NOT install free versions of paid software

Computer Access (continued)

- ShapeShift doesn't install Antivirus software
  - We assume the laptop has malware
- Be careful about the types of files you open.
  - Microsoft Office files and Adobe PDF files can contain viruses
- Send suspicious files to security@shapeshift.com
- When in doubt ask the security team
  - Slack: #team-security
  - Email: security@shapeshift.com

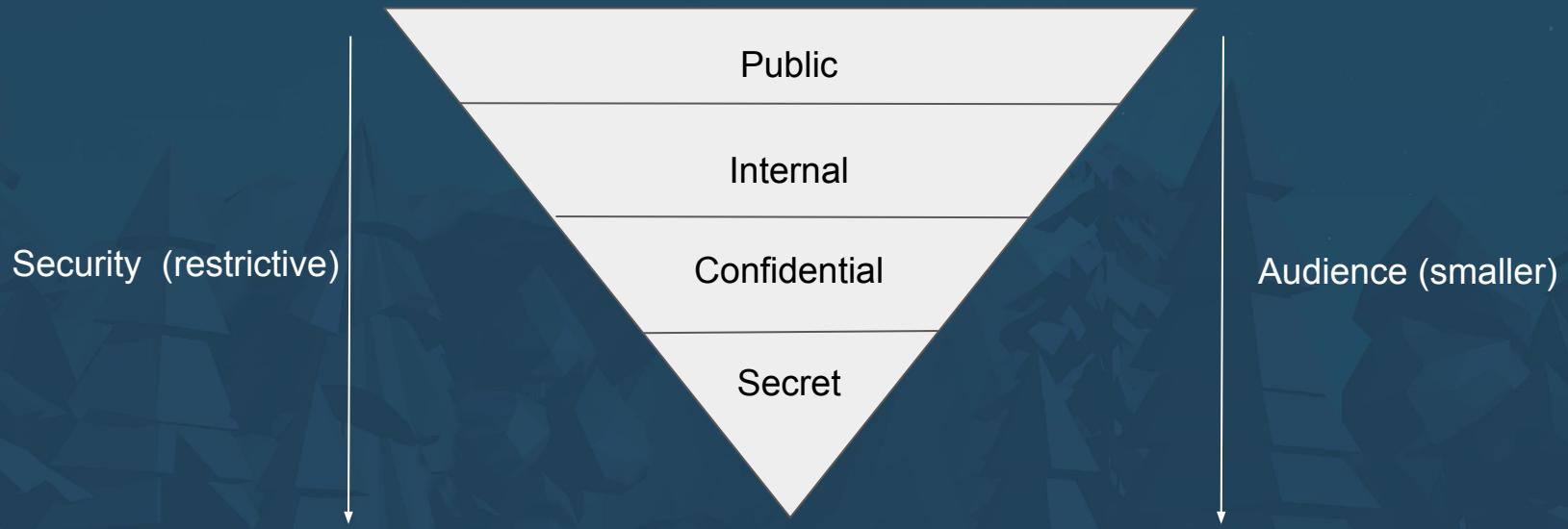
Information Classes (section 2.0)

ShapeShift classifies information in different buckets:

Public
Internal
Confidential
Secret

= Must be encrypted in transit

Classes of Information (Inverted Pyramid)



Public (section 2.0)

Audience:

- The General Public

Protection Requirements:

- Information classified as *public* is not bound by any protection requirements and can be stored and disseminated freely without restriction.

Examples:

- Public website data, press releases, blog posts, etc.

Internal (section 2.0)

Audience:

- ShapeShift personnel, including contractors, vendors, or agents on an “as-needed” basis

Protection Requirements:

- Must be protected with access control
  - i.e. Google account / password

Examples:

- Internal procedures
- Internal tools
- Our AllFox slides
- Physical address of our offices
- Employee last names (if not public)

Confidential (section 2.0)

Audience:

- Select ShapeShift employees/contractors and vendors, on an as-needed basis **only**.

Protection Requirements:

- Must be protected with access control
- When stored on a device, must be encrypted per ShapeShift's Information Encryption Requirements (section 2.2)

Examples:

- ShapeShift's production systems architecture
- Employee (HR) issues, salaries, complaints
- Security vulnerabilities with our products

Secret (section 2.0)

Audience:

- Only **you**.
  - Secrets should never be shared with anyone.

Protection Requirements:

- Must be protected with access control
- When stored on a device, must be encrypted per ShapeShift's Information Encryption Requirements (section 2.2)
- Never shared with anyone else

Examples:

- Passwords
- 2FA Authenticators
- API Keys

Password Policy (section 5.2)

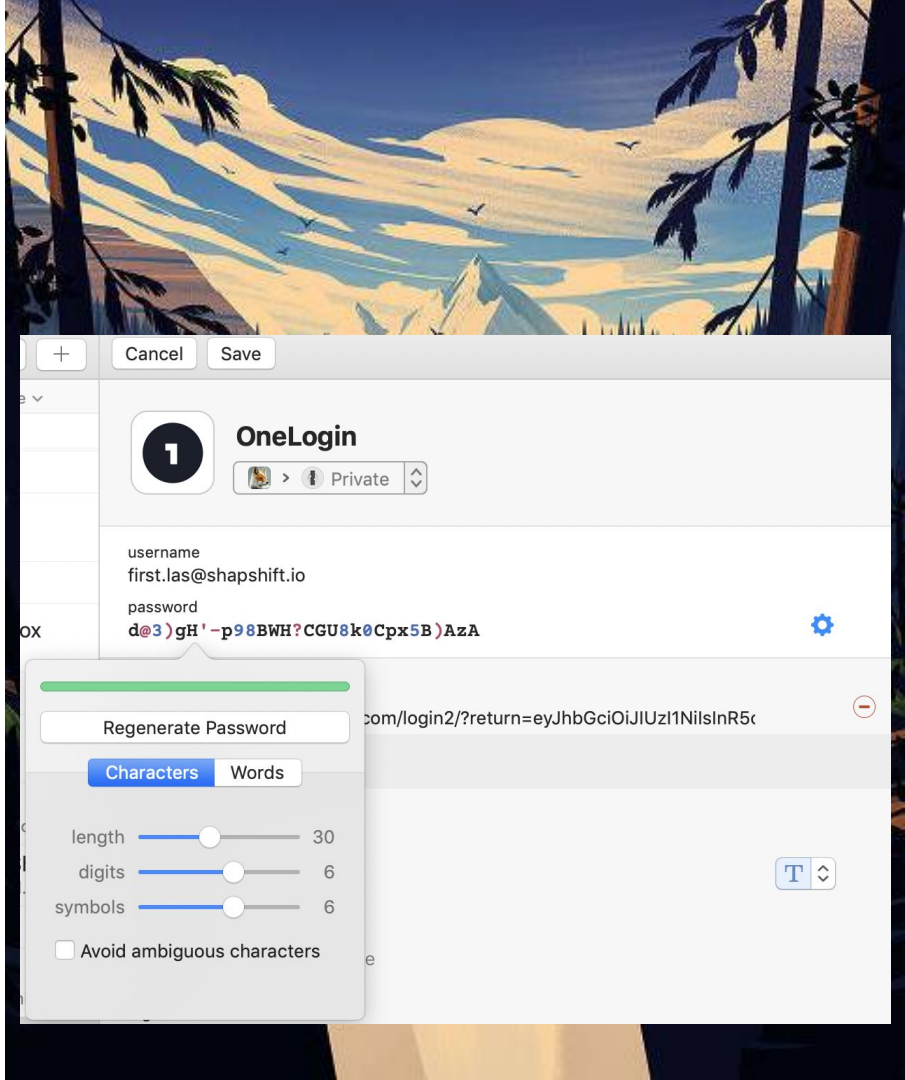
Passwords are an essential part of securing both personal and private accounts.

What makes good passwords?

- **Must** be unique for every account
- **Must** be a minimum of **14** characters
- **Must** contain mixed case
- **Must** contain numerals
- **Must** contain non-alphanumeric symbols

Other password guidelines

- Should be stored in a password vault
- Generated with with maximum security
- Never use “password algorithms”
  - i.e. facebook123, google123



Methods for Memorizable Passwords

Hard:

- Password → Memory

Easy:

- Memory → Password

Methods:

1. Bruce Schneier's Method

2. The Mind Palace Technique

Bruce Schneier's Method

- Take a sentence and turn it into a password.
  - Should be **personal** and **memorable** to you
  - Abbreviate words and combine them in unique ways to form a password

Examples:

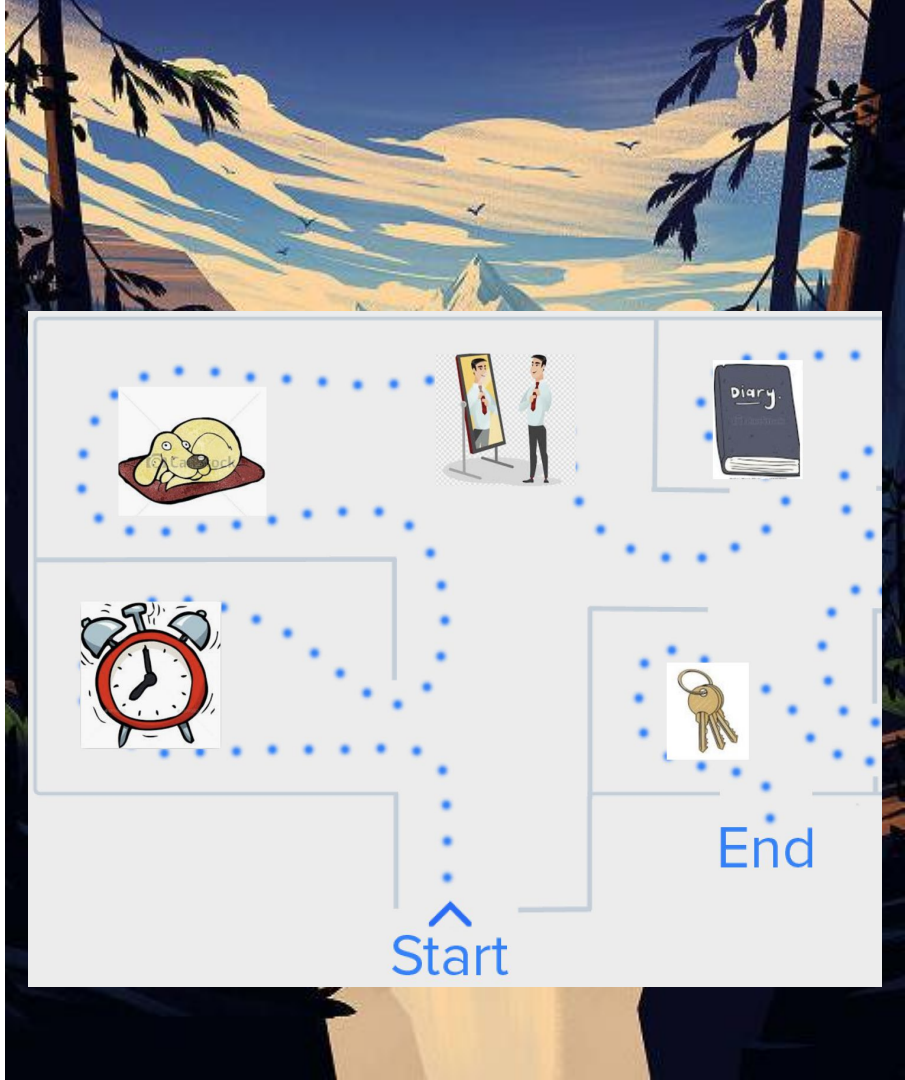
- WOO!TBwontSB
  - Woohoo! The Broncos won the Super Bowl!

- llf,w/asCooP/na()
  - I like fruit, with a scope or in a hoop.

Mind Palace

Technique to turn an existing memory into a strong passphrase

1. Pick an existing memory (i.e. childhood bedroom)
2. “Look” around the room. What do you see?
    - (clock, dog bed, mirror, diary, key)
3. String those things together to form the password
    - Add some numbers and/or symbols
    - `1Clock,Dogbed,mirror.Diary.keys`
4. NEVER USE THINGS YOU CAN LOOK UP
    - It must be a PERSONAL memory



Do what’s best for you!

As long as you can memorize the password easily

2FA (section 5.3)

Two Factor Authentication (2FA) is an extra thing needed to log into an account

- If a password is *something you know*, then a Yubikey is *something you have*.
- Together: they are **two** factors of authentication

It's like using an ATM

- You **have** your debit card
- You **know** your PIN

Yubikey 5

Yubikey 5C

2FA (section 5.3)

ShapeShift:

- Gives you a Yubikey to use for 2FA
- Requires 2FA on all accounts (that support it)

Acceptable 2FA methods for Work accounts:

- Yubikey (tap)
- Yubico Authenticator (TOTP)

Prohibited 2FA (section 5.3)

Never use a phone for 2FA for **any** account you create/use at ShapeShift

Prohibited for work accounts:

- SMS or phone-call 2FA
- 2FA apps on your smartphone
    - i.e. Google Authenticator, Authy
- Biometric identifiers (fingerprint, facial)

Prohibited 2FA (continued)

Why are Text and Phone Prohibited?

- SIM-jacking attacks
    - Attackers take control of the victim's phone by transferring the phone number to the the attackers phone.

How:

- Phishing or Social Engineering attackers can convince the phone company they are YOU.

- Bribing the phone company employees to port your phone number to their SIM card

Prohibited 2FA (continued)

Why are Biometrics (fingerprint/facial recognition Prohibited?

- Biometrics are inherently public
  - You don’t show your password publicly
- Bio-sensors have error thresholds (85% match)
  - It’s like typing most of your password correctly, and being let in anyway
- Biometrics can’t be revoked like passwords/keys
  - If a copy is made you can NEVER revoke it or use that finger for the rest of your life

Questions

Strong Auth

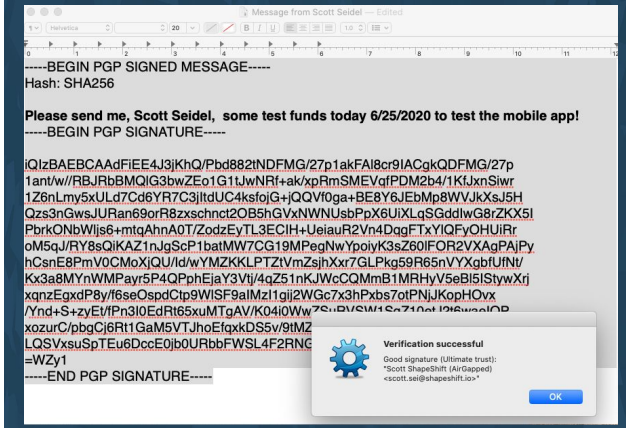
Strong Authentication (**Strong Auth)** is verifying you're communicating with the person you expect.

- ShapeShift employees get impersonated all the time.
- It's a good tool to make sure your dealing with *real* foxes and and not scammers or attackers.

Strong Auth - How

How to perform Strong Authentication?

1. In person
2. Audio + Visual call (both required)
3. A **specific validated** GPG signed message



Strong Auth - When

Think **M.A.C**

- **M**oney (move money anywhere)
- **A**ccess (grant/revoke someone's access)
- **C**onfidential (discuss any confidential info)

You must perform Strong Auth before doing any of these!

Questions

Email Accounts

At ShapeShift we have two email accounts:

1. Corporate email account
    - Used when you need to show you work for ShapeShift

2. Work Alias account
    - Used to protect from a remote breach

Corporate Email Account

Our corporate gmail account takes the form of first.las@shapeshift.com or first.las@shapeshift.io

When do you use our corporate account?

1. When the account or system will be used as a public face of ShapeShift
2. When the account or system is related to your employment
3. When the data in this account already identifies ShapeShift

Alias Email Account

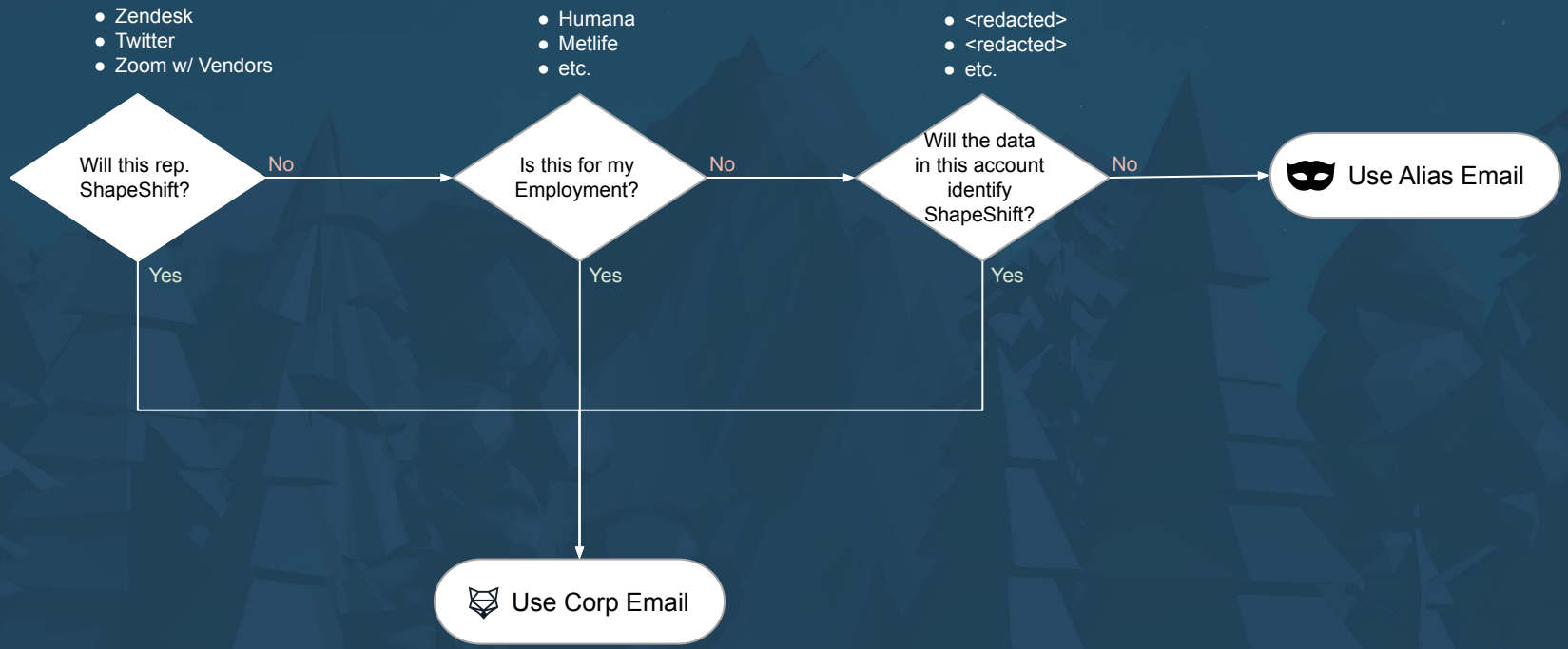
A Gmail account with a made up name
(e.g. sidler.saaz@gmail.com)
and is used whenever we don't use our corporate account.

Why do we have an alias account?

1. So our accounts don't look interesting in other databases
    - Their employees can be curious

2. If another company gets hacked our alias accounts are not a high priority target.
    - Attacks release full databases publicly

Email Account Decision Tree



Questions

Social Media Policy (section 3.0)

We STRONGLY recommend:

- Don’t reveal you work at ShapeShift online yet! This includes:
  - LinkedIn
  - Facebook
  - Instagram
  - Twitter
  - Any Social media

- Finish the **“going public”** training first

- But you *can* tell:
  - Family
  - Friends

Social Media Policy Continued (section 3.0)

A guideline:

Don’t tell them you work at ShapeShift unless you’re comfortable inviting them into your home

Going Public - Protect Yourself!

Going Public Continued (section 3.0)

- 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.
- However, experience has shown that public ShapeShift personnel attract attacks from hackers.
- The “Going Public” training and checklist provide help to employees to protect **their personal** accounts by teaching them good security habits and best practices.

ShapeShift Facilities (section 8.0)

To protect our office and staff:

- ShapeShift Office street addresses are considered **Internal**
- Physical meetings with unknown people should take place off-site.

  Exceptions:
  - Vendors who have signed our NDA
  - New hire candidates on the final phase of the interview process

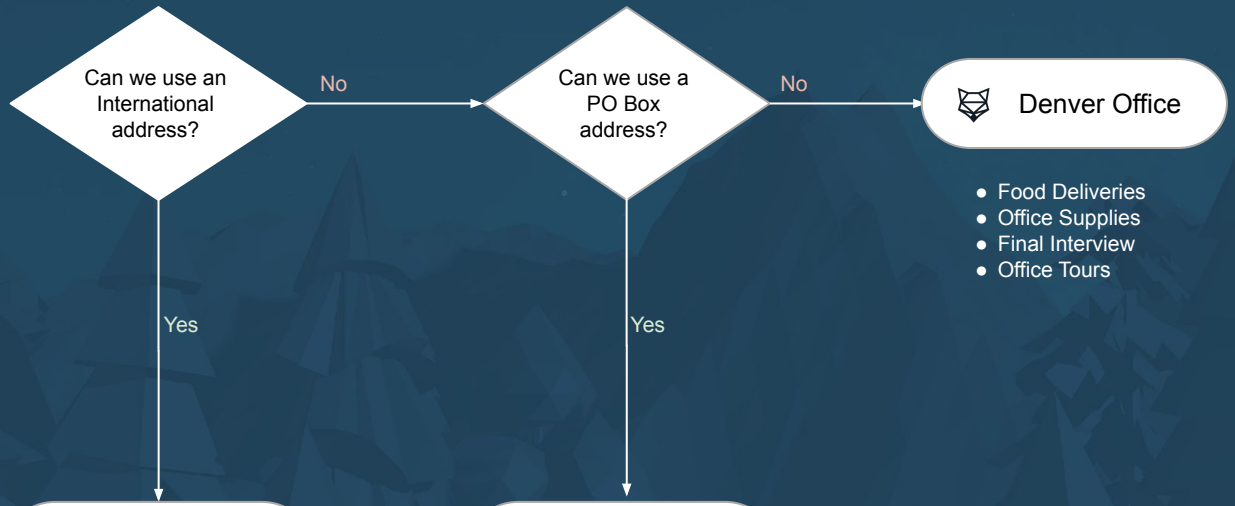
- All personnel are responsible for physical security at the office.

ShapeShift Addresses (section 8.0)

ShapeShift has three addresses:

- Headquarters Address:
  Gartenstrasse 6
  Zug 6300
  Zug, Switzerland
- Mailing Address PO Box:
  1624 Market Street
  Suite 226 #29882
  Denver, CO 80202-5926
- Office Address:
  <redacted>

ShapeShift Address Decision Tree



- Food Deliveries
- Office Supplies
- Final Interview
- Office Tours

- Press Releases
- Public Announcements
- Official docs that need our HQ address

- KeepKey Return Address
- Vendor Signup

Use the Denver address as a last-resort

Data Retention (section 2.4)

ShapeShift deletes old data regularly.

Retention Periods:

- Email - 6 months*
- Slack - 6 months*

Important communications should be archived in long-term locations:

- Google drive
- Internal Notion
- `git` repos

Emails flagged with a ⭐ will not be deleted

Enforcing InfoSec Policy

You can earn points and rewards for helping keep your fellow foxes safe

- Any violation of InfoSec policy reported to Security earns **1 Point**
  - Most common:
    Laptop Left Unlocked! (InfoSec 4.0.6)
- 5 Points = $100 USD
- Offender wears the “Dunce Cap” for ½ a day
- Be Respectful!
  - The goal is to improve security,
    not hurt morale

Questions