

SYNAQ SOFTWARE AS A SERVICE SUPPORT POLICY

Contents

Policy	2
1. DEFINITIONS	2
2. SUPPORT SERVICE REQUEST LOGGING PROCESS	3
3. REMOTE SUPPORT	3
4. ESCALATIONS PROCESS	4
5. MAINTENANCE (SCHEDULED AND EMERGENCY).....	4
6. OUTAGE NOTIFICATIONS	5
7. SYNAQ COMPANY APPOINTED CONTACT DETAILS.....	5
8. SYNAQ SERVICE LEVELS	5
9. SYNAQ SERVICE-SPECIFIC SLA's - CLOUD MAIL AND SECUREMAIL	6

Policy

This Policy document details SYNAQ's Support, Outage and Service Level processes.

1. DEFINITIONS

The following words shall have the meanings assigned to them hereunder and cognate expressions shall have similar meanings:

- 1.1. **"Authorised Contact(s)"** are the personnel authorised by the Client to log Service Requests, access and use Services, request information and who receive all business communications.
- 1.2. **"Availability"** Period of available Service uptime to Client minus all downtime that is not excluded as agreed to under this document.
- 1.3. **"Baseline Volume / Service Scope"** means the initial Service volume as per the Proposal Summary that shall apply as of the commencement date of the particular service.
- 1.4. **"Best Practices Implementation"** means the practices as may be made available from SYNAQ to the Client from time to time.
- 1.5. **"Client"** refers to direct or Reseller Clients who have entered into Agreements with SYNAQ.
- 1.6. **"False Negative"** means a spam email which is not identified as spam by SYNAQ SecureMail.
- 1.7. **"False Positive"** means a legitimate email incorrectly classified as spam by SYNAQ SecureMail.
- 1.8. **"Latency"** refers to the delay in inbound email delivery (i.e. the time it takes from when a mail is sent and the time it arrives in the recipient's inbox).
- 1.9. **"Maintenance"** means maintenance (planned or emergency) performed by the Service Provider to the Services, the Service Provider's network and/or Services infrastructure, solely in order to maintain or improve the performance of the Services (including but not limited to update on software utilized to provide the Service), that reasonably could be expected to have a material adverse effect on the Services and/or the Client's operations.
- 1.10. **"Phishing"** means the act of attempting to acquire information from the recipient of an electronic communication by masquerading as a trustworthy entity.
- 1.11. **"Priority Levels"** means the levels as per clause 8.1;
- 1.12. **"Service"** means current and future active Services rendered by SYNAQ to the Client.
- 1.13. **"Service Levels"** are a set of Service-related metrics used to measure the performance of SYNAQ Services. Service Levels will only be applicable, provided that Client's adhere to the terms of: SYNAQ's Acceptable Use Policy and the SecureMail and Cloud Mail Policies (accessible here: <https://www.synaq.com/legal>), which detail the terms for best practice use of and SLA's for the SYNAQ SecureMail and Cloud Mail Services.
- 1.14. **"Service Request"** is a request from a Client or a Client's authorised contacts that initiates a service action with the SYNAQ Support Desk which has been agreed as a normal part of service delivery. A Service Request includes reporting of an issue/problem.
- 1.15. **"Take on Period"** or **"On-Boarding Period"** means the period during which SYNAQ will take on the Client and implement the Services, i.e., execute the necessary configuration to enable the Client to utilise the Services.
- 1.16. **"TeamViewer"** is a computer software tool which allows remote access and remote control to computers and other devices.
- 1.17. **"Virus"** means (but not limited to) malware, which includes viruses, worms, and Trojan horses.

2. SUPPORT SERVICE REQUEST LOGGING PROCESS

- 2.1. Service Requests may only be logged by the Client's Authorised Primary and Technical Contacts. It is the Client's responsibility to ensure that Authorised Contacts are updated as required.
- 2.2. Service Requests can be logged in two (2) ways: a) telephonically on (011) 262 – 3632, and via email at support@synaq.com.
- 2.3. When logging a Service Request with the SYNAQ Support Desk via email, the Client, acting reasonably and in good faith, will assign a Priority Level to the Incident.
- 2.4. Each Service Request received by the SYNAQ Support Desk shall immediately be logged and assigned a Service Request ticket number together with the agreed Priority Level. The Service Request ticket number shall be communicated to the Client.
- 2.5. The SYNAQ Support Desk shall investigate each Service Request in a timely and diligent fashion and shall use all commercially reasonable efforts to promptly resolve (in a manner that minimises chances of recurrence) the Service Request to permit the Client to resume use of the Service.
- 2.6. Service Requests that are logged after-hours will be investigated during office hours (8am – 5pm), unless the Client follows up the requests telephonically and stipulates that immediate assistance is required.
- 2.7. The Priority Level of a particular Service Request may be upgraded or downgraded after the initial response and diagnosis by agreement and recorded within the ticket between the Parties.
- 2.8. Client's will be responsible for the accurate logging of Service Requests by providing the SYNAQ Support Desk with all information and materials reasonably requested for use in resolving a Service Request.
- 2.9. The SYNAQ Service Support Desk shall keep the Client regularly informed of all Service Request progress and shall reasonably endeavour to adhere to the Support Service Levels.

3. REMOTE SUPPORT

- 3.1. Should any logged Service Request require remote support, the SYNAQ Support Desk will utilise the TeamViewer tool. TeamViewer will be used subject to the consent from Client who will be required to provide a passcode to access the tool.
- 3.2. Once the remote support has been completed, the access via TeamViewer will be terminated forthwith by the SYNAQ Support Desk and the Client by exiting the tool.

4. ESCALATIONS PROCESS

4.1. Clients can utilise the below escalation path (in sequence) only once their Service Request(s) has not been responded to or resolved in accordance with SYNAQ's Service Level.

Level	Name	Email	Designation	Landline	Cell
1st	Support Desk	support@synaq.com	Support Team	011 262 3632	011 262 3632
2nd	Nicholas Dooling	nicholasd@synaq.com	Senior Sales Manager	011 262 3632	079 392 3513
3rd	Sonic Kwepile	sonic@synaq.com	Support Team Lead	011 262 3632	076 823 2424
4 th	Lodewyk de Kock	lodewykd@synaq.com	Tech Ops Manager	011 262 3632	082 353 3727
5 th	Thirusha Chetty	thirushac@synaq.com	CTO	011 262 3632	073 165 4496
6 th	David Jacobson	davidj@synaq.com	CEO	011 262 3632	083 235 0760

5. MAINTENANCE (SCHEDULED AND EMERGENCY)

5.1. SYNAQ shall from time to time perform Scheduled Maintenance/Changes or Emergency Maintenance/Changes, subject to: -

5.1.1. Prior written notification shall be provided to the Client of at least 2 (two) days/ 48 hours; except in the case of Emergency Maintenance, where the circumstances under which Emergency Maintenance are to be performed may preclude SYNAQ issuing a notification to the Client within any specified, minimum time period.

5.1.2. Scheduled Maintenance/Changes are only carried out between 22h00 and 06h00 in the region within which the applicable Client site is located from Monday to Saturday mornings and from 22h00 to 08h00 on Sunday mornings.

5.2. All maintenance/ Changes will be communicated via SYNAQ status page: <http://status.synaq.com>.

5.3. The Client is responsible for subscribing to the status page and communicating any Maintenance/Changes to their end users.

5.4. Scheduled Maintenance/Changes shall not be included in the calculation of interrupted service minutes.

5.5. In the event that any scheduled or emergency maintenance period is extended beyond the time initially communicated, SYNAQ will inform the Client via Status Page as well as a telephonic discussion with their Sales Representative to discuss the relevant detail pertaining to same including without limitation, the time at which the Client may expect the services to resume.

6. OUTAGE NOTIFICATIONS

- 6.1. All platform outages and breach notifications will be communicated via the SYNAQ status page: <http://status.synaq.com> provided that the relevant contacts have subscribed to these notifications.
- 6.2. The client is responsible for subscribing to the status page and communicating this to their end users.
- 6.3. Client is responsible for communicating outages to their end users.

7. SYNAQ COMPANY APPOINTED CONTACT DETAILS

Designation	Name	Email	Cell
SYNAQ Sales	SYNAQ Sales	sales@synaq.com	011 262 3632
Senior Sales Manager	Nicholas Dooling	nicholasd@synaq.com	079 392 3513
Finance Manager	Liza Claassen	lizac@synaq.com	083 678 4411
Tech Ops Manager	Lodewyk de Kock	lodewykd@synaq.com	082 353 3727
Client Success	Noluthando Sompeta	noluthandos@synaq.com	0732777293
CTO	Thirusha Chetty	thirushac@synaq.com	073165 4496
CEO	David Jacobson	davidj@synaq.com	083 235 0760

8. SYNAQ SERVICE LEVELS

8.1. Support Service Levels

- 8.1.1. The SYNAQ Support Desk shall investigate each Service Request in a timely and diligent fashion and shall use all commercially reasonable efforts to promptly resolve (in a manner that minimises chances of recurrence) the Service Request to permit the Client to resume use of the Service.
- 8.1.2. The SYNAQ Service Support Desk shall keep the Client informed of all Service Request progress and shall reasonably endeavour to adhere to the Support Service Levels below:

Priority	Response Time ¹	Resolution Time ²	Criteria
CRITICAL	1 hour	8 hours	Business impact CRITICAL: Platform-wide outage affecting entire business and/ or all users. Feedback will be provided consistently.
HIGH	3 hours	8 hours	Business impact serious: Problems impacting the entire business and/or all users.
MEDIUM	3 hours	12 hours	Business impact medium: Problems impacting parts of business and/ or any of their users; Administrative requests for existing services; Sales requests.
LOW	3 hours	24 hours	Business impact non-existent: Administrative requests for new services; "How do I?" type question; Investigative questions.

Note:

- **IMPORTANT: Service Requests that are logged after-hours will be investigated during office hours (8am – 5pm), unless the Client follows up the requests telephonically and stipulates that immediate assistance is required.**
- In the absence of no Priority classification the default Priority will be 4;
- It must be stated that the time frames indicated for resolve times are the average times required to resolve a logged incident / event. SYNAQ will always endeavour to provide excellent support, and as such will always aim to improve on these times. Note that the maximum time to resolve an incident / event is three times the average times indicated above.

1) Time limits

- ¹ -**Response Time** shall mean the elapsed time between a report of a Problem to the SYNAQ help desk [or SYNAQ Engineer and the commencement of problem resolution efforts].
- ² - **Resolution Time** shall mean the elapsed time between commencement of the problem resolution efforts and the successful resolution (i.e. repair, not escalation) of the problem.

9. SYNAQ SERVICE-SPECIFIC SLA'S - CLOUD MAIL AND SECUREMAIL**9.1. Onboarding Period**

- 9.1.1. No measurement of Service Levels will take place during the Onboarding Period. The Service Levels below will only apply subsequent to the Onboarding Period.
- 9.1.2. During the Onboarding Period the Client shall assist reasonably and where necessary where required by SYNAQ to enable SYNAQ to perform the Onboarding tasks to enable the acquired Service.
- 9.1.3. During the Onboarding Period the Client shall execute the necessary configuration (i.e., DNS changes, mail server configuration, firewall configuration etc.) in accordance with SYNAQ's Best Practices Implementation methods. No Service Levels shall apply where Client has not executed the necessary configuration or any other related action in accordance with SYNAQ's Best Practices Implementation document or any other instructions from SYNAQ.
- 9.1.4. SYNAQ shall, at the request of the Client reasonably assist the Client in executing the necessary configuration or check whether the Client has executed the configuration correctly.
- 9.1.5. SYNAQ understands that the Client may not be entirely familiar with the Best Practices Implementation utilised by SYNAQ and as such will provide the Client with assistance required in the use of same to attend to the necessary configuration, within reason. Similarly, should SYNAQ identify that the client has not configured Services correctly, SYNAQ shall inform Client of this and provide the Client with the information necessary to do so.

9.2. Service Level Reporting and Service Level Review**9.2.1. Measurement and Measurement Period**

- a) After the Take on Period, the Service Levels shall equal or exceed the levels set out below as

measured by SYNAQ.

- b) The Measurement period for each Service Level below will be monthly.
- c) Measurement of SYNAQ SecureMail Service Levels will be executed by SYNAQ by using internal service monitoring and reporting tools, or such tool as may be communicated to the Client from time to time.
- d) Measurement of Service Levels only takes place on SYNAQ infrastructure and does not extend to the Client's network (see Service Level Relief below).
- e) Service Levels will only be applicable, provided that Client's adhere to the terms of: SYNAQ's
- f) Acceptable Use Policy and the SecureMail and Cloud Mail Policies (accessible here: <https://www.synaq.com/legal>), which detail the terms for best practice use of the SYNAQ SecureMail and Cloud Mail Services.

9.3. Investigation and Correction

9.3.1. SYNAQ shall promptly investigate and correct failures to meet the Service Levels by:

- a) conducting service analyses of failures in areas for which SYNAQ is responsible and correcting issues in a manner to minimise chances of recurrence, and,
- b) promptly reporting issues to Client that reasonably could be expected to have a material adverse effect on Client's operations.

9.3.2. To enable SYNAQ to achieve its Service Levels on its own infrastructure the Client agrees to correct issues in areas for which Client is responsible and which may prevent SYNAQ from meeting the Service Levels, in a manner that will minimise the chances of recurrence.

9.4. Changed Services

If the composition of a Service is changed (i.e., the Baseline Volume) and it has an effect on the delivery of the Service, then the Parties shall review the Service Levels applicable to the changed Service and, if applicable, agree in writing on new Service Levels, signed by both Parties.

9.5. Service Level Relief

9.5.1. SYNAQ shall be relieved of responsibility for meeting any Service Level where a failure to meet a service level was attributable to:

- a) problems resulting from components (hardware/software/network) for which the Client or another third party is operationally responsible, and which event action or inaction can be proven by SYNAQ to have been out of its control or influence,
- b) changes made by Client, or a Third-Party Supplier, to the Client's environment that may have an effect on the Services to be performed by SYNAQ, which changes were not communicated in advance and authorised by SYNAQ,
- c) where the Client is not using a Best Practice Implementation as supplied by SYNAQ; or circumstances that constitute an event of force majeure, subject to any provision to the contrary contained herein,
- d) an event, action, or inaction outside SYNAQ's control or influence and which event

action or inaction can be proven by SYNAQ to have been out of its control or influence (including but not limited to force majeure events or Internet access or related problems).

- e) performance or non-performance of Third-Party Suppliers and vendors not directly contracted to SYNAQ.

9.5.2. Service Levels shall not apply during Take on Period or during planned maintenance periods.

9.5.3. Notwithstanding the aforementioned Service Level relief SYNAQ will nevertheless attempt to continue to render the Services in accordance with the provisions of the Master Services Agreement and the applicable Service Schedule to the extent that is able to without incurring any additional cost, and taking into account any dependencies that it relies on to enable it to do so. However, if it is unable to do so for any reason without incurring any additional costs, it will be relieved from doing so until such time that Client has approved such additional costs.

9.6. Availability

9.6.1. The Services (unless specifically stated under a Contract) will be available 99% of the time to those paid-up Clients, excluding the periods:-

9.6.1.1. in which SYNAQ are performing Scheduled Maintenance;

9.6.1.2. that result from a termination as described in the Agreement between the parties;

9.6.1.3. that result from suspension due to overdue payments;

9.6.1.4. caused by Client's use of the Services in a manner inconsistent with the documentation or SYNAQ's guidance;

9.6.1.5. caused by Client's use of the Services after SYNAQ advised Client to modify its use of the Services;

9.6.1.6. attributable to acts by persons gaining unauthorized access to or use of the Services due to Client's failure to maintain and control security and access to the Services;

9.6.1.7. attributable to the acts or omissions of customer or its employees, agents, contractors, or vendors, or anyone gaining access to the Services by means of Client's credentials or equipment; and such periods as may result from actions/omissions as per the Service Level Relief as stated under clause 9.5.1 above.

9.6.2. Downtime due to faults, security, software upgrades and/ or deemed critical should be communicated and resolved quickly without significantly affecting the Client or its Users;

9.6.3. The SYNAQ shall use commercially reasonable endeavours to make the Services available as per the above service level, except for:

- 9.6.3.1. planned maintenance carried out during the scheduled maintenance period as notified to the Client were reasonably possible.
- 9.6.3.2. unscheduled maintenance performed outside Normal Business Hours, provided that the SYNAQ has used reasonable endeavours to give the Client at least 6 (six) Normal Business Hours' notice in advance.

9.6.4. It is agreed that the service levels will not apply during the Implementation Phase or Initial Customisation Phase (where applicable).

9.7. Phishing and Cyber Incidents

- 9.7.1.1. It is imperative to take note that no Financial Institution will request a user to provide confidential information, such as a password, username or PIN code via email.
- 9.7.1.2. SYNAQ shall not be liable for any losses, damages or claims (including direct, indirect, consequential, special, or indirect damages or expenses) as a result of any phishing attempt/email or any other cyber incidents that occur during the use of the Services under a user's Service Account credentials (whether authorized or not by the user).
- 9.7.1.3. The Client shall indemnify SYNAQ, its directors and employees accordingly against any claim, losses, expenses and damages whatsoever in terms of a Phishing attack or similar cyber incident.
- 9.7.1.4. It is the responsibility of the Client to educate its employees accordingly and/or other users and to ensure that the users protect their Service Account details.
- 9.7.1.5. The Client is further required to promptly notify SYNAQ of any suspected phishing attempts or cyber incidents.