Estate Valuations & Pricing Systems, Inc.
Information Security Policy

Overview

It is EVP Systems policy to follow industry-standard best practices for information security. All employees of EVP Systems must be familiar with and adhere to the following Information Security Policy.

Under no circumstances should any EVP Systems employee, system or database accept, manipulate or store any confidential client information, including personally identifiable information (PII). If an employee comes into contact with client PII, an Awareness Notice must be filed immediately.

Computer Systems

EVP Systems uses Microsoft Windows 10 for its desktop and laptop computers, and Canonical Ubuntu 20.04 for its servers. All systems owned by EVP Systems are for corporate-related uses only.

Accounts

All employees have a single, unique account on Windows, controlled through Azure ActiveDirectory. Relevant permissions are granted on an as-needed basis depending on duties, and all accounts are revocable and resettable as needed. A login audit trail is maintained by ActiveDirectory.

Certain technical employees have a single, unique account on Ubuntu, on the development server only. Access is granted on an as-needed basis depending on duties. A login audit trail is maintained by Ubuntu.

There are also two role-based ActiveDirectory accounts, `admin` and `it`. The `admin` account is a global administrator with full access to all Windows-based services, and is accessible only to senior company management. The `it` account is a local administrator and is accessible to EVP Systems' IT Department, for the installation and maintenance of Windows machines.

There are two system-level Ubuntu accounts as well, `root` and `ubuntu`. `root` is the required super-user on Linux systems, and access to it is not granted. `ubuntu` is the default user for Canonical Ubuntu, and it is the only account available on production systems.

Passwords

At EVP Systems, Windows passwords require ten characters, and at least one instance each of lowercase letters, capital letters, numerals, or special characters like punctuation. This requirement is enforced by ActiveDirectory. Normal access to Windows accounts is via a Windows Hello-defined PIN.

The role-based Windows accounts use closely held passwords, known to members of senior management and the IT Department.

Ubuntu passwords require ten characters, and three of either lowercase letters, capital letters, numerals, or special characters like punctuation. This requirement is enforced by `pam_cracklib`.

The `ubuntu` role-based Ubuntu account is accessed through a PEM file, implemented PKI. The `root` role-based Ubuntu account is accessed through elevating permissions of the `ubuntu` account via the `su` command.

Passwords are changed during annual workstation re-imaging, but not between, based on FTC guidance: `https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes`.

Third-Party Systems

EVP Systems uses several third-party systems in the course of its business. Access to all third-party systems is conducted using SSL-protected connections.

Google Workspace (formerly G Suite, formerly Google for Work) is used for e-mail, calendaring, contact management, and shared document creation. Unique accounts per user are maintained through the Google Workspace administrative console, and are revocable and resettable on administrative demand. Passwords are required to be ten characters at minimum, and password complexity must be “green” as measured by the Google Workspace password monitoring tool. Senior members of EVP Systems management have administrative access.

Dropbox Business is used for file-sharing. Unique accounts per user are maintained through the Dropbox Business dashboard, and are revocable and resettable on administrative demand. Passwords are required to be “Very Strong” as measured by the Dropbox Business password control setting. Senior members of EVP Systems management have administrative access.

Azure ActiveDirectory is used for Windows account management, and Microsoft OneDrive for Business is used to share OneNote for Business notebooks. Both use Windows accounts for access, as defined above.

Slack is used for intra-company communication and task planning, and accounts are created with company-provided and controlled e-mail accounts, for each employee.

Amazon Web Services (cloud compute services), Github (source code control), Papertrail (logging), rsync.net (offsite backup) and Uptime Robot (external site monitoring) use service-specific accounts, with distinct passwords. They are accessible only to members of EVP senior management.

Session Locking

When a computer has been left inactive for longer than fifteen minutes, a screensaver begins, blanking the screen and locking the session. The user must re-enter their password or PIN to regain access.

Mass Storage Devices

Mass storage devices (such as burnable CDs or DVDs, or USB thumb drives) are disabled on all EVP Systems workstations.

Remote Access and Telecommuting

Remote, off-site access to EVP Systems resources and data (including via third-party services) is discouraged, but if required, it is conducted using the same accounts and control as on-site access. EVP Systems does not allow telecommuting.

(During the COVID-19 pandemic, EVP Systems staff used their company-provided workstations at home, maintaining all the same security precautions as when in the office.)

Updates

All Windows computers at EVP Systems have updates and security patches applied by the standard Windows Update process weekly. In an emergency or under specific circumstances, the process will be triggered manually on an as-needed basis by the local administrator account, `it`. Individual applications not compatible with Windows Update are updated during company-wide upgrade cycles, or after notice from the vendor of security issues.

All Ubuntu servers are updated nightly with vendor-provided upgrades, via an automatic process driven by `cron`. In an emergency or under specific circumstances, the process will be triggered manually on an as-needed basis by the local administrator account, `root`.

Third-party services are expected to update their own systems in a timely and consistent manner.

Viruses and Rootkits

All Windows computers at EVP Systems run Windows Defender antivirus, and its virus signatures are updated nightly. In an emergency, the process can be triggered manually on demand.

All Ubuntu servers at EVP Systems run `rkhunter` to detect rootkits, and its kit signatures are updated with system upgrades. In an emergency, the process can be triggered manually on demand.

Third-party services are expected to maintain their own defenses against viruses and rootkits.

Please see “Intrusion Detection and Audit Process” for further details.

Monitoring

Please see “Intrusion Detection and Audit Process.”

Backup

It is EVP Systems policy to store all but temporary files used on Windows machines in Dropbox, which provides both off-site backup, restoration, and versioning. All files on Windows computers not stored on Dropbox are not backed up. Dropbox retains each version of each file indefinitely.

Shared documents, such as company procedures and policies, are stored in Google Drive. Google Drive retains each version of each document indefinitely.

The Ubuntu servers hosted at Amazon Web Services all use EBS-based boot volumes, which are automatically replicated across AWS Availability Zones. The databases have RDS snapshots taken nightly, with two days of history kept.

The servers also share an AWS EFS file system that is rsync’d to rsync.net (a backup service not hosted on AWS) nightly. Before this process, all AWS databases are dumped to the file system, with daily dumps preserved for a week, and weekly dumps preserved for two months.

Connectivity

Connectivity at the Santa Barbara office is provided by Cox Communications, with the internal LAN behind a firewall that does not allow inbound connections.

Connectivity at the Woodland Hills office is provided by AT&T, with the internal LAN behind a firewall that does not allow inbound connections.

Connectivity at the EVP Systems Data Center is provided by Amazon Web Services, with virtual private networks defined via the AWS console. Security group rules allow only appropriate inbound connections on a per-server basis.

Approved Software

The following software is approved for installation on EVP Systems' Windows computers:

- Windows 10
- Microsoft Office 2016 (Word, Excel, Outlook, OneNote, PowerPoint)
- Microsoft Edge
- Google Chrome
- Adobe Reader
- Slack
- Dropbox Business
- EVP Office

The following software is approved for installation on EVP Systems' Windows computers, in the cited circumstances:

- Windows XP, Vista, 7 and 8 (testing computers)
- Microsoft Office 2013, 2010, 2007, 2003 (testing computers)
- Bloomberg Professional (research computers)
- BitVise (development computers)
- Microsoft Visual Studio 2010 (development computers)
- Inno Setup (development computers)
- kSign (development computers)
- MSI Wrapper (development computers)
- GitHub Desktop (development computers)
- QuickBooks (accounting computers)
- Software from partner vendors (support and testing computer)

Data

Information Classification

EVP Systems deals with six types of data:

- Securities information, including prices, dividends, etc.

- Source code, for EVP Systems' products and internal tools
- Company financial data, for EVP Systems' own accounts
- Customer contact and billing data
- System logs, both from the operating system and from EVP Systems' software
- Notes and documents, for research, processes, and policies

Handling of specific types and instances of data is restricted to employees who need access, per their job function. All information at EVP Systems should be considered confidential and is to be used in the process of conducting normal business; access to EVP Systems' information should be made only on EVP Systems' computers, using the specific employee's unique account.

Under no circumstances should any EVP Systems employee, system or database accept, manipulate or store any confidential client information, including personally identifiable information (PII). If an EVP Systems employee becomes aware of confidential client information that is either beyond what is required to perform their job or that has been accidentally disclosed, they must immediately file an Awareness Notice. While some client information is required to produce EVP Systems work-product—a decedent's name, their date of death, their security holdings, etc.—anything else should be reported. For example, a client's home postal address, their Social Security Number, or any bank identification or routing numbers would trigger an Awareness Notice. Likewise, any information sent to EVP Systems accidentally, regarding someone other than the decedent for instance, would also require reporting.

If an EVP employee receives an encrypted e-mail from a client, it is assumed that the mail contains information strictly for that client, and it is not for general distribution. If the mail contains PII, the employee should file an Awareness Notice.

Awareness Notices

Should an EVP Systems employee, system or database receive client personally identifiable information (PII), they should immediately file an Awareness Notice with company via the e-mail address `awareness@evpsys.com` and include the following details:

- Is the information truly sensitive?
- How was the information received?
- Where did the information originate?
- Is the affected client aware of the communication?
- Is the affected client aware of the nature of the data?
- What was the final disposition of the data?

If the information is determined by senior management to be client PII, the following steps are taken:

- The original data is destroyed, either physically if it was delivered by the post or fax, or virtually if it was delivered by e-mail or other electronic means
- Any copies of the data made in the reporting of the Awareness Notice are destroyed—for example, copies stored both as outbound e-mails from the original recipient, and the associated in-bound data received at `awareness@evpsys.com`, any paper copies used during the determination by company management if the information is PII, etc.
- The client is notified of the receipt of the information, and of its destruction
- If the information delivery was not accidental, the client is informed of what information is required to produce the relevant EVP Systems work-product, to avoid repeated delivery of similar information in the future

Breaches

In the event that an EVP employee believes that there is a breach of EVP Systems' computers or data, they should report the suspicion to the company's IT department via the e-mail account `it@evpsys.com`. For further information, please see "Intrusion Detection and Audit Process" and "Security Incident Response Policy."

Storage

Data at EVP Systems' is stored in various places and via various means, depending on circumstance.

- Securities information is stored in databases hosted at AWS, and on the AWS-hosted file system
- Source code is stored at Github
- Company financial data is stored in QuickBooks Online
- Customer contact and billing data is stored in an AWS-hosted database
- System logs are stored on machine file systems and copied to Papertrail
- Notes and documentation are stored in OneDrive (OneNote), Slack, and Google Workspace (Google Docs)
- Other files are stored in Dropbox

Encryption

All data transmitted to and stored by EVP Systems shall be encrypted, except where noted below. All data communicated to third-party systems is to be encrypted in transit, and is stored per vendor policy or implementation.

Data at rest in EVP Systems databases and file systems shall be encrypted with at least a Federal Information Processing Standard (FIPS)-compliant 256-bit AES cypher. Information in transit should be encrypted with at least TLS 1.2.

EVP Systems Windows 10 workstations have Microsoft's BitLocker enabled in "Transparent Mode," which implements a FIPS-compliant 256-bit version of XTS-AES. AWS-hosted databases and filesystems have encryption turned on, implementing a FIPS-compliant 256-bit version of AES.

TLS 1.2-compatible HTTPS is to be used by all EVP Systems websites and internal tools. TLS 1.2-compatible HTTPS is to be used when communicating with all third-party vendors, including GitHub, OneDrive, Slack, G Suite, and Dropbox.

One current exception to this policy is the connection between the EVP Office applications and the EVP Systems data center when using "Classic" mode—this transmission is unencrypted over a standard TCP/IP channel. However, no proprietary information or PII is ever sent—only security identifiers and valuation dates are transmitted. "Secure" mode uses TLS 1.2.

Retention

EVP Systems retains all data indefinitely.

- Securities information is required for historical pricing, the primary product of the company
- Source code needs all changes preserved, to allow for rollbacks and debugging
- Company financial data is necessary for accounting and auditing
- Customer contact and billing data is needed to preserve payment and usage histories
- System log history is useful for auditing and debugging
- Notes and documentation have revision histories to memorialize changes over time

Review

Once a quarter, all employee access to data available at EVP Systems is reviewed and revised. If an employee has changed roles, privileges that are longer required for the new job function are removed.

Physical Sites

EVP Systems has two offices:

1531 Chapala Street, #1
Santa Barbara, CA 93101

5855 Topanga Canyon Blvd., #520
Woodland Hills, CA 91367

Security at the Santa Barbara office is provided by building, office, and file-cabinet locks, and security cameras that monitor the front door, the back door, the central “bullpen,” the mailboxes, and the parking lot between the hours of 4:45pm and 7:15am on weekdays, and all day on weekends. The video recordings are stored for 30 days, and real-time software analyzes movement in each video, and alerts company staff if humans are detected during monitoring time.

Security at the Woodland Hills office is provided by building, office, and file-cabinet locks, with off-hours building access via an electronic key card that logs access. Armed on-site security is also present after hours.

Training

All EVP Systems employees receive this document upon hire, and review it annually. Also, all EVP Systems employees are given an information security training presentation annually.

Last Updated: April 30, 2021