Estate Valuations & Pricing Systems, Inc.
Security Incident Response Policy

Estate Valuations & Pricing Systems' primary software—the EVP Office applications EstateVal, GiftVal, CostBasis, and CapWatch—do not transmit or store Personally Identifiable Information (PII) or Sensitive Personal Information(SPI). Each sends only security identifiers and evaluation dates to the EVP data center; not decedent or grantor names, account numbers filenames, lot sizes, or other personally identifiable information.

However EVP Systems takes data security seriously and values the information that it has been entrusted with, including client contact phone numbers, e-mail conversations, billing metadata, and other details of doing business.

Accordingly, potential security incidents are handled in the following manner.

Discovery

The discovery of potential security incidents is primarily through three avenues:

- Monitoring software, as detailed in the "Security Information Policy"
- Security news, via the on-going monitoring of industry news, forums, and social media
- Employee alerts, informed by the annual security training provided by the company

Classification

When a possible security incident is discovered, an initial assessment of the severity of the incident is done by EVP Systems technical staff, and that informs the speed and intensity of the response.

"Minor" security incidents are trivial or accidental violations of security policy by an employee.

"Major" security incidents are potential external breaches of systems that do not contain client or company-critical data, or internal access of those resources by employees without official sanction.

"Critical" security incidents are major potential breaches of the integrity of the company's digital assets, including company-critical or client data, by internal or external actors.

If it is determined that no actual security incident occurred and the report was made out of an abundance of caution, no further response is required. In cases of high profile or newsworthy security issues, the non-response will be documented in the “Internet Vulnerability Responses” document.

Response

The response to a “minor” incident is made at a time convenient for both the company technical staff and the employee involved in the incident itself, usually within a single business day.

“Major” security incidents are addressed immediately upon discovery, by taking the affected system off-line for a forensic review of how access was gained and what data might have been exfiltrated. In the case of unauthorized employee access, appropriate permissions are tightened and a review of all access controls is performed. In the case of external access, the breached systems are either hardened or replaced after a review of the method of attack and if it was the result of a vendor bug, a local misconfiguration, or a fundamental flaw in security procedures and practices.

“Critical” security incidents are addressed immediately upon discovery, by taking all active company systems off-line. The “Disaster Recovery and Business Continuity” process is begun, to rebuild client-facing functionality as quickly as possible. A complete forensic analysis is done on the breached system, including the possible retention of a third-party expert.

Resolution and Remediation

“Minor” security incidents are usually resolved by a restatement of the appropriate policy, further training, and (if similar incidents are repeated) by the start of an official response as defined by the “Employee Disciplinary Policy.” This will happen within one work-week of the incident.

“Major” security incidents are resolved by a correction in the bug or misconfiguration that allowed inappropriate access, and a thorough review of the system to ensure that no unintended changes remain on the affected system. The affected system might be rebuilt from scratch as part of this process if it cannot be definitively determined that a breach did not result in unofficial changes. Documentation of system configurations and installations are changed to reflect the updates, including new lower-allowable versions and updated configuration requirements. If senior company management deems it appropriate, criminal and/or civil legal complaints may be filed against identified offenders. Technical resolution of the issue will be completed within four hours; documentation changes will be completed within two days; if required, criminal or civil charges will be filed within two months.

“Critical” security incidents are resolved with a complete reconstruction of the company’s technical infrastructure, after a determination is made of how the incident occurred. The specific circumstances of the breach are addressed in the reconstruction, though other re-engineering might also take place if existing security practice complicates or inhibits the remediation steps. A third-party expert may be retained to assess and analyze the changes to the infrastructure, as well as aid in the re-implementation. If senior company management deems it appropriate, criminal and/or civil legal complaints may be filed against identified offenders. Technical resolution will be completed within eight hours; re-engineering of potential design flaws will take place within two weeks followed by an eight-hour rebuild of the infrastructure; if required, criminal or civil complaints will be filed within two months.

Notification

In the case of any security incident that results in client information being exposed to either outside actors or employees without appropriate access, the company will notify the affected clients as soon as possible, using one or more of the following methods:

- Via Message Center. The EVP Office Message Center allows messages to be sent to EVP Office installations and presented to the user, either all at once or on a per-account or per-user basis. After a data breach, details will be provided through the Message Center at the appropriate granularity, including a link to a detailed Web posting.

- Via e-mail or the post, specifically to the primary contact EVP Systems has in its client database. After a data breach, e-mail will be sent to the affected clients that have an address on record with us; otherwise postal mail will be sent. The URL of a page detailing the breach will be included.

- Via website. A post will be made on the front page—and later stored in the archives—detailing the breach, who was affected, how the problem was remediated and what steps have been taken to prevent the intrusion from happening again.

Review and Update

This policy is reviewed and updated at least annually.

Approval

This policy has been approved by the President of EVP Systems, Michael A. Walker, on the following dates:

November 4, 2022 [Signed:] Michael A. Walker

November 18, 2022	[Signed:] Michael A. Walker
July 1, 2023	[Signed:] Michael A. Walker
July 1, 2024	[Signed:] Michael A. Walker

Last update: October 13, 2024