Jean B. DeWitt, CPA LLC
Cyber Security/Data Protection Policy

This plan was established and approved by **Jean B. DeWitt, CPA** on **February 7, 2020**. The Plan will be reviewed and updated, as applicable, at least once per year.

Table of revision history

Version	Date	Details of change	Issued by
1.0	02/07/2020	Initial Version	Jean B. DeWitt

Policy brief & purpose

For my client's protection, as well as the reputation of my firm, my Cyber Security/Data Protection Policy refers to our commitment to treat information of clients, employees (if applicable), stakeholders and other interested parties with the utmost care and confidentiality.

With this policy I ensure that we gather, store, and handle data fairly, transparently and with respect to individual rights.

Scope

This policy applies to all parties (clients, employees, contractors, suppliers, volunteers, etc.) who process, store, transmit, or have access to sensitive information including personal information (PI) or other confidential information (CI). This policy applies to both electronic and non-electronic information. Generally, my policy applies to anyone we collaborate with or acts on our behalf and may need occasional access to data.

Policy elements

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, birth dates, usernames and passwords, digital footprints, social security numbers, driver's license information, financial data, photographs, etc.

My firm collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Jean B. DeWitt, CPA LLC
Cyber Security/Data Protection Policy

Our data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only
- Processed by my firm within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties.

Our data will not be:

- Communicated informally
- Stored for more than a specified/required amount of time
- Transferred to individuals, organizations, etc. that do not have adequate data protection policies in place
- Distributed to any party other than any agreed upon by the data's owner (exempting legitimate requests from the IRS or other law enforcement authorities).

In addition to ways of handling data, my firm has direct obligations towards the people to whom the data belongs. Specifically, we must:

- Let people know which of their data is collected
- Inform people about how we will process their data
- Inform people regarding who has access to their information
- Implement protections in case of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases.

To exercise data protection my firm is committed to:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees (if applicable) in online privacy and security measures
- Build secure networks to protect online data from cyber attacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish proper/adequate data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization, regular password changes, etc.).

If applicable, remote employees must also follow this policy's instructions.

My data protection provisions will appear on my website.

Jean B. DeWitt, CPA LLC
Cyber Security/Data Protection Policy

Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possible legal action.

Appendix – Specific Policy Provisions

Protecting personal and company devices

When we use digital devices to access company emails or accounts, this introduces security risk to our data. We keep personal and company issued computers, tablets and/or cell phones secure. We do this by:

- Keeping all devices password protected.
- Deploying a complete/comprehensive and current antivirus software package.
- Utilizing a third party to provide internet security software and services.
- Ensuring that devices are not left exposed or unattended.
- Installing security updates of browsers and systems monthly or as soon as updates are available.
- Logging into company accounts and systems through secure networks only.

We also avoid accessing internal systems and accounts from other people's devices or lending devices to others.

Keeping emails safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing").
- Be suspicious of clickbait titles (e.g. offering prizes, advice).
- Check email and names of people from whom a message has been received to ensure their legitimacy.
- Look for inconsistencies or giveaways (e.g. grammar and spelling mistakes, capital letters, excessive number of exclamation marks).

Jean B. DeWitt, CPA LLC
Cyber Security/Data Protection Policy

Appendix – Specific Policy Provisions (Continued)

Managing passwords properly

Password leaks are dangerous since they can compromise my entire infrastructure. Not only should passwords be secure so they can't be easily hacked, but they should also remain secret. For this reason, we:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays).
- Remember passwords instead of writing them down.
- Change passwords every two months.

Transferring data securely

Transferring data introduces security risk. I/we:

- Avoid transferring sensitive data (e.g. client information, employee records) to other devices or accounts unless necessary.
- Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts.