Regulatory & Compliance

Customer Contingency Plan

Document Information

Code:	**CD-CCP**	Created by:	**Steve Dodson**
Version:	**2.0**	Approved by:	**Lars Sneftrup Pedersen**
Date:	**1 December 2025**	Confidentiality:	**Public**

Admin By Request
ZERO TRUST PLATFORM

Copyright © 2025 Admin By Request

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this document is to ensure customers can respond to unforeseen events that affect services, software, personnel, and security on the service provider side (us), so as to minimize damaging effects on business operations on the customer side (you).

1.2 Scope

The document:

- Summarizes the preventative controls in place at Admin By Request to minimize the negative effects of unforeseen events on its customers.
- Outlines Admin By Request's policies and procedures regarding customers during and following such events.
- Identifies possible risk scenarios and their predicted business impact for customers, and details steps that can be taken by customers to remediate issues until they can be resolved, or recovered from, by the service provider.

1.3 Limitations

This document should not be confused with any Admin By Request company remediation documents of a similar nature (i.e., our BC / DR Plan), as it does not go into detail about the steps and procedures that we, the service provider, will follow in response to unforeseen events.

Rather, this document focuses on scenarios and remediations from *the customer* side.

1.4 Audience

The intention of this document is that it can be used by Admin By Request **customers** for their own Contingency Planning in relation to the service our company provides.

1.5 Definitions

1.5.1 Unforeseen Event

In this document, 'unforeseen event' is used to refer to an event that has the possibility of occurring in future, such as a disaster, crisis, emergency, accident, or something else unexpected or unplanned for.

The document examines such events that result in the service provider's inability to provide some or all regular services for a period of time.

The scenarios described are grouped into the following categories:

- **Service Outage** – All systems are non-functional
- **Software Failure** – One or more vital systems are non-functional
- **Loss of Communication** – Service provider support is unavailable
- **Cyber Attack** – Customer data is compromised
- **Customer-Instigated** – Customer's service is discontinued

These scenarios are covered in detail in "Scenario-Based Risk Management" on page 8.

1.6 Related Documents

This document may refer to, and should be read in conjunction with, the following:

- Commitments and responsibilities in ABR's Data Processing Agreement
- Support provisions in ABR's Terms and Conditions and Customer Support Services
- Data handling processes in How We Handle Your Data
- Collection, use and disclosure of personal data in ABR's Privacy Policy and Data Privacy Settings

Refer also to ABR's Trust Center documents.

This document is available online:

Customer Contingency Plan

2 Data Protection

2.1 Introduction

Our software service makes use of a fully managed database (Microsoft Azure SQL) and a combination of cross-region geo-replication and failover techniques to ensure data resiliency.

These measures, as well as data encryption and file scanning, protect customer data from unavailability, theft and corruption, minimizing negative outcomes for customers.

IMPORTANT

The scenarios described in this document are highly unlikely.

Admin By Request has procedures and policies in place to ensure that, in any unforeseen event, the resulting effects on our customers are minimized from the outset.

2.2 How is Customer Data protected?

2.2.1 Multiple-location storage

ABR hosts its service entirely in Microsoft Azure. At the time of writing, customer data is stored in Azure SQL databases located in **five** geographic regions. Each region operates a primary and a secondary data center.

Your data is stored in a data center that is located in one of the geographic locations listed below. These are in Europe, the USA, the UK and Asia.

To determine your data location, go to page Tenant Settings > Data in the portal and click the **RETENTION** tab. Note the geographic location shown in field **Data Location** - it will be one of the following:

- **EU West, Netherlands** (Europe - Netherlands)
- **US East, Virginia** (USA)
- **London, United Kingdom** (UK)
- **Frankfurt, Germany** (Europe - Germany)
- **Singapore** (Asia)

2.2.2 Cold storage backups

Our service provides Acronis cold storage backups daily in case Microsoft Azure fails in both locations in your region.

2.2.3 Encryption

Customer data is protected both at rest and while in transit, using Azure SQL transparent data encryption and SSL encryption, respectively.

Raw data is protected using 256-bit encryption against attackers that may have physical access to a client.

2.2.4 Geo-replication

SQL replication between the two storage locations of your data preserves its consistency and integrity, and ensures it is backed up in case of an unforeseen event.

2.2.5 Failover

If one location fails, automatic failover switches the handling of your data to the secondary location in your region.

Refer to How We Handle Your Data for more information.

2.3 How is Customer Data restored?

2.3.1 Point-in-Time restore

Admin By Request uses Microsoft Azure SQL, which gives us the ability to do an Azure SQL restore from any point in time within the **past 35 days**.

2.3.2 Time taken for a data restore

The time taken for an Azure SQL restore varies depending on the size of the database and the point in time selected. It can range from minutes, to several hours for very large and/or active databases.

2.4 Other options for data access

Admin By Request provides customers with the ability to download all Auditlog data via our API and store it locally in a SIEM tool.

This ensures that, during a service outage event, customers still have access to their previously downloaded Auditlog data (keeping in mind, this data may not be completely up to date).

2.5 Other security measures

Before we even begin handling customer data, we ensure the integrity of our own files.

2.5.1 Access to the production environment

A strictly limited number of people have access to Admin By Request's production environment. These are:

- The Head of Development
- The Chief Technical Officer (CTO)

2.5.2 Internal security

We have strict security policies in place for all our employees. The Data Processing Agreement (Annex III: Technical and Organisational Measures) contains more information on the steps we take to protect your data.

We have been audited and are certified in a number of areas, including **ISO 27001**, **Cyber Essentials Plus** and several **independent pentests** - please refer to the Trust Center for full details.

Don't hesitate to contact us if you have any questions about data security at Admin By Request.

2.5.3 Software update security

When we do software updates, we use the Google service VirusTotal Monitor3 to scan the binary files by 70+ antimalware engines including Crowdstrike, McAfee, TrendMicro and Acronis. Files cannot be deployed without passing the scan of all 70+ engines, so before we put files into production for you to download, we have confirmation that they are safe.

Refer to our Data Processing Agreement (Annex III) for more information on internal security.

2.6 Customer confidentiality

Customer confidentiality in the case of an unforeseen event remains paramount, with Admin By Request adhering at all times to the European General Data Protection Regulation (GDPR). Specifically:

- **Clause 7.4 (b)** of our Data Processing Agreement states that:

  "The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality."
- **Section 17** of our Terms & Conditions requires (among other things) that Admin By Request keep confidential information of all customers strictly confidential, including not disclosing any confidential information to any person without prior written consent.
- **Annex III** of our Data Processing Agreement requires Admin By Request to take appropriate technical and organizational security measures against the accidental loss of personal data and ensure that the data is not disclosed to any unauthorized person and is not misused or otherwise processed in contravention of the GDPR.

In the case of a personal data breach,Admin By Request shall notify affected customers in accordance with our DPA and applicable law.

More on the GDPR and customer confidentiality can be found in our Terms & Conditions and Data Processing Agreement documents.

3 Communication

3.1 Communication Policy

Our communication policy with customers during an unforeseen event has the main objective of full transparency.

3.1.1 What we Communicate

In the face of such an event, Admin By Request will communicate to customers:

- What has gone wrong
- What and/or who is affected
- What you, the customer, can usefully do in the meantime
- What we, the service provider, are doing now (i.e., our BC / DR remediation plan - high-level steps)
- When we, the service provider, expect to return to business-as-usual

3.1.2 When we Communicate

When we will contact customers in an unforeseen event depends on the nature of the event and the severity of its effects on each customer.

As mentioned in "Customer confidentiality" on page 5, in the case of a personal data breach, Admin By Request shall notify affected customers in accordance with our DPA and applicable law.

3.1.3 How we Communicate

In unforeseen events that directly affect our customers, our two primary means of communication are:

1. **Email** (either group or one-on-one)
2. **Phone** (including video call)

Depending on the nature of the event and the severity of its effects on customers, either or both may be used at any time.

During an incident, the **Send to** email address used for contacting you will be the one entered into the *Security email* field in your tenant. To view or change this email address, go to page Tenant Settings > Tenant in the portal and click the **INCIDENTS** tab.

> *Security email* is the email address where you wish to receive security communications, including incident alerts, vulnerability disclosures, and other information security notifications.

For real-time details on the status of our infrastructure, refer to Admin By Request - Services Status.

3.2 Key Personnel

The following are your emergency contacts at Admin By Request in the case of an unforeseen event.

Name and Title	Contact Details
Ryan Akers Territory Director Americas and Oceania	Email: rak@adminbyrequest.com Phone: +1 262 299-4600
Jeff Rhys-Jones Territory Director EMEA and APAC	Email: jrj@adminbyrequest.com Phone: +44 20 3808-8747
Jens Ole Andersen Territory Director Nordics and DACH	Email: joa@adminbyrequest.com Phone: +45 55 55 36 57
Jacob Buus Chief Operating Officer (COO)	Email: jbu@adminbyrequest.com Phone: +45 55 55 36 57
Lars Senftrup Pedersen Chief Executive Officer (CEO)	Email: lsp@adminbyrequest.com Phone: +45 55 55 36 57

4 Scenario-Based Risk Management

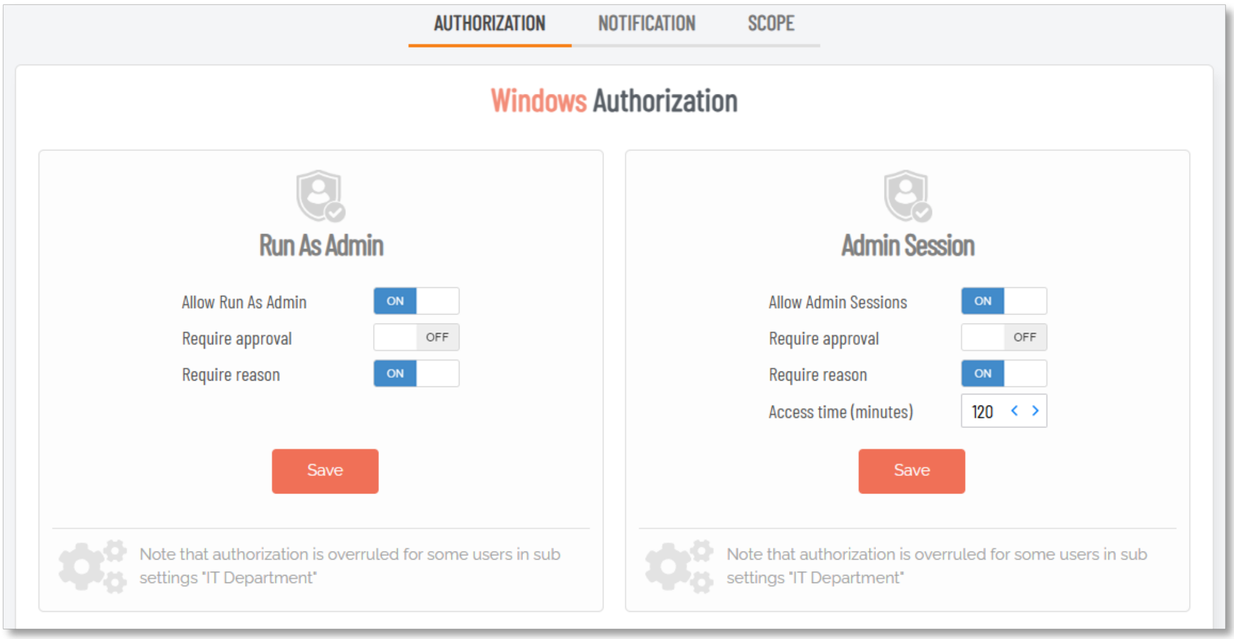
4.1 Introduction

This section describes potential scenarios that you, *the customer*, can remediate to minimize downtime while we, the service provider, resolve the issue.

> This document does not describe the steps and processes to be taken by Admin By Request to recover from disasters and other such unforeseen events - that information is covered in our internal company BC / DR plan.

4.2 Service Outage Scenarios

For these types of scenarios, it is important to understand the different *result* for organizations that are using **Require approval** mode (where users require *approval* of requests before elevation) and organizations that are not (where users do not need their requests approved in order to gain elevation). An example of a portal setting that illustrates approval *not required* is shown in the following image:



Windows Authorization

Run As Admin

Allow Run As Admin: ON
Require approval: OFF
Require reason: ON

Note that authorization is overruled for some users in sub settings 'IT Department'

Admin Session

Allow Admin Sessions: ON
Require approval: OFF
Require reason: ON
Access time (minutes): 120

Note that authorization is overruled for some users in sub settings 'IT Department'

Many customers opt not to use **Require approval** mode at all. They use Admin By Request as an auditing tool with roadblocks to prevent obvious abuse (such as **Require reason**, blacklists, etc.) and assurance of malware protection (OPSWAT MetaDefender).

For these customers, the business impact of a service outage scenario is always low, because the end user experience stays the same – even in worst cases.

These points are illustrated in the following scenarios.

In this document, the definition of an **acceptable period of time** is determined by each customer's **RTO**.

Customers not using Require Approval mode

For service outage scenarios where the customer is not using **Require approval** mode, the result and business impact will be similar to that described below.

4.2.1 Scenario: Worst-case all systems non-functional

This scenario covers both short and extended time periods.

Description: The entire Admin By Request service is non-functional for what is considered an acceptable or unacceptable period of time including website, APIs and mobile app.

Result: Users function normally from their endpoints, as their requests do not need to wait for approval. The current settings at the time of the service outage are maintained throughout, however editing of settings is unavailable. Any uploads to the Auditlog are queued on the endpoint and will upload when the service is functioning again. Once service is restored and all endpoints have worked through their upload queues, the Auditlog will appear as if the service was never down.

Business Impact Rating: LOW

Customers using Require Approval mode

For customers using **Require approval** mode, service outages can cause varying results and business impacts, illustrated in the following scenarios.

4.2.2 Scenario 1: Worst-case all systems non-functional (short)

This scenario covers only *short* or *acceptable* time periods.

Description: The entire Admin By Request service is non-functional for an acceptable period of time, including website, APIs and mobile app.

Result: Users cannot get approval of requests, which sit on endpoints until the service is up again. When this happens, requests are updated from the endpoint to the API. User experience is that response time is longer than usual. Administrators cannot access the Auditlog or other portal pages during the incident.

Business Impact Rating: MEDIUM

Remedial Actions: None.

4.2.3 Scenario 2: Worst-case all systems non-functional (extended)

This scenario covers *extended* or *unacceptable* time periods.

Description: The entire Admin By Request service is non-functional for an unacceptable period of time, including website, APIs and mobile app.

Result: Users cannot get approval of requests, which sit on endpoints until the service is up again. When this happens, requests are updated from the endpoint to the API. User experience is that response time is considerably longer than usual. Administrators cannot access Auditlog or other pages during the incident.

Business Impact Rating: HIGH

Remedial Actions:

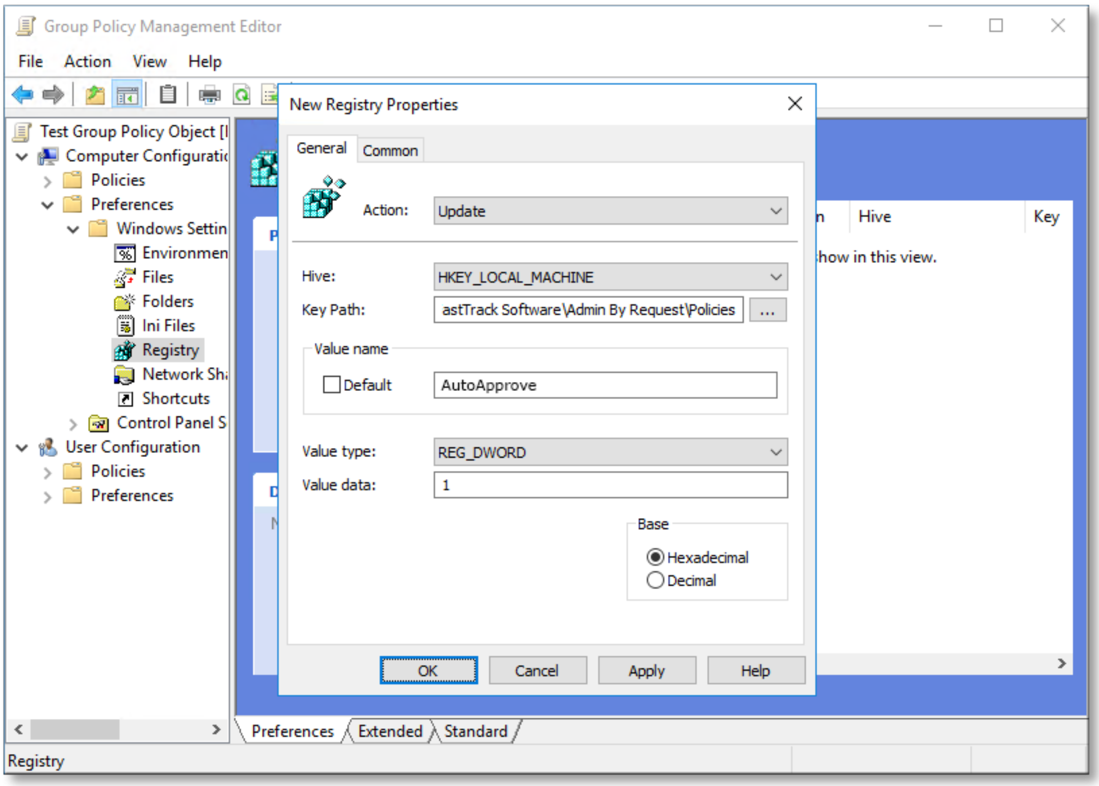
For Windows, set the *AutoApprove* and *EnableAppElevations* registry keys to temporarily allow elevations without approval. These keys are for *Admin Session* and *Run As Admin* respectively:

1. Open the **Group Policy Management Editor** from the Windows search bar (**Edit group policy** in menu)
2. Go to **Computer Configuration > Preferences > Windows Settings > Registry**
3. Policies are set under the following registry key:

```
HKEY_LOCAL_MACHINE\Software\FastTrack Software\Admin By
Request\Policies
```

KeyPath must be **Software\FastTrack Software\Admin By Request\Policies**

4. Set the *AutoApprove* registry key to **1** (for *Admin Session*):



Action: Update

Hive: HKEY_LOCAL_MACHINE

Key Path: astTrack Software\Admin By Request\Policies

Value name

□ Default AutoApprove

Value type: REG_DWORD

Value data: 1

Base

● Hexadecimal

○ Decimal

5. In the same way, set the *EnableAppElevations* registry key to **1** (for *Run As Admin*). More on this here: Policies for Windows.

For macOS, set the*RequireApproval* and *EnableAppElevations* policy values to temporarily allow elevations without approval:

1. Go to **/Library/Application Support/Admin By Request/adminbyrequest.policy**
2. Edit the file so that it includes setting the *RequireApproval* boolean value to **0** (false) and *EnableAppElevations* to **1** (true):

```
{
    "RequireApproval" : "0",
    "EnableAppElevations": "1"
}
```

More on this here: Policies for Mac.

IMPORTANT
Once a contingency scenario is over, do not forget to reset any endpoints where approvals have been temporarily disabled.

4.2.4 Scenario 3: Service ceases to operate

Description: The entire Admin By Request service ceases to operate indefinitely or permanently, including the website, APIs and mobile app.

Note that this scenario is unrealistic because you pay a subscription for the Admin By Request service. Therefore, you would be made aware if our service were to cease operating.

Result: Users cannot get approval of requests, which sit on endpoints until the service is up again. When or if the service is up, requests are queued, and the user experience is an exceptionally long approval time.

Business Impact Rating: CRITICAL

Remedial Actions:

1. **Option 1:** As a temporary solution while planning a replacement, set the *AutoApprove* and *RequireApproval* registry keys to temporarily allow elevations without approval. See "Remedial Actions:" on the previous page.
2. **Option 2:** Uninstall Admin By Request on endpoints and install a replacement solution.

4.3 Software Failure Scenarios

These scenarios cover *individual* aspects of Admin By Request's cloud-based service:

- Website is Down
- Mobile Application is Down
- Support Assist Feature is Unavailable

Customers using Require Approval mode

For customers that use **Require approval** mode only - the scenarios do not apply if users do not require approval.

4.3.1 Scenario 1: Website is Down

Description: The Admin By Request website is entirely non-functional for a short / extended period of time.

Result: IT administrators are not able to use the website for any function, including approving requests, viewing the Auditlog and configuring settings. Users may have to wait longer than usual for requests to be approved.

Business Impact Rating: LOW

Remedial Actions: Perform all functions using the Admin By Request mobile application on any iPhone, iPad or Android device, apart from change settings, which is unavailable via the app.

4.3.2 Scenario 2: Mobile Application is Down

Description: The Admin By Request mobile application is entirely non-functional for a short / extended period of time.

Result: IT administrators are not able to use the mobile app for any function, including approving requests and viewing the Auditlog. Administrators out of the office will not be able to approve requests on the move via the mobile app. Users may have to wait longer than usual for requests to be approved.

Business Impact Rating: LOW

Remedial Actions: To use Admin By Request on a mobile device, log in to the website user portal from the internet browser of a mobile device.

4.3.3 Scenario 3: Support Assist Feature is Unavailable

Description: The Admin By Request *Support Assist* feature is non-functional for a short or extended period of time.

Result: End users who are not able to self-service (either due to lacking IT skills or having *Run As Admin* and *Admin Session* disabled) cannot use the *Support Assist* feature to gain elevation.

Business Impact Rating: LOW

Remedial Actions: Log out the user who is unable to self-service or use *Support Assist* and log the Help Desk person in to perform the task that requires elevation.

4.4 Loss of Communication Scenarios

These scenarios cover situations where Admin By Request's support services and/or key contacts are unavailable, unresponsive or cannot be contacted.

4.4.1 Scenario 1: Service Provider General Support is Unavailable or Unresponsive

Description: Attempted contact with the service provider by the customer is unsuccessful – no reply or answer in a timely manner.

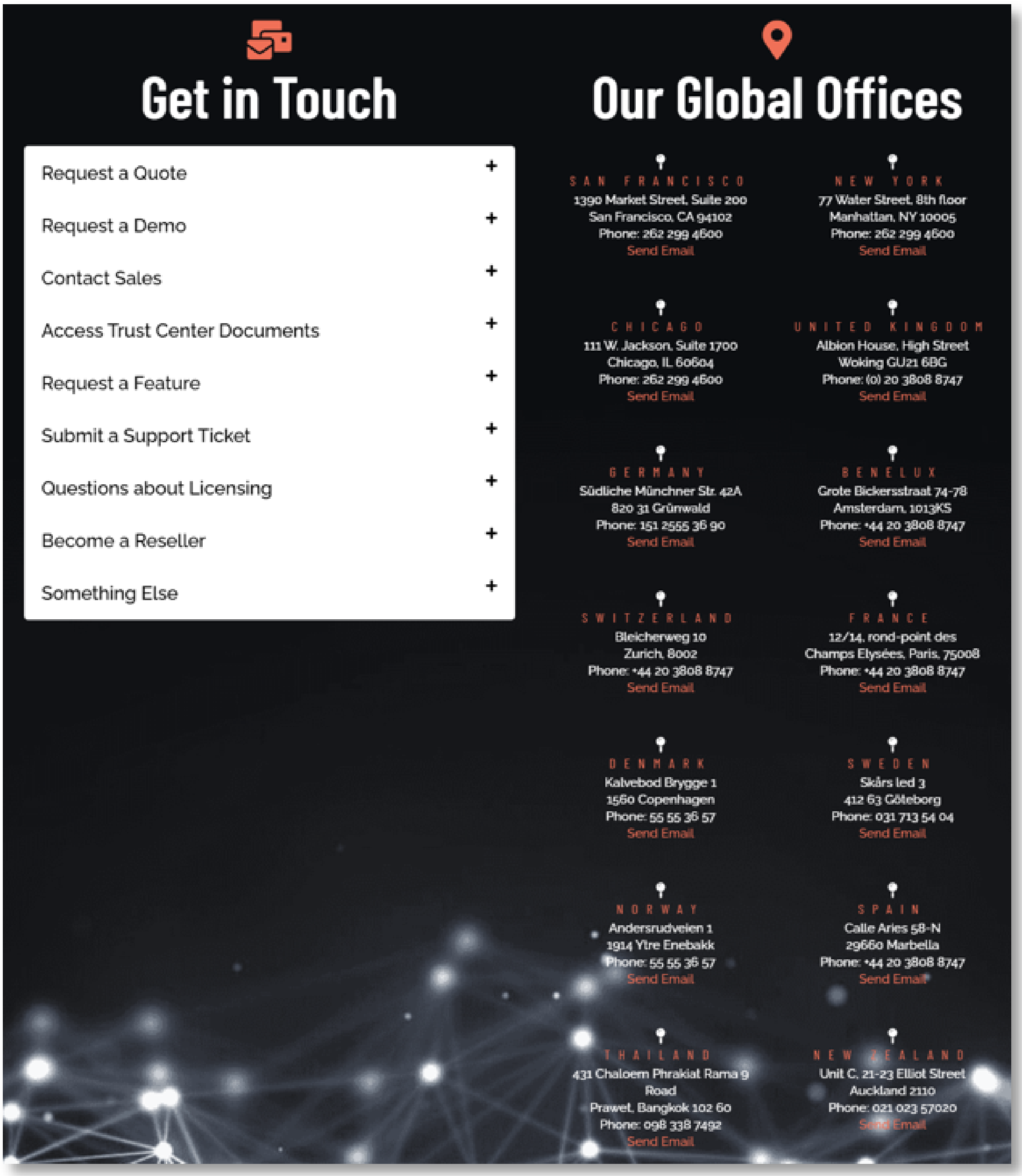
Result: Customers cannot get general support from service provider.

Business Impact Rating: LOW

Remedial Actions:

Try all possible means of contact:

1. **Option 1:** Create a support ticket, using either the Admin By Request portal or the main website, which will return a response within one business day.
2. **Option 2:** Contact your Admin By Request account executive (the representative you purchased the software subscription from).
3. **Option 3:** Use any of the listed mechanisms for contact on the Admin By Request website Get in Touch page:



Get in Touch

Request a Quote +
Request a Demo +
Contact Sales +
Access Trust Center Documents +
Request a Feature +
Submit a Support Ticket +
Questions about Licensing +
Become a Reseller +
Something Else +

Our Global Offices

SAN FRANCISCO
1390 Market Street, Suite 200
San Francisco, CA 94102
Phone: 262 299 4600
Send Email

NEW YORK
77 Water Street, 8th floor
Manhattan, NY 10005
Phone: 262 299 4600
Send Email

CHICAGO
111 W. Jackson, Suite 1700
Chicago, IL 60604
Phone: 262 299 4600
Send Email

UNITED KINGDOM
Albion House, High Street
Woking GU21 6BG
Phone: (0) 20 3808 8747
Send Email

GERMANY
Südliche Münchner Str. 42A
820 31 Grünwald
Phone: 151 2555 36 90
Send Email

BENELUX
Grote Bickersstraat 74-78
Amsterdam, 1013KS
Phone: +44 20 3808 8747
Send Email

SWITZERLAND
Bleicherweg 10
Zurich, 8002
Phone: +44 20 3808 8747
Send Email

FRANCE
12/14, rond-point des
Champs Elysées, Paris, 75008
Phone: +44 20 3808 8747
Send Email

DENMARK
Kalvebod Brygge 1
1560 Copenhagen
Phone: 55 55 36 57
Send Email

SWEDEN
Skårs led 3
412 63 Göteborg
Phone: 031 713 54 04
Send Email

NORWAY
Andersrudveien 1
1914 Ytre Enebakk
Phone: 55 55 36 57
Send Email

SPAIN
Calle Aries 58-N
29660 Marbella
Phone: +44 20 3808 8747
Send Email

THAILAND
431 Chaloem Phrakiat Rama 9
Road
Prawet, Bangkok 102 60
Phone: 098 338 7492
Send Email

NEW ZEALAND
Unit C, 21-23 Elliot Street
Auckland 2110
Phone: 021 023 57020
Send Email

4. **Option 4:** Use the contact Information from "Key Personnel" on page 7.

4.4.2 Scenario 2: Customer's Key Contact in Service Provider is Suddenly Unresponsive

Description: The customer's Admin By Request account executive (the representative you purchased the software subscription from) is suddenly unresponsive to attempted contact.

Result: Customers cannot get general or specific support from service provider or service provider key contact.

Business Impact Rating: **LOW**

Remedial Actions: See "Remedial Actions:" on the previous page.

4.5 Cyber Attack Scenarios

4.5.1 Scenario 1: Hackers Reveal Cyber Attack on Service Provider

Description: It is revealed online that Admin By Request has suffered a security breach and customer data has been compromised (before the service provider is aware or has contacted customers about the issue).

Result: Customer may have had data compromised. Customer may suffer disruption to normal business operations due to downtime while the issue is being resolved, damage to reputation and uncertainty in the workforce. Relationship and/or contract with service provider may be damaged or terminated.

Business Impact Rating: **HIGH**

Remedial Actions: Activate own organization's remediation plan / DRP. Admin By Request personnel will keep you informed at every stage of the recovery process. See the Data Processing Agreement on our website for more information.

4.6 Customer-Instigated Scenarios

4.6.1 Scenario 1: Customer Fails to Renew Subscription

Description: A customer fails to renew their subscription with Admin By Request, either by accounting or other error.

Result: The customer's plan reverts from the paid version to the free plan.

Business Impact Rating: **LOW**

Remedial Actions: Contact your Admin By Request account executive as soon as possible. If unavailable or unresponsive, use one of the options listed in "Remedial Actions:" on the previous page.

5 Summary

5.1 Key Takeaways

Summarizing the key points in this Customer Contingency Plan:

- This Contingency Plan is for the *customer's use*; to take useful action during unforeseen events. It does **not** describe how Admin By Request (the service provider) will take remedial action in such events.
- Admin By Request has already taken tangible steps to ensure the negative effects of an unforeseen event on its customers are minimized, by how we store, encrypt, and manage customer data, maintain customer confidentiality, and by our communication protocols with customers in the face of such events.
- The scenarios listed in this document, although improbable, describe remedial actions that can be taken by the customer to minimize the negative effects of unforeseen events on business operations, should they occur.

5.2 Our Brand Promise

Our core commitment is to our customers and the experience we create for you, even when unforeseen events occur.

We understand that while we cannot plan for, or prevent every possible future event, we can help you to minimize resulting negative impacts if they do occur.

6 Glossary

The following terms and definitions are used in this document.

Term	Short for	Definition
API	Application Programming Interface	A a set of rules, protocols, and tools that allows different software applications to communicate with each other.
BC / DR	Business Continuity / Disaster Recovery	A plan consisting of the set of policies, processes and procedures that enable a business to minimize the negative effects of a disaster and remain operational during and following its occurrence.
DNS	Domain Name System	The Internet's "phone book," translating human-friendly domain names like google.com into numerical IP addresses that computers use to locate each other.
DPA	Data Processing Agreement	Admin By Request's main contractual specification of its obligations to customers.
DPO	Data Protection Officer	The role at Admin By Request responsible for data protection and ensuring compliance with data privacy regulations like the GDPR.
GDPR	General Data Protection Regulation	The primary European specification for ensuring compliance with data privacy and security regulations.
Microsoft Azure SQL	Microsoft Azure SQL	A cloud-based family of database management products developed by Microsoft.
OPSWAT	OPSWAT	Us-based software company that develops and sells MetaDefender.
RTO	Recovery Time Objective	The amount of time within which an organization's processes, systems and/or applications must be restored in order to avoid significant damage to the business.
SIEM	Security Information and Event Management	A subsection within the field of computer security, where software products and services combine security information management (SIM) and security event management (SEM).
SQL	Structured Query Language	Language used for managing data in relational database management systems. Often incorporated into product names (e.g. Microsoft Azure SQL).
SSL	Secure Sockets Layer	A computing protocol that ensures the security of data sent via the internet by using encryption.

7 Document History

Version	Author	Changes
19 March 2021 **1.0**	Sophie Dodson	Initial document release.
1 September 2023 **1.1**	Steve Dodson	Annual review and company name change from FastTrack Software to Admin By Request.
1 December 2025 **2.0**	Steve Dodson	Annual review, including addition of new data centers, updates to contact details and customer confidentiality, updates to scenarios and new document template.