WISP Road Map

VALLEY TECHLOGIC

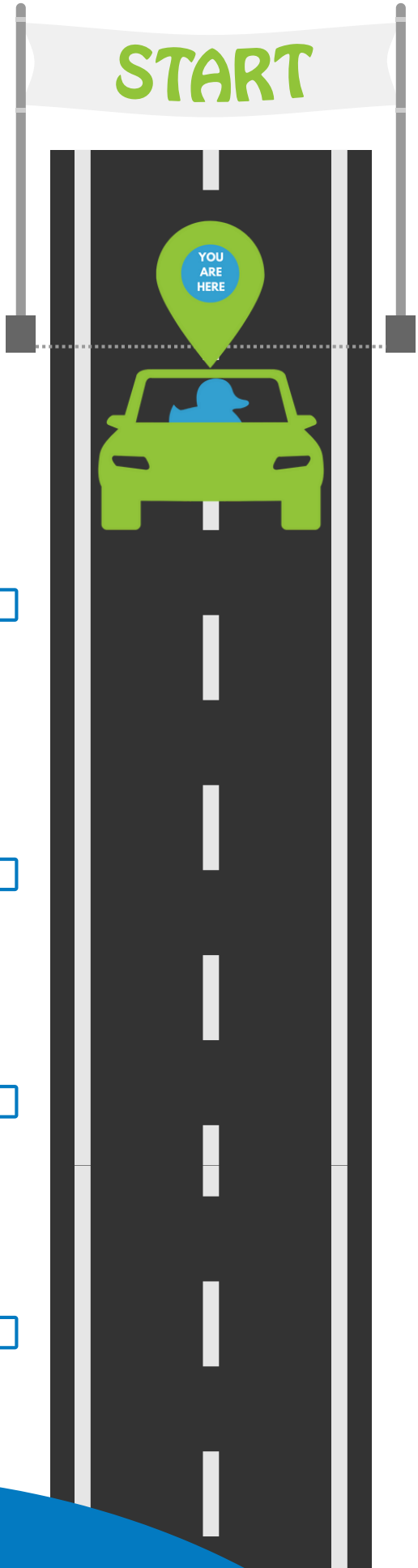
WISP@ValleyTechlogic.com

209-357-3121

111 Business Park Way,
Atwater CA 95301

At Valley Techlogic, we help CPA firms take the guesswork out of Written Information Security Plan (WISP) compliance. Our roadmap is designed to guide your firm step-by-step - from the initial assessment of your current security posture, through the drafting of policies and procedures, all the way to annual reviews and updates while simultaneously providing IT solutions that meet WISP regulatory requirements.

With Valley Techlogic as your partner, your firm can move confidently from start to finish in WISP planning, ensuring regulatory compliance, reducing risk, and creating a clear, sustainable framework for safeguarding client data.



Defining Your WISP

The first step in creating a WISP is outlining the purpose of creating one in the first place. Beyond being a regulatory requirement defining your goals when creating your WISP can make sure the plan you're creating is tailored to your business and can be adequately followed, after all a plan is only as good as it's execution.

Objective Statement

Your objective should contain your reasoning behind the creation of the WISP including to fulfill any provisions your company must personally follow, such as California Consumer Privacy Act (CCPA) or the Gramm-Leach-Bliley Act (GLBA).

Purpose Statement

This statement needs to address how your WISP works to protect the PII (Personal Identifying Information) your company obtains in the course of doing business.

Scope Statement

This statement outlines the scope of your WISP and sets a limit on what your business will be responsible for as it stands at the time of writing. Because of the everchanging landscape of tech, your WISP and procedures should be updated regularly to remain compliant.

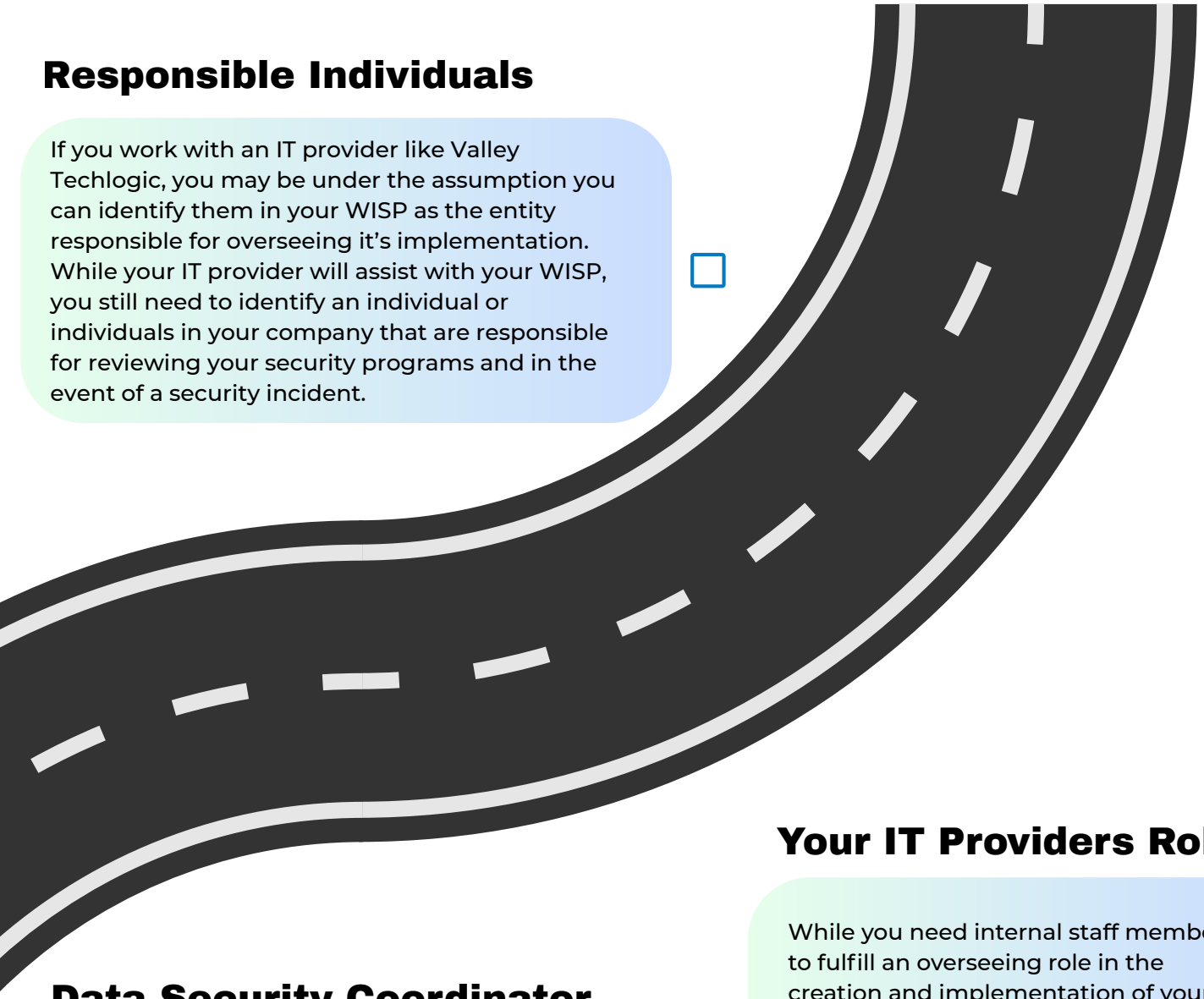
WISP Road Map

VALLEY TECHLOGIC

WISP@ValleyTechlogic.com

209-357-3121

111 Business Park Way,
Atwater CA 95301



Responsible Individuals

If you work with an IT provider like Valley Techlogic, you may be under the assumption you can identify them in your WISP as the entity responsible for overseeing it's implementation. While your IT provider will assist with your WISP, you still need to identify an individual or individuals in your company that are responsible for reviewing your security programs and in the event of a security incident.

Data Security Coordinator

Your Data Security Coordinator needs to be up to speed on your security processes, including organizing staff training and making sure steps outlined in your WISP are being implemented effectively.

Public Information Officer

Your Public Information Officer should be a single voice that is able to speak on behalf of the company should an incident occur. In most cases this should be a separate individual from your Data Security Coordinator but in the case of smaller firms it can be one person doing both roles.

Your IT Providers Role

While you need internal staff members to fulfill an overseeing role in the creation and implementation of your WISP, your IT provider must assist you with it's creation including providing recommendations and solutions that fulfill your ongoing WISP requirements.

WISP is not a one and done process, there can be severe penalties for CPA firms found to be out of compliance with current state and federal regulatory guidance, especially in the event of a security incident.

Your IT provider (or a provider like Valley Techlogic) will ensure your WISP is solid and achievable.

WISP Road Map

VALLEY TECHLOGIC

WISP@ValleyTechlogic.com

209-357-3121

111 Business Park Way,
Atwater CA 95301

Assessing Risks

It goes without saying that the key driver behind creating a WISP is increasing your company's security posture to better ward off outside threats.

Identifying the risks within your organization means having a frank and honest look at the vulnerabilities you and your staff face on a day to day basis and how to mitigate those threats, for example staff members who believe MFA is too complicated or fail to report suspicious emails to IT staff.

It also may mean looking at areas where you are underspending on cyber security, when the average cost of a breach is in the 10s of thousands of dollars, it is penny-wise and pound-foolish to not invest in IT protections for your business and that is before regulatory fines come into play.

Identifying The Information You Store

Your WISP should outline the types of PII your company handles and stores, and not all PII data is created equally (a breach involving just email address data is less significant than a breach containing social security numbers). The IRS instructs that you also must identify the types of documentation your company handles including paper documentation.

Assessing Future Loss

Part of preparing for the future is estimating the loss potential should a potential breach occur and having plans in place for a variety of potential events, which includes digital security threats but also events such as natural disasters, accidental exposure of data and physical theft. You need to have plans in place for your clients data regardless of what outcomes your company may face.

Procedures For New And Emerging Threats

As we mentioned, your WISP is not one and done. In the same way threats are not one and done, new threats emerge daily and it is critical your WISP is updated to address them - working with your IT provider is the best way to stay apprised of current threats and what is being done to prevent them from impacting your company.

WISP Road Map

VALLEY TECHLOGIC

WISP@ValleyTechlogic.com

209-357-3121

111 Business Park Way,
Atwater CA 95301

Inventory Of Your Hardware

It is a requirement that any device enrolled on your network undergo a security review (which should include being up to date in patches, having passwords that fit your companies password policy, disabling “Auto Run” features, and more).

In order to make sure this is happening, you will also need to complete a thorough inventory of all the devices in your firm that come in contact with taxpayer data. The list may be more expansive than you are expecting (especially if what comes to mind is just computers and servers).

Below is a list of the type of inventory you should be inventorying but this is in no means exhaustive. You must work with your IT provider to create an accurate IT inventory list to ensure compliance.

Examples Of Hardware To Track

- Personal Computers (Desktops & Laptops)
- Servers (Physical & Cloud)
- Network Devices (Router, Modem, Switch, Access Points, Firewall, Etc.)
- Mobile Devices
- Printers
- And More

Your inventory list should include a description of each device as well as it’s location and a brief description of how it may interact with client PII data.

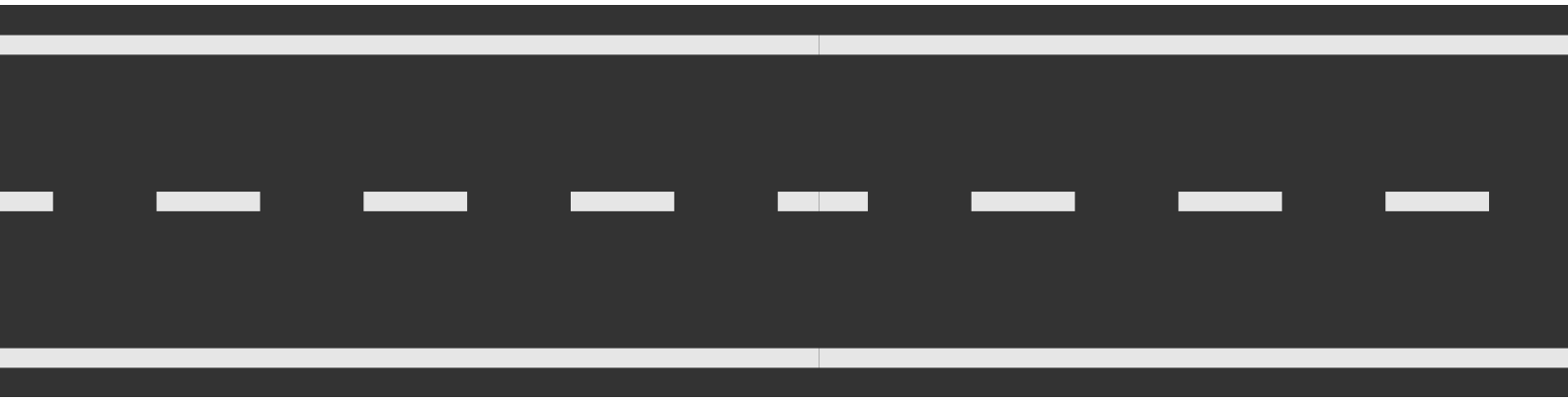
WISP Road Map

VALLEY TECHLOGIC

WISP@ValleyTechlogic.com

209-357-3121

111 Business Park Way,
Atwater CA 95301



Documenting Safety Procedures

There are several components necessary to documenting the safety procedures your firm will be following as part of your WISP compliance.

The first relates to your data collection, storage and destruction of unneeded data. You must precisely identify the type of data you collect and the lifecycle that data undergoes within your firm.

Data Disclosure Policy

You will also need to notify your clients of how you are securing their data via a data disclosure statement. You will need to identify any third-party vendors that interact with client data (this can even include your internet provider and cloud hosting providers). You need to also state how you may share their data with these third-parties as well as stating your own privacy policies.

Data Collection Policy

Your IT provider will assist you in creating a data collection policy, which as we mentioned will cover the lifecycle of the data you collect.

This will include:

- Defining the Data Your Firm Collects
- How it is Stored
- Who Handles that Data
- Designing When and How Documents and Data Are Destroyed

General User Access & Network Protection

Identifying your user access and in-place network protections are a crucial component of your WISP. Policies that restrict access in the event of unsuccessful logins, having multi-factor authentication in place, and a strong password policy will ensure client data is protected.

Strong network protections like a firewall, restricting access by role, network monitoring and endpoint protection, and patching and update policies will not only comply with WISP but also keep your firm safe from external threats.

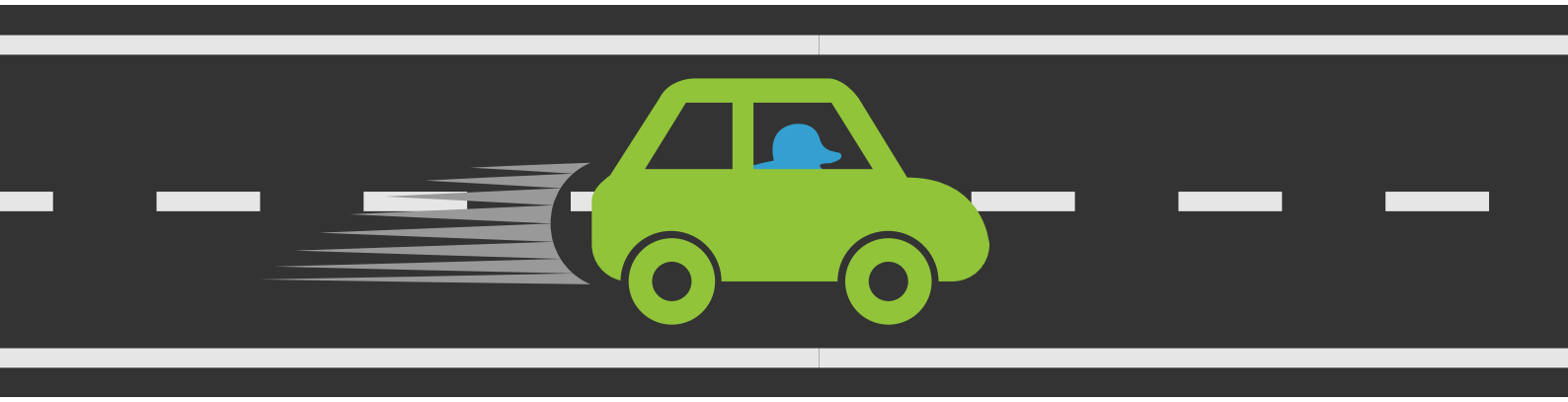
WISP Road Map

VALLEY TECHLOGIC

WISP@ValleyTechlogic.com

209-357-3121

111 Business Park Way,
Atwater CA 95301



Remote Access Policy

You will also need to set guidelines for remote access. They should outline how employees may access PII data remotely and policies should keep data security, confidentiality and regulatory expectations in mind.

Some suggestions include having a no-exceptions MFA policy for all of your users, as well as restricting employees to company owned devices only and setting work hours for access to company systems.

Connected Devices

Next, your firm will need to determine and set policy for how new devices and/or software is introduced to your network. All new devices, computers and servers must undergo a security review before being added to the network according to IRS guidance. This should include adding your firm's anti-virus and anti-malware software.

Software will need to be reviewed by your IT provider and should not be installed without their approval.

Reportable Incident Policy

A Incident Response Plan and Breach Notification Plan are both requirements of WISP. These policies should outline in detail what steps your firm will take in the event of a security breach including steps your firm will take to resecure your network.

These documents should also describe how your Data Security Coordinator will notify customers and outside agencies (insurance providers, law enforcement, stakeholders etc.).

Employee Code Of Conduct

It's important that your Employee Code of Conduct reflect the steps that you are taking towards implementing your WISP. You and your employees must be on the same page for WISP implementation to be successful.

Mandating security awareness training, guidelines for behavior and ensuring all new employees undergo a background check will ensure you are remaining compliant.

WISP Road Map

VALLEY TECHLOGIC

WISP@ValleyTechlogic.com

209-357-3121

111 Business Park Way,
Atwater CA 95301

Regulatory Risks

There are both regulatory and operational risks for CPA firms who do not implement a WISP. We'll first cover some of the regulatory risks which include:

- **FTC Safeguards Rule (under GLBA)**: The FTC clarified in 2022 that CPA firms are considered "financial institutions" under the Gramm-Leach-Bliley Act (GLBA) which requires a WISP, without one you can face civil penalties' of up to $50,120 per day.
- **IRS Publication 4557:** Requires tax preparers to implement a security plan (WISP). Failing to protect tax payer data can result in fines and could even result in being reported to your state licensing board.
- **CCPA/CPRA (California Consumer Privacy Act / California Privacy Rights Act)**: California CPA's must implement "reasonable security procedures". Failure to do so may result in fines of $2,500 per violation, or $7,500 per intentional violation.
- **AICPA Professional Standards:** ET Section 1.700 of AICPA states CPAs must not disclose confidential information without client consent. Failure to comply can result in a suspension or loss of your CPA license.

Operational Risks

There are also operational risks to consider when it comes to the benefits of implementing a WISP. Meeting compliance regulations may be a primary driver of your WISP journey but it should not be discounted just how much risk your firm will avoid by following these guidelines, including:

- **Financial Risk:** Fines are one thing, but a significant data breach can cost your firm big time - from the cost of recovery, audits, legal fees and more.
- **Business Disruption:** You may have a rough idea of how much it costs to operate your business, now multiply that cost by the time spent down during a security incident (which may be days, weeks or even months).
- **Reputational Risks:** What value do your customers hold for your business? Now imagine losing that value if news of a data breach causes them to take their business elsewhere.
- **Ethical Risks:** Without a proper WISP in place you may not be following advisable procedures that will keep you and your clients data safe. While this may not have a monetary cost it can speak to your firms capabilities to clients and shareholders.

WISP Road Map

WISP@ValleyTechlogic.com
209-357-3121
111 Business Park Way,
Atwater CA 95301

Implementation

Now that you have your ducks in the row when it comes to the preparation of your WISP, it's time to look towards implementation.

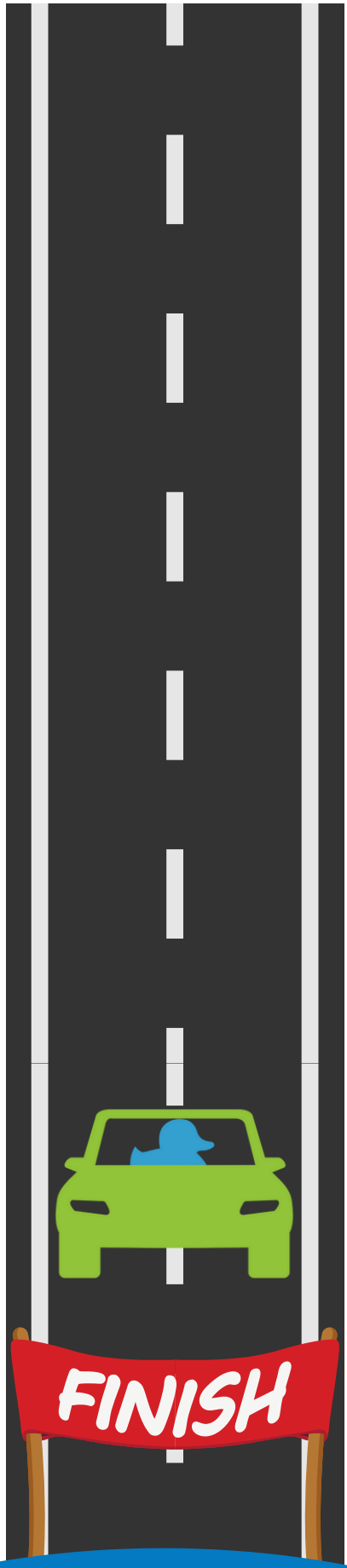
You will need to work with your IT provider to ensure that your WISP can be followed adequately and create what the IRS calls an "Implementation Clause".

Your implementation clause should include the date of implementation, your firm's name, acknowledgement that the firm follows GLBA and FTC Financial Privacy and Safeguards Rule. It will also need to make note of any state regulatory conditions you must follow (Ex: CCPA/CPRA California Consumer Privacy Act / California Privacy Rights Act).

Your Implementation clause will need to be signed and dated by the company owner, and the DSC.

It's important to note that you do not have extra time to complete these steps, GLBA went into effect June 9, 2023 and enforcement for firms failing to comply is already happening.

Compliance requirements are immediate and ongoing, do not wait to implement a WISP in your firm today to protect your business from future fines and threats.



Ancillary Documents

Once your WISP is in place you will need to save the documentation that relates to the policies you have set in motion, this will act as a record should regulatory bodies request proof of your compliance and also allow you to make changes without updating your entire WISP. If for example you make a change to your record retention policy you would update the supporting ancillary documentation to reflect that change.

Your IT provider will assist you with this documentation as well as provide guidance on how long to retain older records.

Need Assistance?

Schedule a free consultation today by visiting:

www.ValleyTechlogic.com/WISP-Consulation

Or by reaching out to directly to:

Ashton Fortuna,
Sales Engineer

Ashton@ValleyTechlogic.com

209-357-3121 Ext. 323