ISEC-14 Responsible Disclosure Policy

Revision 1

Effective date: September 1, 2025

Publication summary

Created by:	Alessandro Gai (CISO)
Approved by:	Alessandro Gai (CISO)
Policy Owner:	Alessandro Gai (CISO)
Classification:	**PUBLIC**

Change/revision history

Date	Rev.	By	Description of change
Jun 03, 2025	0.1	A. Gai	First draft
Jul 17, 2025	0.2	A. Gai, A. Duclos, M. Palokangas, E. Somhorst, J. Norsa	Final draft after reviews
Aug 13, 2025	1	A. Gai	Final version approved

Term of validity

This version replaces all previous versions and is valid until the next version is issued or the expiration date if it has been set.

Reference documents

- efficy security
- efficy security hall of fame

Index

1 Introduction

Data security is a priority for Efficy. We aim to enhance the reporting process of security vulnerabilities through a controlled and structured model.

This approach makes it easier for the sender to notify system vulnerabilities to the correct team inside Efficy, following a defined approach, thereby contributing significantly to security of our services and preventing potential damage or disruptions.

1.1 Purpose

The purpose of this policy is to encourage the responsible reporting of security vulnerabilities and provide a clear framework for security researchers, partners, and the public to report vulnerabilities in Efficy services and systems.

1.2 Scope

This policy applies to the Efficy products or services associated with them, including those associated with marketing websites. (Full list of domains in scope is described in "2.3 Inclusions and Exclusions" chapter).

1.3 Executive summary

If you believe you've found a security vulnerability in Efficy's service, please notify us, we will work with you to resolve the issue promptly.

Report vulnerability to the following email: security@efficy.com.

2 Responsible Disclosure Policy

2.1 Reporting process

External researchers, partners, and the public are encouraged to report security vulnerabilities to Efficy team via security@efficy.com.

To ensure a constructive process for both the reporter and Efficy organization, we request to **adhere following guidelines when reporting vulnerabilities**:

1. **Confidentiality**. Report vulnerability only to security@efficy.com email.
2. **Detail**. Provide detailed information to help Efficy understand the nature and impact of the vulnerability. This includes at least:
    - A description of the vulnerability.
    - Steps to reproduce the issue.
    - Potential impact.
    - Any proof-of-concept code, if applicable.
3. **Integrity**. Any discovery and reporting must be done in good faith, avoiding actions that could harm Efficy systems, data, or users.

    Do not exploit the vulnerability for any purpose other than testing.
4. **Coordination.** Do not publicly disclose the vulnerability. Following the responsible disclosure process, the reporter will be privately acknowledged for their contribution via email.

2.2 Responsible disclosure process

After having reported a vulnerability, the process is formalized in next phases:

- **Vulnerability receipt**. Efficy team will acknowledge receipt of vulnerability reports and notify the reporter via email.
- **Assessment and resolution**. Reported vulnerabilities will be assessed, prioritized, and resolved based in their severity.

    The reporter will be kept informed of the resolution progress.
- **Reporter acknowledgement.** Following the responsible disclosure process, the reporter will be privately acknowledged for contribution via email and if agreed the reporter nominative will be published on our website security section in the hall of fame page.

Some extra notes for reporters:

- Please provide Efficy with a reasonable amount of time to resolve the issue before disclosing it to the public or a third party. We aim to resolve critical issues within ten business days of disclosure.
- As for the nature of the CVEs to inform end-users to patch or take action on a vulnerable product we allow reporters to publish CVEs ONLY for not cloud components (eg: plugins, on premise applications, ...).
- Make a good faith effort to avoid violating privacy, violating any applicable laws / regulations, destroying data, or interrupting or degrading the Efficy service. Please only interact with accounts you own or for which you have explicit permission from the account holder.
- Avoid exploiting a security issue that you discover for any reason beyond what's needed to demonstrate it.

2.3 Inclusions and Exclusions

This policy applies to the Efficy **applications or services hosted or associated at next domains and possible subdomains**:

- *.anpdm.com
- *.anpasia.com
- *.apsis.com
- *.apsis.one
- *.e-deal.net
- *.e-deal.biz
- *.efficy.cloud
- *.efficy.com
- *.efficy.io
- *.efficytest.com
- *.inescrm.com
- *.perfectview.nl
- *.pvcrm.de
- *.sumacrm.com
- *.tribecrm.nl
- *.webcrm.com

We do not accept reports for vulnerabilities solely affecting our marketing websites which contains no sensitive data.

In addition, reports that describe theoretical attack vectors without substantiated proof of exploitability are excluded.

2.4 Safe harbour

To encourage responsible reporting, subject to the exclusion below Efficy offers safe harbour to security researchers and reporters:

- **Legal Protection.** If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized, we will work with you to understand and resolve the issue quickly, and Efficy will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known.
- **Confidentiality**. Efficy will not share reporter's personal information without his permission, except as required by law.
- **Recognition**. Following the responsible disclosure process, the reporter will be privately acknowledged for his contribution via email and his nominative will be published on our website security section in the hall of fame page if agreed.

Efficy is providing this service to help ensure a safe and secure environment for all its users. As such, any users believed to be engaging in the below activities will have their user credentials immediately deactivated.

Excluded from the Safe Harbour, are the following acts that may lead to further action, including legal actions.

We'd like you to refrain from:

- **Data destruction or alteration**. Actions leading to deleting, modifying, or corrupting data or systems.
- **Denial of Service** (DoS). Performing or attempting to perform actions that degrade, disrupt, or deny access to services or systems.
- **Exploitation**. Exploiting vulnerabilities for purposes other than responsible disclosure, including persistence, lateral movement, or privilege escalation.
- **Privacy Violations**. Accessing, copying, modifying, or deleting personal or sensitive data beyond what is strictly necessary to demonstrate the vulnerability.
- **Spamming**: Sending unsolicited or bulk messages through any communication channel.
- **Social engineering or phishing**. Engaging in deceptive practices targeting Efficy employees, contractors, or partners to gain unauthorized access or information.

- **Supply chain attacks**. Targeting or compromising third-party vendors, partners, or service providers to gain access to Efficy systems or data.
- **Physical security attacks**. Attempting unauthorized access to Efficy's physical premises, hardware, or third-party data centers.

2.5 Standards adopted by efficy

Efficy security findings are categorised by the OWASP ASVS[5] categories.

We are adopting the Cobalt vulnerability dictionary database[6].

To rate the findings we are using the Base Metrics of CVSS V 4.0 standard[7].

[5] OWASP Application Security Verification Standard (ASVS)
[6] Vulnerability Wiki
[7] Common Vulnerability Scoring System Version 4.0 Calculator - CVSS v4.0 User Guide