<COMPANY> DATA SECURITY PLAN

<AUTHOR OR DEPARTMENT>

Version 2020.1

Table of Contents

1. [Overview and Purpose 2](#_bookmark0)
2. [Company Description 2](#_bookmark1)
3. [Authorizing Official 2](#_bookmark2)
4. [Assignment of Security Responsibility 2](#_bookmark3)
5. [General System Description/Purpose 2](#_bookmark4)
6. [Related Laws/Regulations/Policies 2](#_bookmark5)
7. [System and Data Inventory 2](#_bookmark6)
8. [Risk Assessment and Mitigation 3](#_bookmark7)
9. [Security Awareness Training Program 3](#_bookmark8)
10. [Password and Account Requirements 4](#_bookmark9)
11. [Anti-Virus and Vulnerability Management Program 4](#_bookmark10)
12. [Data Security 4](#_bookmark11)
13. [Vendor Management 5](#_bookmark12)
14. [Information Disposal 5](#_bookmark13)
15. [Physical Security 5](#_bookmark14)
16. [Incident Response 5](#_bookmark15)
17. [Backups and Disaster Recovery Plan 5](#_bookmark16)
18. [Acceptable Use Policy 6](#_bookmark17)
19. [Updates to the Plan 6](#_bookmark18)
20. [Revision History 6](#_bookmark19)

[Appendix A. Risk Register 7](#_bookmark20)

[Appendix B. Acceptable Use Policy 8](#_bookmark21)

## Overview and Purpose

The objective of the Data Security Plan (DSP) is to document the protection of the data and systems within the organization’s scope. The purpose of the data security plan is to provide an overview of the security requirements of the systems and describe the controls that have been implemented or plan to be implemented to comply with IRS regulations. Senior management will authorize the system to operate based on the assessment of the management, technical and operational controls.

## Company Description

<Company name and description and location>.

## Authorizing Official

<Name>, <Title>, <Company>, <Address>, <Phone>, <email address> is the designated authorizing official of the <Company> systems.

## Assignment of Security Responsibility

<Name>, <Title>, <Company>, <Address>, <Phone>, <email address>

## General System Description/Purpose

System functions to provide tax preparers the ability to prepare taxpayer’s tax

forms in a safe and efficient manner. System is also configured to keep the

client’s data protected in accordance with IRS Regulations.

## Related Laws/Regulations/Policies

System(s) must comply with IRS regulations for the confidentiality, integrity and availability of the data which is contained within the system(s).

## System and Data Inventory

Below is the inventory of the systems and where the data is stored and the type of information which is stored on the system.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **System Description (name, make, model, serial number, or other identifying information)** | **Location (where the data is stored)** | **Type of Information stored or processed (Public, PII, etc.)** | **Quantity** | **Connected to the Internet Y/N** |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **System Description (name, make, model, serial number, or other identifying information)** | **Location (where the data is stored)** | **Type of Information stored or processed (Public, PII, etc.)** | **Quantity** | **Connected to the Internet Y/N** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Risk Assessment and Mitigation

Risk is based on whether the integrity or availability of the data changed as well as whether possible disclosure of information could cause harm to our business or customers. Please view the Risk Register located in Appendix A for a list of risks which were assessed.

Risk is mitigated by many of the following administrative and technical controls which are put in place. Administrative controls include security awareness training, least privilege, information disposal, vulnerability management and Acceptable Use Policy. Technical controls include access control for accounts, data backups and security controls for protecting data.

## Security Awareness Training Program

Employees are required to complete security awareness training upon hire. The training helps employees to identify potential phishing emails, how to identify PII, and how to protect PII as well as how to recognize trick and techniques hackers may use to harm employees or the organization.

## Password and Account Requirements

All user accounts will be required to be at least 8 characters long. It is recommended that the systems be setup to allow up to 64-character passwords to allow people to set a passphrase since this has shown to be more secure and less likely of someone forgetting. If only requiring an 8-character password then it will need to be complex which also requires capital letters, numbers, and special characters and it will need to be changed every 90 days. It is highly recommended to have personnel select a passphrase of at least 14 characters long. It is a best practice to also utilize Multi-Factor Authentication (MFA) when available.

Administrative or privilege accounts will be required to be a minimum of 14 characters and be required to change every 60 days. Administrative accounts will also be required to use MFA if available.

Systems will be set to lock an account after 3 failed login attempts. Doing so helps to mitigate the risk of someone trying to brute force a password.

Accounts are setup to have least privilege required to perform work. Only administrator/privilege accounts are given to those with a need to know to perform their job function.

When an employee is no longer employed accounts and access to the building will be removed within <#> days.

## Anti-Virus and Vulnerability Management Program

<Company> has <name> anti-virus installed on all systems and it is set to automatically update when a new virus definition is released. Systems are set to automatically install updates when they are released. Applications that are used on the systems are set to automatically update and/or the system administrator receives email updates when a new version is available for download. Anti-virus will be checked at least weekly to ensure systems are being updated accordingly. Systems and applications will be checked at least monthly to ensure updates have been installed if applicable.

## Data Security

Data that contains customer data that is considered PII will always be encrypted this includes data at rest. This also includes if an email is to be sent with PII it will be sent encrypted.

All devices and papers which include customer data or PII will be kept in a secure location and will be restricted to only authorized personnel.

## Vendor Management

Before entering a contract or sharing data with a vendor, the vendor will be assessed as to whether they have the proper security controls in place to protect the type of data that will be shared or stored. Also, contract language will include at a minimum that the vendor is required to contact <Your Company> within 72 hours if there has been a breach which involved our data or customer data. The contract also states that the vendor is required to keep the security controls at the current level or above in place to protect the data.

## Information Disposal

Systems which process or transmit PII will follow the latest NIST Special Publication 800-88 of Guidelines for Media Sanitization for clearing, purging, or destroying the devices. This guideline will also be followed for disposing of hard copy information which has PII or customer data on it, such as using a cross-cut shredder.

## Physical Security

The building is controlled by lock and key and only <List Individual(s) who have key access> maintain key access to the facility. The facility also has an alarm and <individual and/or police station> will be notified once alarm goes off.

## Incident Response

Tax practitioners need to report the loss or theft of taxpayer data immediately to their IRS Stakeholder Liaison, <List name and phone and/or email here>. This will help to ensure that appropriate precautions can be made to protect clients from fraudulent returns possibly being filed in their names. The IRS Stakeholder Liaison can also assist in the recovery efforts to include getting a new EFIN if required.

## Backups and Disaster Recovery Plan

Critical data will be backed up on a <daily/weekly> basis to <list of location or system where data is backed up>. It is recommended that the business have a Disaster Recovery Plan (DRP) in the event a disaster strikes to detail how the

business will recover from the disaster and provide a plan as to how to provide services for the customers. This is especially important if your business is in an area that is affected by possible hurricanes or tornadoes.

## Acceptable Use Policy

Employees are required to review and sign an acceptable use policy upon hire. The acceptable use policy will outline the rules of behavior for employees on the company’s IT provided resources and the company’s data that resides on the assets. (Template provided in Appendix B)

## Updates to the Plan

This plan will be reviewed annually or as changes are made to the environment. The <Title of Authorizing Official or the Person with Security Responsibility> will be the final approving authority for changes made to the plan.

## Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision #** | **Date of Change** | **Approved By** | **Summary of Change** |
|  |  |  |  |
|  |  |  |  |

# Appendix A. Risk Register

(These are a list of some examples of possible risk to your organization, please add any additional items that relate to your organization)

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk Description** | **Likelihood of Risk Occurring** | **Impact if Risk Occurs** | **Mitigating Action** |
| Disclosure of PII | Medium | High | Data is encrypted |
| Ransomware | Low | High | Security Awareness Training is required and Critical Data is backed up regularly |
| Malware | Medium | Medium | Vulnerability Management program is in place and Anti- Virus is up to date |
| Unauthorized Access | Low | High | Least privilege is used on systems |
| Phishing | Medium | Medium | Security awareness training and ensure anti-virus is up to date |
| Preparer leaves company with taxpayer data on personal devices | Medium | High | Only allow taxpayer data to be entered and stored on company devices, terminate access to taxpayer information for anyone who is no longer employed |
| Public Wi-Fi | Medium | Medium | Only use trusted networks; when unable ensure VPN service is in use |

|  |  |  |  |
| --- | --- | --- | --- |
| **Key** | High | Medium | Low |

OVERVIEW

# Appendix B. Acceptable Use Policy

This document shall serve to outline what is determined as <**Company Name**> defined rules of behavior and acceptable use of <**Company Name**> resources. If an employee/contractor has further questions about this policy, they shall contact HR/Management for more information.

RULES OF BEHAVIOR

These rules of behavior apply to the use of **<Company>-provided IT resources and <Company> data**, regardless of the geographic location:

* Data and system use must comply with <Company> policies and standards.
* Unauthorized access to data and/or systems is prohibited.
* Users must prevent unauthorized disclosure or modification of sensitive information, including

Personally Identifiable Information (PII).

### ACCEPTABLE USE

#### Users shall:

* In accordance with organizational procedures, immediately report all lost or stolen equipment, known or suspected security incidents, known or suspected security policy violations or compromises, or suspicious activity to the <**Name of Department**>. Known or suspected security incidents are inclusive of an actual or potential loss of control or compromise, whether intentional or unintentional, of authenticator, password, or sensitive information, including PII, maintained or in possession of the user.
* Log-off or lock systems when leaving them unattended.
* Complete security awareness training in accordance with the <**Company**> requirements.
* Permit only authorized users to use organization-provided systems.
* Secure sensitive information (on paper and in electronic formats) when left unattended.
* Keep sensitive information out of sight when visitors are present.
* Sanitize or destroy electronic media and papers that contain sensitive data when no longer needed, in accordance with organization records management and sanitization policies, or as otherwise directed by management.
* Only access sensitive information necessary to perform job functions (e.g., need to know).
* Use PII only for the purposes for which it was collected, to include conditions set forth by stated privacy notices and published notices.
* Ensure storing of PII is only done in approved locations and is marked accordingly.
* Ensure the accuracy, relevance, timeliness, and completeness of PII, as is reasonably necessary.
* *Wear organization-issued identification badges where they are always visible in organization-operated facilities.* (**If this applies to your organization**)
* Only use USB storage devices that have received written approval.
* Only store business data in approved locations **(*Give example of approved locations*)**

### PROHIBITED USE

#### Users shall not:

* Download or install software without approval from IT department and/or management.
* Remove, disable, or alter any software installed by IT from their device unless given explicit permission in writing.
* Use personal email for business-related activities.
* Use personal accounts or personal computers for storing any company data.
* Connect unapproved devices to the corporate network.
* Direct or encourage others to violate organizational policies, procedures, standards, or guidelines. Circumvent security safeguards or reconfigure systems except as authorized (e.g., violation of least privilege).
* Use another user’s account, identity, or password.
* Share their own password with another user.
* Exceed authorized access to sensitive information.
* Cause congestion, delay, or disruption of service to any organization-owned IT resource. For example, greeting cards, video, sound, or other large file attachments can degrade the performance of the entire network, as does some use of “push” technology, such as audio and video streaming from the Internet.
* Create, download, view, store, copy or transmit materials related to sexually explicit or sexually

oriented materials.

* Create, download, view, store, copy or transmit materials related to gambling, illegal weapons,

terrorist activities, illegal activities or activities otherwise prohibited.

* Store sensitive information in public folders or other insecure physical or electronic storage locations.
* Share sensitive information, except as authorized and with formal agreements that ensure third

parties will adequately protect it.

* Transport, transfer, email, remotely access, or download sensitive information, inclusive of PII, unless

such action is explicitly permitted by the manager or owner.

* Store sensitive information on mobile devices such as laptops, smart phones, USB flash drives, or on remote systems without authorization.
* Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information for

personal use for self or others.

* Engage in “for-profit” activities or in support of other outside employment or business activity (e.g., such as consulting for pay, administration of business transactions, sale of goods or services, etc.) while using <Company> provided assets unless explicitly approved.
* Engage in any outside fund-raising activity, including non-profit activities, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity while using <Company> provided assets unless explicitly approved.
* Establish unauthorized personal, commercial, or non-profit organizational web pages on organization- provided systems.
* Use organization-owned IT resources as a staging ground or platform to gain unauthorized access to other systems.
* Create, copy, transmit, or retransmit chain letters or other unauthorized mass mailings regardless of

the subject matter.

* Engage in activities that are inappropriate or offensive to fellow employees/contractors or the public. Such activities include, but are not limited to hate speech, harassment, bullying, intimidation or other abusive conduct that ridicules others on the basis of race, creed, religion, color, age, sex, disability, national origin, or sexual orientation, etc.
* Add personal IT resources to existing organization-owned systems without the appropriate authorization from IT and/or Management.
* Intentionally acquire, use, reproduce, transmit, or distribute any controlled information including computer software and data that includes information subject to the Privacy Act, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.
* Send anonymous messages.
* Remove organization-provided IT resources from organization property without prior management authorization.
* Post information to external blogs, social networking sites, newsgroups, bulletin boards or other public forums which is/are: Derogatory to <**Company**> or its management; Contrary to <**Company**> mission or stated positions; or brings discredit or embarrassment to <**Company**>.
* Configure/enable personal Wi-Fi hotspots while in vicinity of the <**Company**> premises.
* Auto-forward email from a <**Company>** address to a personal email address. Additionally, employees/contractors shall not auto-forward email from a personal email address to a

<**Company**>address.

If you would like to review a copy of this policy, you may request so through Human Resources and/or Management.

### NON-COMPLIANCE

Failure to comply with this policy may result appropriate disciplinary/corrective actions which may include termination of employment.

REVISION HISTORY

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date of Change | Responsible | Summary |
|  |  |  |  |
|  |  |  |  |

### Acknowledgement Statement

I, , acknowledge that I have read and fully understand the information set

forth in <Company’s> ***Acceptable Use Policy*** and agree to comply with the requirements stated in said policy. I also understand that by demonstrating noncompliance with said policy, I shall be subject to all disciplinary or legal actions enacted by <Company>.

Printed Name

Signed Name Date