AccuExchange Policies Regarding the Use of USB Drives

and

Removable Media

Vince Kelly

Jason Mays

Duy Nguyen

Pascal Allison

Table of Contents

- Overview
- Rationale for Restricting USB use
- Scope – Who & What Policies Apply
- Compliance – Who is Responsible & What Are They Responsible For?
  - Individual User Responsibilities
  - Office Administrator Responsibilities
  - Security Organization Responsibilities
  - Audit Organization Responsibilities
  - Manager & HR Responsibilities
- Technical Controls & Inappropriate USB Use
- Supporting Documents
  - FinCEN, Federal, and State Government Guidelines
  - National Institute of Standards and Technology (NIST)
- Information Classification and Impact Assessment Model
- Appendix A
  - AccuExchange Approved Standard USB Drive & Encryption Software Details
- Appendix B
  - CryptArchiver Encryption Software Details
  - WinEncrypt USB Drive and CryptArchiver Software Directions for Use

AccuExchange Policies Regarding the Use of USB Drives

Overview

As a world leader in virtual currency exchange, AccuExchange is committed to providing the most secure and stable trading platform in the industry.

With this in mind, AccuExchange board of directors and senior management have approved policies regarding the use of USB removable media which are outlined in this document.

The Rationale for Restricting USB Use

In general, AccuExchange bans the use of removable media including, but not limited to:

- Writable CD and DVD devices
- SD memory cards
- PDA devices
- Mobile phone technology as a data storage and data exchange medium.

While it is widely recognized that banning the occasional use of USB removable media in the course of business activities is impractical, it is also clear that inappropriate use of USB devices do pose a potentially serious threat to AccuExchange. There have been numerous examples in the financial services community where USB devices were used to infiltrate and collect extremely sensitive company information as well as to propagate software like malware and spyware. This, in turn, resulted in severe fines and penalties as well as exposure to legal liabilities and lawsuits for negligence, loss of customer confidence and trust, etc.

Document Scope - Who and What These Policies Apply To

The policies contained in this document are effective immediately and will remain permanently in force subject to annual review. These policies apply without exception to all employees, partners or any individual with physical or remote access to AccuExchange facilities or computing infrastructure within the US and the United Kingdom.

The Context and Purpose of These Policies

AccuExchange Management Goals and Intentions

The policies outlined in this document are components of AccuEchange’s overall security architecture and management directives and should be regarded in that context.

The board of directors and management of AccuExchange have outlined the following goals and intentions regarding the AccuExchange security architecture in general and the use of USB removable media specifically:

1. To protect AccuExchange stakeholders, company assets, intellectual property and proprietary information.
2. To facilitate a safe, appropriate and inclusive work environment for all AccuExchange employees, trading partners and customers.
3. To comply wherever possible with all standards, laws, and restrictions that are applicable and considered reasonable within the financial services industry.
4. To curtail or eliminate risks associated with the introduction or propagation of any form of inappropriate software or data including; malware, viruses, illegally obtained AccuExchange or competitor proprietary software, data or information.
5. To prevent any form of inappropriate disclosure, manipulation, leak or breach of sensitive personal, customer, or non-public company information.

Compliance - Who is Responsible and What They Are Responsible For

It is the responsibility of all employees, partners, consultants, contractors or anyone who conducts business with AccuExchange to understand and comply with these policies. Failure to adhere to these policies or any other AccuExchange security policy will, at the discretion of the employee's manager, result in immediate dismissal, forfeiture of the annual company performance bonus or both.

Individual User Responsibilities:

1. Individuals must not use USB drives for anything other than appropriate and proper AccuExchange business activities as outlined in the "Inappropriate Use of USB Drive" section of this document.
2. Attend mandatory training conducted for all employees to make users aware of the risks that removable media impose on our internal networks and systems
3. Individuals may only use AccuExchange approved WinEncrypt CryptArchiver encrypted USB drives that are obtained from the AccuExchange office administrator (the OA).
4. All USB drives must remain on-site at the AccuExchange facility from which it was obtained and must never leave the premises under any circumstances.
5. Users who have signed for a USB device may not 'loan' or give the device to anyone else at any time.
6. Users must keep USB drives in their possession or in a locked desk drawer when not in use.
7. Any missing or misplaced USB drives must be reported to the OA immediately. The OA, security organization and the individual involved will conduct a reasonable search for the USB. The individual user will provide,(to the best of their ability), a detailed accounting of what information was contained on the drive before it was lost.
8. Users must back up the entire USB to the company data repository after each use.
9. Users must use the AccuExchange approved "Crash Plan 42" backup software for backing up all USB drives.
10. Users must return all non-functional USB drives to the OA for proper destruction.

OA Administrative Responsibilities:

1. Attend mandatory training conducted for all employees to make users aware of the risks associated with USB use.
2. Attend mandatory technical training for OA's on USB drives
3. The OA is responsible for acquiring, properly labeling, managing, accounting for and destroying all USB devices.
4. The OA is responsible to keep all unused USB drives in a secure location which is only accessible by the OA, head of security, head of the audit and the CIO
5. All USB drives must be formally accounted for and reported by the OA once per quarter.
6. The OA will report lost USB drives to the individual's immediate manager, audit and security organizations and provide the serial number of the lost device, the circumstances of how it was lost as well as the information that it contained when it was lost.
7. Each USB device must be signed for by the user and properly recorded by the OA. It is the responsibility of the OA to maintain an audit trail of the location and current user of all USB devices at all times.
8. All USB drives must be assigned serial numbers by the OA that are recorded on the USB internal volume headers. These drives are also to be labeled with bright orange stickers by the OA,(so that they are clearly visible).
9. The OA must also ensure that all drives are formatted as non-bootable and that all drives are fully encrypted at all times using industry standard 256 bit AES encryption.
10. USB drives must not contain autorun, autoplay or any other automatic command execution programs or utilities.
11. The OA is responsible to ensure that any defective or non-functional USB drive is properly destroyed – e.g., properly demagnetized, physically unusable, etc. before being sent to the e-waste
12. The OA must ensure, to the best of their ability that the contents of USB drives contain appropriate AccuExchange related business information as outlined in the "Inappropriate Use of USB Drive" section of this document.

Security Organizations Responsibilities:

1. The AccuExchange security organization is responsible to ensure that physical conformance to policy is followed. This includes:
   - Ensuring that USB drives are not left unattended
   - Ensuring that USB drives are not removed from the facilities
   - Ensuring that no other removable media outside of USB devices are being used
   - Performing spot checks to ensure compliance and that drives contain appropriate content to the best of their ability as outlined in the “Inappropriate Use of USB Drive” section of this document
2. Any breach of policy – e.g., unattended USB drives, USB drives taken off-site by an individual, etc. must be documented and reported immediately to both the individual’s manager and the audit organization.

Audit Organization Responsibilities:

1. AccuExchange internal audit organization is responsible to ensure that proper tracking and audit logs are being maintained and that all physical, technical and administrative controls are in place and being followed.
2. The head of the audit organization will provide quarterly reports to the CIO of all USB activities with particular attention paid to lost devices (the loss circumstances, what information was on the drives, the frequency of losses, etc.)

Manager and Human Resources Enforcement Responsibilities:

1. Immediately convene an in-person meeting with the employee to understand the situation from their perspective
2. Convene a meeting between the manager and HR to determine if termination proceedings should commence.
3. If termination of the employee is deemed inappropriate by the manager and HR, documentation of the incident is to be made part of the employee's permanent file.
4. The employee is to be informed in writing that they will be required to forego the company performance bonus for the year.
5. It is the manager's responsibility to ensure that no other removable media outside of USB devices are being used by their individual contributors

Technical Controls and Inappropriate Use of USB Drives

1. Individuals must not use USB drives for anything other than appropriate and proper AccuExchange business activities.
2. WinEncrypt USB drive with CryptArchiver encryption software is the only approved standard for USB drives and encryption.
3. Unapproved USB drives or encryption software from any non-AccuExchange individual or company is not permitted in any AccuExchange facilities and may not be used with any AccuExchange asset at any time. Failure to comply with this directive will result in immediate confiscation of the device.
4. The OA is the only person permitted to reformat USB drives.
5. Individuals are not permitted to place any form, of executable code or automatic command execution files on AccuExchange USB drives.
6. USB labels and volume serial numbers may not be tampered with or removed.
7. The following information is not permitted to be stored on any AccuExchange USB drive:
    - Copyrighted material of any kind
    - Company proprietary or non-company proprietary information of any kind.
    - Illegally obtained source or executable software, files, data or content of any kind.
    - Music, pictures, recordings, videos or any information of a personal nature
    - USB thumb drives are not permitted to be used as storage devices for any file sharing, peer-to-peer or bit torrent content of any kind.
    - Downloading and storing files from the Internet

Supporting Documents and Data Classification

The purpose of this section is to outline the following processes, technology standards, procedures, guidelines, related policies and information classification models that were relied upon to create this document. The overall objective is to ensure the confidentiality and integrity of client and business data of AccuExchange and the prevention of deliberate or inadvertent manipulation or removal of data from AccuExchange's systems or infrastructure. Policies for memory drive usage will also be defined but not limited to the below:

- Information **Confidentiality** entails that all sensitive data and documentation are stored in compliance with Gramm-Leach-Bliley Act (GLBA)* standards.
- Information **Availability** entails that all sensitive data and documentation access are restricted based on OMB Memorandum M-06-16** standards.
- Information **Integrity** ensures that only authorized employees with proper security access will have access to appropriate data classified below.
- Client privacy entails only AccuExchange employees with work-related interest are authorized to access client's data and documents for the sole purpose of job function.

**Gramm-Leach-Bliley Act (GLBA). GLBA requires financial institutions to protect their customers' information against security threats. This includes ensuring "the security and confidentiality of customer records and information" and protecting "against unauthorized access to or use of such records or information". (Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices)*

***OMB Memorandum M-06-16. OMB M-06-16 addresses the protection of agency information that is either "accessed remotely or physically transported outside of the agency's secured, physical perimeter". It specifically requires that agencies encrypt all data stored on mobile computing devices, such as laptops and PDAs, unless the data has been determined by the designated agency official to be non-sensitive.6 Similar requirements are also included in OMB Memorandum M-07-16.7 (Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices)*

FinCEN, Federal & State Government Guidelines

Fin-2014-R002

Application of FinCEN’s Regulations to Virtual Currency Software Development and Certain Investment Activity

FIN-2013-G001

Application of FinCENs Regulations to Persons Administrating, Exchanging or Using Virtual Currencies

Division of Consumer Services (DCS)

Interim Regulatory Guidance on Virtual Currency Activities

Washington Uniform Money Services Act, chapter 19.230 RCW

FISMA, 44 U.S.C. § 3541

Federal Information Security Management Act (FISMA) 2002

The US and European Guidelines

Organization for Economic Cooperation and Development (OECD)

Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data

National Institute of Standards Special Publication Documents

NIST SP 800-111

Guide to Storage Encrypted Technologies for End User Devices

NIST SP 800-122

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

NIST SP 800-175B

Guideline for Using Cryptographic Standards in the Federal Government

NIST SP 800-60

Guide for Mapping Types of Information and Information Systems to Security Categories

NIST SP 800-100

Information Security Handbook: A Guide for Managers

NIST FIPS PUB 199

Standards for Security Categorization of Federal Information & Information Systems

Information Classification and Impact Assessment Model

I. Data Classification
   a. Public: Information published and shared
   b. Internal: Information is confidential and protected, may be shared with only essential organizational personnel.
   c. Restricted: Information is highly confidential and protected, access is granted to only the highest level of security.

II. Impact Level
   a. Low: No financial loss or legal liability resulting from exposure or improper use.
   b. Medium: Exposure may lead to limited legal liability, loss of customer trust or financial loss.
   c. High: Exposure or misuse could result in catastrophic fines and legal liability, loss of customer trust or financial losses.

Data Classification	***Impact Level***	***Description***	***Data***
Public	N/A	Information that has low impact and accessible by anyone	• Organizational name • Organization Address
Internal (Confidential)	Medium	Information that has a medium impact and only accessible by organizational personnel. Exposure of information may lead to legal liabilities, financial loss, and loss of client's trust.	• Organization data • Budgetary information • Departmental information • Proprietary data • Client's information o Tax Identification # o Contractual Information o Intellectual property o Financial data
Restricted (Confidential)	High	Information that has a high impact level and is only accessible by organizational personnel with highest security authorization. Exposure of information may lead to significate legal liabilities, financial loss, and loss of client's trust.	• Organizational salary information • HR Personnel Information o Social Security # o Driver's License # o Home Address o Biometric data o Health information o Benefits information o Contact information o Bank information o Employee Identification #

APPENDIX A

AccuExchange Approved Standard for USB Drives

WinEncrypt USB Drive with CryptArchiver Software

The WinEncrypt USB Drive with CryptArchiver encryption software has been designated as the standard USB Drive for AccuExchange. This drive provides the following features:

- Easy to use

Unbreakable Encryption has never been this easy! Just plug in your pen drive, enter your password and drag-and-drop your important files into the vault.

- Strong Encryption

Extremely strong encryption algorithms surpass U.S. Government standards for data security. Up to 448-Bit Blowfish and 256-bit AES ciphers provide sufficient protection for businesses as well as personal use.

- Installs on your removable drive

The Traveler Edition is portable and installs directly to your USB drive. You do not need the software installed on any computer to access your data. Just plug in your USB drive to any computer, and you're set.

- Protects Any File

- Easy to hide

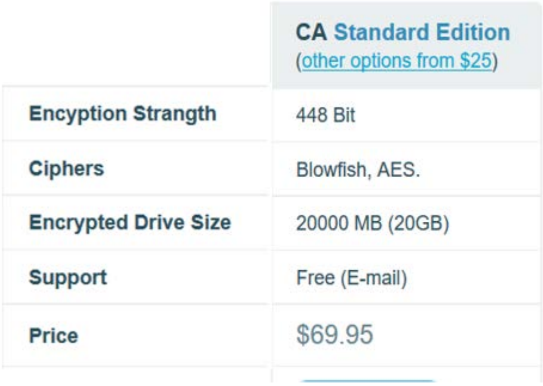
Creates encrypted vaults, within which your files are stored. When you are not using a vault, your data is absolutely hidden. No tell-tale filenames or individual files left behind to steal. You can even install programs secretly to your encrypted drive.

- One password for one vault

You don't have to store each file separately or enter your password repeatedly. Your password unlocks your vault, allowing you direct access to your files when needed. Once you lock your vault, everything in the vault is encrypted and invisible.

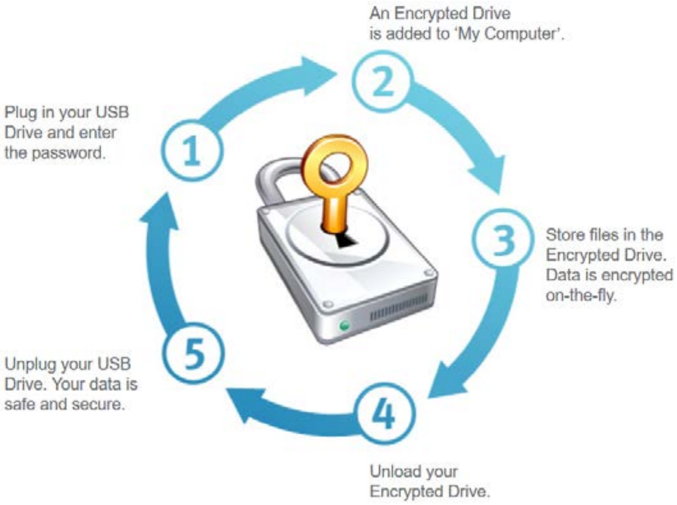
APPENDIX B

CryptArchiver Software Details



	CA Standard Edition (other options from $25)
Encyption Strangth	448 Bit
Ciphers	Blowfish, AES.
Encrypted Drive Size	20000 MB (20GB)
Support	Free (E-mail)
Price	$69.95

WinEncrypt Drive and CryptArchiver Directions For Use



1 Plug in your USB Drive and enter the password.

2 An Encrypted Drive is added to 'My Computer'.

3 Store files in the Encrypted Drive. Data is encrypted on-the-fly.

4 Unload your Encrypted Drive.

5 Unplug your USB Drive. Your data is safe and secure.