Coordinated Vulnerability Disclosure Policy

Code	
Version	1.0
Date of version	05/02/2024
Created by	J. B. Sorensen
Approved by	Lars Sneftrup Pedersen
Confidentiality level	Public

Change history

Date	Version	Created by	Description of change
05/02/2024	1.0	J. B. Sorensen	Initial version

Table of Contents

1.0 Purpose and scope

The purpose of this policy is to define clear rules for the reporting of vulnerabilities to Admin By Request. This document is applied to the entire scope of the services provided by Admin By Request.

2.0 Reference documents

- Incident & Vulnerability Management Procedure

3.0 Coordinated Vulnerability Disclosure Policy

3.1 Background

At Admin By Request, we recognize the critical importance of safeguarding the security and integrity of our products and services. This policy seeks to promote responsible reporting of potential vulnerabilities, ensure proper patching and minimizing the risk of security incidents for our users.
It is crucial to acknowledge that premature disclosure of vulnerabilities can be counterproductive to its purpose as it may lead to security incidents, as users may not have the opportunity to implement timely patches and thereby exposing them to the vulnerability. This policy aims to strike a balance between transparency and security by establishing a coordinated and responsible disclosure process.
We understand that vulnerabilities are an inherent part of technology, and our focus is on addressing them promptly to ensure a secure environment for our users. We value the contributions of the security community in helping us maintain the highest standards of security.

3.2 Scope

This policy encompasses all services and products provided in the Admin By Request platform. We encourage security researchers, users, and other stakeholders to report any potential vulnerabilities they discover within the scope of our offerings.

3.3 Out of scope

The following are considered out of scope for this policy:

- Vulnerabilities that necessitate unrealistic prerequisites
- Issues resulting from user misconfiguration or misuse of the product/service, such as inadvertently exposing sensitive information due to improper settings or permissions.
- Bugs in the software that do not pose a security risk, such as minor display errors, cosmetic issues, or non-critical functionality failures.

3.4 Reporting

To report any vulnerabilities within the scope of this policy, please email **security@adminbyrequest.com**.
We appreciate your cooperation and adherence to responsible disclosure practices. Upon receipt of your report, our security team will promptly assess and address the reported vulnerability. We encourage you to provide detailed information to facilitate a quicker resolution.

3.5 Assessment and Validation

Our security team will evaluate and validate reported vulnerabilities within a reasonable timeframe, typically no more than 30 days.
We prioritize the assessment based on the severity, impact, and potential exploitation of the vulnerability.

3.6 Remediation and Disclosure

Once a vulnerability is confirmed, Admin By Request will work diligently to develop a fix or mitigation strategy.
We aim to release patches or updates for significant vulnerabilities within 90 days of report validation.
Details of the vulnerability and its resolution will be disclosed responsibly, in coordination with the reporter, and in a manner that minimizes risk to our customers.